APROBAT
Preşedintele interimar al Colegiului Penal
al Curţii de Apel Bălţi

_____
Gheorghe Scutelnic

Notă informativă

Generalizarea practicii judiciare cu privire la examinarea cauzelor penale ce vizează infracțiunile comise prin intermediul tehnologiilor informaționale

PREFAȚĂ

Conform planului de activitate al Colegiului penal al Curţii de Apel Bălţi pentru anul 2023, ţinând cont de importanţa şi actualitatea problemei legate de examinarea cauzelor penale ce vizează infracțiunile comise prin intermediul tehnologiilor informaționale, s-a efectuat prezenta notă informativă.

Nota informativă respectivă a Direcţiei sistematizare, generalizare a practicii judiciare şi relaţii cu publicul, cuprinde generalizarea practicii judiciare şi analiza datelor statistice cu privire la examinarea cauzelor penale în ordine de apel privind infracțiunile comise prin intermediul tehnologiilor informaționale, pentru perioada anului 2022.

INTRODUCERE

Odată cu evoluția timpului, societatea îmbrăţişează din ce în ce mai mult tehnologia informaţiei. Informaţia care până nu de mult avea la bază hârtia îmbracă acum forma electronică. Informaţia pe suport de hârtie mai este încă rezervată documentelor oficiale, acolo unde este necesară o semnătură sau o ștampilă. Adoptarea semnăturii electronice deschide însă perspectiva digitizării complete a documentelor, cel puţin din punct de vedere funcţional.

Acest nou mod de lucru, în care calculatorul a devenit un instrument indispensabil şi un mijloc de comunicare prin tehnologii precum poşta electronică sau Internetul, atrage după sine riscuri specifice. O gestiune corespunzătoare a documentelor în format electronic face necesară implementarea unor măsuri

specifice. Măsurile ar trebui să asigure protecţia informaţiilor împotriva pierderii, distrugerii sau divulgării neautorizate. Cel mai sensibil aspect este acela de a asigura securitatea informaţiei gestionată de sistemele informatice în noul context tehnologic.

În timp ce în domeniul tehnologiilor informaţionale schimbarea este exponenţială, componenta umană rămâne neschimbată. Asigurarea securităţii informaţiilor nu se poate realiza exclusiv prin măsuri tehnice, fiind în principal o problemă umană. Majoritatea incidentelor de securitate sunt generate de o gestiune şi organizare necorespunzătoare, şi mai puţin din cauza unei deficienţe a mecanismelor de securitate.

Scopul generalizării

Efectuarea unei analize cu privire la calitatea examinării de către instanțele de fond aflate în jurisdicția Curții de Apel Bălți a cauzelor penale ce vizează infracțiunile comise prin intermediul tehnologiilor informaționale.

Metodologia realizării studiului

Obiectul generalizării a constituit analiza dosarelor penale cu privire la infracțiunile comise prin intermediul tehnologiilor informaționale, examinate de Colegile penale ale Curții de Apel Bălți în perioada 01.01.2022 - 31.12.2022.

Eșantionul studiat

În prezenta generalizare au fost supuse analizei 8 dosare penale care au parvenit în adresa Curții de Apel Bălți în perioada 01.01.2022 - 31.12.2022 și care au avut drept obiect al examinării infracțiunile comise prin intermediul tehnologiilor informaționale.

Această notă informativă este efectuată în baza fişelor de evidenţă statistică a dosarelor penale aflate în procedura de examinare a Colegiului penal al Curţii de Apel Bălţi şi, respectiv, a deciziilor adoptate în cauzele penale în ordine de apel cu privire la infracțiunile comise prin intermediul tehnologiilor informaționale, plasate în Programul Integrat de Gestionare a Dosarelor, pentru perioada anului 2022.

Cadrul normativ relevant

- Constituţia Republicii Moldova;
- Codul penal al Republicii Moldova nr. 985 - XV din 18 aprilie 2002;
- Codul penal al Republicii Moldova, Comentariu, cu modificările de până la 08 august 2003, Centrul de Drept al Avocaţilor, Chişinău 2003;
- Drept penal, Partea Specială, Volumul II, Chișinău 2011, autori Sergiu Brînză și Vitalie Stati;
- Codul de procedură penală al Republicii Moldova Nr.122-XV din 14 martie 2003;
- Codul de procedură penală al Republicii Moldova, Comentariu, Editura Cartier Juridic, Ediţie apărută cu Sprijinul Fundaţiei Soros Moldova şi al Programului Naţiunilor Unite pentru Dezvoltare, Proiectul ”Centrul de Studii şi Politici Juridice”;
- Tratat de Drept Penal, Partea Specială, Volumul II, Chișnău 2015, autori Sergiu Brînză și Vitalie Stati;
- Manualul judecătorului pentru cauze penale, Chișinău 2013, autori Poalelungi Mihail, Dolea Igor, Vîzdoagă Tatiana ș.a;
- Convenţia Europenă pentru Apărarea Drepturilor Omului şi a Libertăţilor Fundamentale;
- Aplicarea pedepsei penale pe categorii de infracțiuni, îndrumar pentru practicieni, Chișinău 2021, autori Gh. Ulianovschi, L. Catan, M. Ghervas, V. Puica, V. Șterbeț;
- Răspunderea penală pentru accesul ilegal la informația computerizată, Chișinău 2023, autor Alexandru Strîmbeanu.

Scurt istoric asupra apariției și evoluției infracțiunilor comise prin intermediul tehnologiilor informaționale

Evoluția tehnologiei informației și sistemelor informatice aflată în pronunțata accesiune și-a pus amprenta asupra tuturor domeniilor vieții sociale, economice, civile etc., influențând decisiv progresul umanității. Acest adevărat *“cyberspațiu”* oferă pe lângă multiplele avantaje, posibilitatea săvârșirii de infracțiuni într-o altfel de modalitate decât cea tradițională.

Criminalitatea în mediul virtual, generic denumită *e-crime* sau *cybercrime* a cunoscut o evoluție dramatică, acestui fenomen putem distinge patru etape, și anume:

- prima (specifică anilor ’80), care a fost caracterizată de banalizarea informaticii, piratarea programelor, falsificarea cărţilor de credit;
- a doua (specifică sfârşitului anilor ’80), a fost favorizată de apariţia reţelelor

locale şi extinse, precum şi a punţilor de legătură, şi caracterizată de importante deturnări de fonduri şi „isprăvile" hacker-ilor care accesau calculatoarele NASA, CIA şi oricare altă ţintă care reprezenta un simbol politico-tehnologic sau un element al puternicului complex militaro-industrial american;

- a treia (specifică anilor '90), care a coincis cu proliferarea sistemelor informatice şi reţelelor de comunicaţii (Internet-ului, în special) şi a fost caracterizată de specializarea infractorilor, apariţia unor „veritabili" profesionişti ai pirateriei, deturnărilor de fonduri, sabotajelor informatice;
- a patra (în prezent), favorizată de faptul că sistemele informatice au pătruns în toate sectoarele vieţii sociale şi le controlează pe cele mai importante dintre ele (transporturi, apărare, etc.), şi care este caracterizată de conturarea de noi şi grave ameninţări ca terorismul informatic, războiul informatic etc.

Printre primele organizaţii internaţionale ce au efectuat un studiu privind unificarea legislaţiei în domeniu, este Organizaţia pentru Cooperare Economică şi Dezvoltare (OECD). Astfel, OECD în anul 1983, a întocmit un raport în care a invocat mai multe recomandări de origine legislativă, statelor membre ale UE, precum şi o listă minimă de activităţi ce urmează a fi sancţionate: *fraudarea şi falsificarea realizată prin calculator, alterarea programelor de calcul şi a datelor, copyright-ul, interceptarea comunicaţiilor sau a altor funcţii a unui calculator, accesul şi utilizarea neautorizată a unui calculator*.

În acelaşi timp, ulterior acţiunilor OECD, Consiliul Europei a iniţiat o nouă cercetare de caz pentru examinarea cadrului legal privind combaterea criminalităţii informatice, în vederea dezvoltării acestuia.

Este de reţinut, că elemente de iniţiere în materia criminalităţii informatice au fost realizate de către Consiliul Europei cu ocazia celei de-a XII-lea conferinţe a directorilor Institutelor de Cercetare Criminologică – *Conferinţa Consiliului Europei asupra aspectelor criminologice ale infracţiunilor economice* (15-17 noiembrie 1976). În acest context, au fost instituite un şir de infracţiuni în domeniul informatic, inclusiv pentru prima dată s-a introdus cea de fraudă.

Începând cu aprilie 1976, în interiorul Uniunii Europene au fost adoptate mai multe rezoluţii şi recomandări (1976, 1979, 1982), apogeul acestor activităţi a finalizat cu recomandarea parvenită de la Comisia Europeană pentru statele-membre să semneze *Convenţia pentru protecţia persoanelor cu privire la prelucrarea automată a datelor cu caracter personal*, la Strasbourg la 28 ianuarie1981(ratificată de către Republica Moldova prin Hotărârea Parlamentului RM nr. 483-XIV din 02 iulie 1999).

Ulterior, Consiliul Europei în 1985 a instituit - Comisia de experţi în domeniul criminalităţii pe calculator de pe lângă Consiliul Europei - care a analizat prevederile mai multor legislaţii naţionale, a dezbătut problema criminalităţii informatice şi şi-a încheiat activitatea în anul 1989 când a perfectat şi a rezultat cu adoptarea *Recomandării R(89)9*, deşi fără a impune obligaţii statelor membre, aceasta constituie o veritabilă călăuză pentru statele membre ale UE.

În consecinţa adoptării *Recomandării R(89)9,* Consiliul Europei a înfiinţat Comitetul de experţi (1991) în scopul acostării aspectelor procedurale care ţin de investigarea infracţiunilor din domeniul informatic, stabilind că specificul acestor infracţiuni urmează a fi repercutat cu instrumente juridico-procedurale inedite, adaptate tehnologiilor informaţionale. În consecinţă, raportul Comitetului de experţi a constituit fundamentul adoptării de către Comitetul de Miniştri a *Recomandării (95) 13 din aprilie 1995* relativ aspectelor de procedură penală cu privire la tehnologia informaţiei.

În temeiul unui raport întocmit de *Comitetul pentru mass-media, Comitetul de Miniştri* adoptă şi publică *Recomandarea (88)2* din 18 ianuarie1988 privind măsurile, ce vizează combaterea pirateriei în domeniul drepturilor de autor şi al drepturilor conexe, care reţinea printre altele că *autorii programelor software trebuie să se bucure de protecţia drepturilor de copyright*.

Activitatea Comisiei Europeane şi Consiliului Europei a fost una enormă, desfăşurând mai multe evenimente cu obiectul de referinţă printre care şi Conferinţa de la Luxemburg (1987).

Urmează directiva europeană *91/250/ EEC23 cu privire la protecţia legală a programelor de calculator*, prin care Uniunea Europeană obliga respectarea drepturilor de autor în acest domeniu şi sancţiona pirateria informatică, iar prin directiva *95/46/EC24* protecţia persoanelor cu privire la prelucrarea automată a datelor cu caracter personal şi libera circulaţie a acestor date, statele-membre au fost obligate să pună în aplicare dispoziţiile acesteia, între care se aflau şi confidenţialitatea şi securitatea procesării acestor date, precum şi remediile de natură judiciară, sancţiuni şi pedepse.

Comunitatea internaţională în marea ei parte recunoaşte că *Convenţia Consiliului Europei privind Criminalitatea Informatică* reprezintă partea economică printre reglementările juridice internaționale în domeniul prevenirii şi combaterii criminalității informatice, deoarece aceasta aspiră să devină acel instrument juridic mondial, fiind ratificată și semnată de un număr crescând de state din diferite părţi ale lumii, semnată la Budapesta la 23 noiembrie 2001 (ratificată de către Republica Moldova prin Legea Parlamentului RM nr. 6 din 02.02.2009).

Convenției Consiliului Europei privind criminalitatea informatică i s-a alăturat un protocol adiţional (adoptat la Strasbourg la 28 ianuarie 2003). Protocolul conţine prevederi prin care sunt incriminate - *publicarea prin reţelele informatice a oricăror conţinuturi propagandistice rasiste sau xenofobe* - ca fapte penale.

Organizaţia Naţiunilor Unite s-a implicat, la fel, în cercetarea şi elaborarea unor măsuri privind combaterea fenomenului enunţat. În consecinţă au fost întocmite şi publicate mai multe acte, printre care se enumeră:

- raportul "*Propuneri privind concertarea acţiunilor internaţionale privind combaterea oricărei forme de activitate criminală*" (1985);
- *Rezoluţia introdusă de reprezentantul Canadei privind combaterea criminalităţii pe calculator* (1990);

- *Rezoluţia 54/95 Adunării Generale ONU (1990) privind principiile de bază pentru reglementarea datelor informatice cu caracter personal*;
- *Declaraţia Naţiunilor Unite privind principiile de bază ale justiţiei aplicabile victimelor abuzului de putere şi crimei* (1990);
- raportul "*Provocarea fără frontiere: Cybercrime - eforturi internaţionale pentru combaterea crimei organizate, transnaţionale*" (2000);
- *Rezoluţiile Adunării Generale a ONU nr. 55/63 din 4.12.2000 şi nr. 56/121 din 19.12.2001;*
- *Convenţia Naţiunilor Unite privind drepturile copilului adoptată la 20.11.1989* (fiind incriminată pornografia infantilă);
- *Convenția Națiunilor Unite împotriva criminalității organizate transfrontaliere* (cuprinde prevederi în legătură cu asistența judiciară internațională în materie penală (art.18) și dispoziții referitoare la extrădare (art.16)).

În cadrul ONU, în mod efectiv lupta împotriva criminalităţii informative se consideră desfăşurarea lucrărilor *Congresului al VIII-lea al ONU privind prevenirea infracţiunilor şi tratamentul infractorilor* de la Havana 27 august - 7 septembrie 1990, unde au fost puse în discuţie şi unele aspecte ale criminalităţii informatice, rezoluţia adoptată la finele congresului vizează încurajarea statelor-membre să adopte măsuri pentru a preveni şi combate acest fenomen.

Congresul X al ONU privind prevenirea criminalităţii şi justiţia penală de la Viena desfăşurat între 10 - 17 aprilie 2000 a avut pe agenda sa dezbateri privind eficacitatea măsurilor luate atât la nivel naţional, cât şi la nivel internaţional în vederea prevenirii şi combaterii criminalităţii informatice şi a criminalităţii noilor tehnologii. Un alt subiect dezbătut relativ cu criminalitatea informatică a fost cel privind oportunitatea acordării asistenţei tehnice, financiare şi materiale din partea statelor industrializate statelor puţin dezvoltate, dar în care se oferă teren propice infractorilor-cibernetici.

Un eveniment important în interiorul ONU din punctul de vedere al cercetărilor în materia examinată l-a reprezentat cel privind publicarea de către ONU al *Manualului Naţiunilor Unite pentru prevenirea şi controlul infracţiunilor informatice*. Acest document a strălucit prin identificarea categoriilor infracţiunilor din domeniul informatic, or aceasta constituie segmentul iniţial important. Astfel, acest document a sintetizat următoarele categorii de infracţiuni:

- fraude prin manipularea calculatoarelor electronice;
- fraude prin falsificarea de documente;
- alterarea sau modificarea datelor sau a programelor pentru calculator;
- accesul neautorizat la sisteme şi servicii informatice;
- reproducerea neautorizată a programelor pentru calculator protejate de lege.

Începutul procesului de legiferare în domeniul infracţiunilor informatice a înregistrat mai multe etape, prima datând cu anii 1970, ulterior urmând şi alte multe etape.

Prima etapă este caracterizată de oportunitatea protejării dreptului la viaţa privată. Norme privind protecţia persoanei fizice în domeniul prelucrării datelor cu caracter personal au fost adoptate în multiple state din sistemul continental, dar şi din sistemul englezo-american, cum ar fi: *Suedia* (1973), *SUA* (1974), *Austria*, *Danemarca*, *Franţa* şi *Norvegia* (1978); mai târziu în *Belgia*, *Spania*, *Elveţia* (1992), *Italia şi Grecia* (1997).

A doua etapă coincide cu etapa de represiune a infracţiunilor din domeniul economic, soldate cu modificări la nivel legislativ: în *SUA* şi *Italia* (1978), *Australia* (1979), *Marea Britanie* (1981), *Elveţia* (1994) şi *Spania* (1995).

Cea de a treia etapă de intervenţie legislativă – este cea privind protecţia proprietăţii intelectuale în domeniul legat de tehnologii informatice, modificări ce au fost operate în următoarele state: *SUA* (1980), *Ungaria* (1983), *Germania*, *Franţa, Japonia, Marea Britanie* (1985), *Austria* (1993), *România* (1996), *Luxemburg* (1997).

A patra etapă priveşte reglementările vizând distribuirea informaţiilor ilegale sau cauzatoare de prejudicii, demonstrând la sfârşitul anilor 1980 o impulsionare de amploare prin intermediul reţelei Internet.

A cincea etapă ţine de modificările legislative ce au intervenit în materia dreptului procesual-penal, impuse de imperfecţiunile în aplicarea normelor de procedură penală, ca rezultat al utilizării tehnologiei informaţiei.

Etapa a şasea priveşte aspectul legislativ prin instituirea unor obligaţii şi limite în materia securităţii informatice.

Potrivit Parlamentului European, amenințările cibernetice au cunoscut o creștere importantă în anul 2021, pandemia Covid-19 având un impact major. În contextul în care progresul înregistrat de transformare digitală a adus inevitabil și noi amenințări de securitate cibernetică. Infractorii cibernetici au profitat de pandemia Covid-19, vizând în special organizațiile și companiile care activau de la distanță.

Dreptul a fost pus în faţa noilor provocări condiţionate de dezvoltările tehnologice. Tocmai de aceea legiuitorii din toate statele au fost preocupaţi de elaborarea unui cadru normativ care să reglementeze accesul şi desfăşurarea activităţii prin intermediul sistemelor informatice în diferite sectoare.

Aspecte generale asupra infracțiunilor comise prin intermediul tehnologiilor informaționale

Asigurarea securităţii internaţionale a devenit în vârful actualităţii cercetărilor recente or, odată cu avansarea tehnologiilor informaţionale în practica zi de zi în diverse sfere ale vieţii s-a reclamat o intensitate a criminalităţii prin intermediul acestora.

Criminalitatea informatică reprezintă totalitatea faptelor comise în zona tehnologiilor informaţionale, într-o anumită perioadă de timp bine determinată şi pe un anumit teritoriu. Ca orice fenomen social, criminalitatea informatică reprezintă un sistem cu proprietăţi şi funcţii proprii, distincte calitativ de cele ale elementelor componente. În cercetarea criminologică, criminalitatea ca fenomen social cuprinde:

- criminalitatea reală – presupune totalitatea faptelor penale săvârşite pe un anumit teritoriu şi într-o anumită perioadă de timp;
- criminalitatea aparentă – cuprinde întregul set de infracţiuni semnalate organelor abilitate ale statului şi înregistrate ca atare;
- criminalitatea legală – reprezintă totalitatea faptelor de natură penală comise în spaţiul tehnologiilor informaţionale şi pentru care s-au pronunţat hotărâri judecătoreşti rămase definitive.

Fiecare din acest segment de criminalitate îşi are corespondenţa şi în criminalitatea informatică. Diferenţa dintre criminalitatea informatică reală şi criminalitatea informatică aparentă reprezintă cifra neagră a acestui nou gen de crimă şi ea cuprinde toate faptele sancţionate de legiuitor, dar care, din anumite motive, rămân nedescoperite de către organele abilitate ale justiţiei penale.

Investigarea criminalistică a sistemelor informatice prezintă o serie de particularităţi care o diferenţiază în mod fundamental de alte tipuri de investigaţii. Investigarea criminalistică a sistemelor informatice poate fi definită ca: utilizarea de metode ştiinţifice şi certe de asigurare, colectare, validare, identificare, analiză, interpretare, documentare şi prezentare a probelor de natură digitală, obţinute din surse de natură informatică în scopul facilitării descoperirii adevărului în cadrul procesului penal.

Un algoritm din practica investigaţiilor criminalistice de natură informatică cuprinde următorii paşi:

1. Identificarea incidentului – recunoaşterea unui incident şi determinarea tipului acestuia. Nu reprezintă efectiv o etapă a investigaţiei criminalistice, dar are un impact semnificativ asupra următoarelor etape.
2. Pregătirea investigaţiei – pregătirea instrumentelor, verificarea procedurilor, obţinerea documentelor ce permit percheziţia etc.
3. Formularea strategiei de abordare – formularea unei strategii în funcţie de tehnologia implicată şi de posibilele consecinţe asupra persoanelor şi instituţiilor implicate. Scopul formulării acestei strategii este să maximizeze potenţialul obţinerii de probe relevante, minimizând în acelaşi timp impactul negativ asupra victimei.
4. Asigurarea probelor – izolarea, asigurarea şi păstrarea probelor de natură fizică şi digitală. Aceasta include îndepărtarea celor care ar putea denatura probele în orice fel.
5. Colectarea probelor – înregistrarea ambianţei fizice şi copierea probelor digitale, folosind practici şi proceduri comune şi acceptate.
6. Examinarea probelor – examinarea în profunzime a probelor în căutarea elementelor care sunt în legătură cu fapta penală investigată. Acest lucru presupune

localizarea şi identificarea probelor, precum şi documentarea fiecărui pas în scopul facilitării analizei.

7. Analiza probelor – determinarea semnificaţiei probelor şi relevarea concluziilor cu privire la fapta investigată.

8. Prezentarea probelor – sintetizarea concluziilor şi prezentarea lor într-un mod inteligibil pentru nespecialişti. Această sinteză trebuie susţinută de o documentaţie tehnică detaliată.

9. Restituirea probelor – dacă este cazul, returnarea către proprietarii de drept a obiectelor reţinute în timpul investigaţiei. Dacă este cazul, determinarea, în funcţie de prevederile legilor procedurale penale, a confiscării obiectelor.

Investigarea criminalistică a sistemelor informatice trebuie să prezinte o serie de caracteristici specifice, necesare asigurării unui grad înalt de corectitudine a concluziilor rezultate. Aceste caracteristici sunt:

1. Autenticitate (dovada sursei de provenienţă a probelor);
2. Credibilitate (lipsa oricăror dubii asupra credibilităţii şi solidităţii probelor);
3. Completitudine (prelevarea tuturor probelor existente şi integritatea acestora);
4. Lipsa interferenţelor şi a contaminării probelor ca rezultat al investigaţiei sau al manipulării probelor după ridicarea acestora.

Criminalitatea informatică poate să aibă un preţ foarte ridicat pe plan economic, dar şi în termenii securităţii umane. Uşurinţa accesului la informaţie în sistemele informatice, combinată cu posibilitatea practic nelimitată de schimb sau disiminare a acestora, indiferent de graniţele geografice sau naţionale, a dus la o creştere explozivă a cantităţii de informaţie disponibilă şi a cunoştinţelor ce pot fi extrase din aceasta. Această evoluţie a dat naştere la schimbări economice şi sociale fără precedent, dar în acelaşi timp foloseşte şi scopuri mai puţin legitime: apariţia unor noi infracţiuni sau săvârşirea infracţiunilor tradiţionale prin intermediul noilor tehnologii. Adesea locul săvârşirii infracţiunii diferă de locul unde se găseşte infractorul. Prin o simplă apăsare a unui buton acesta poate declanşa catastrofe la mii de km depărtare. Infractorul digital este ascuns în spatele tastaturii și riscul de a fi descoperit este destul de mic.

În timpul pandemiei Covid-19, companiile au fost nevoite să se adapteze rapid noilor condiții de lucru „oferind” astfel noi posibilități pentru criminalii cibernetici. Conform Agenției Uniunii Europene pentru Securitate Cibernetică (ENISA), există nouă tipuri de amenințări principale:

1. **Ransomware** – atacatorii criptează datele unei organizații și cer o răscumpărare pentru a reda accesul;
2. **Cryptojacking** – criminalii folosesc în secret puterea de calcul a dispozitivului victimei pentru a genera criptomonede;
3. **Amenințări la adresa datelor** – accesări ilicite de date/ scurgeri de date;
4. **Malware** – un software care declanșează un proces ce afectează un sistem;
5. **Dezinformare** – distribuirea de informații înșelătoare;

6. **Amenințări fără potențial dăunător** – erori umane și configurări greșite ale unui sistem;
7. **Amenințări la adresa disponibilității și integrității** – atacuri care împiedică utilizatorii unui sistem să își acceseze informațiile;
8. **Amenințări legate de email** – urmăresc să manipuleze persoane pentru a cădea victime ale unui atac prin email;
9. **Amenințări pe lanțul de aprovizionare** – atacarea unui furnizor de servicii, pentru a obține acces la datele clienților acestuia.

Potivit doctrinei internaționale, utilizatorii sunt cei care favorizează şi înlesnesc operarea infractorilor, dând dovadă de naivitate şi neatenţie în momentul în care se angajează în tranzacţii financiare cu persoane sau companii care nu le sunt cunoscute şi care nu prezintă siguranţă. Din categoria factorilor favorizanţi ai criminalităţii informatice, care depind în mare măsură de factorul uman, sunt:

- utilizarea măsurilor de plată on-line în medii de lucru nesecurizate;
- neutilizarea de site-uri dedicate unor anumite activităţi şi care au un grad ridicat de certificare;
- neverificarea informaţiilor furnizate de vânzătorii on-line: numere de telefon, adrese de email;
- furnizarea datelor cu caracter secret la accesarea unor site-uri de origine dubioasă;
- efectuarea de plăţi în avans, fără a exista o confirmare a trimiterii produselor;
- furnizarea de informaţii suplimentare de către cumpărător, în condiţiile în care acestea nu sunt necesare pentru validarea tranzacţiei.

Marea majoritate a acestor infracțiuni sunt comise în sfera financiar bancară. Totodată, această categorie juridico-penală nu cuprinde nici pe departe întregul spectru al aplicării tehnologiilor informaționale în scopuri criminale. Informațiile electronice sunt folosite de frecvente ori și la comiterea unor asemenea infracțiuni tradiționale cum sunt escrocheriile, falsurile, dobândirea creditelor prin înșelăciune, practicarea ilegală a activității de întreprinzător, evaziunile fiscale etc., ca de exemplu, pentru: falsificarea documentelor de plată; sustragerea mijloacelor bănești prin transferul acestora în conturi fictive; procurarea bunurilor prin folosirea mijloacelor de plată electronice falsificate sau sustrase; vânzarea informațiilor secrete ș.a.

Caracteristica componențelor de infracțiuni comise prin intermediul tehnologiilor informaționale

În Partea specială a Codului penal al Republicii Moldova, componențele de infracțiuni sunt grupate în capitole, în funcție de obiectul juridic generic. Așadar,

obiectul juridic generic reprezintă factorul unificator pentru un grup de infracțiuni prevăzute de un anumit capitol al Părții speciale a Codului sus numit.

Astfel, Capitolul XI din Codul Penal al Republicii Moldova reglementează la moment următoarele infracţiuni:

1. Accesul ilegal la informaţia computerizată (art. 259);
2. Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau produselor program (art. 260);
3. Interceptarea ilegală a unei transmisii de date informatice (art. 260^1);
4. Alterarea integrităţii datelor informatice ţinute într-un sistem informatic (art. 260^2);
5. Perturbarea funcţionării sistemului informatic (art. 260^3);
6. Producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similare (art. 260^4);
7. Falsul informatic (art. 260^5);
8. Frauda informatică (art. 260^6);
9. Încălcarea regulilor de securitate a sistemului informatic (art. 261);
10. Accesul neautorizat la reţelele şi serviciile de telecomunicaţii (art. 261^1).

Titlul initial al capitolului XI din partea special a Codului penal al Republicii Moldova a fost "Infracțiuni în domeniul informaticii". Ulterior, a fost adoptată Legea nr. 254 din 09.07.2004 pentru modificarea și completarea Legii telecomunicațiilor nr. 520-XIII din 07.07.1995 și a Codului penal al Republicii Moldova nr. 254 din 09.07.2004, prin care respectivul cod a fost completat cu articolul 261^1 "Accesul neautorizat la rețelele și serviciile de telecomunicații", iar capitolul XI din partea specială a Codului penal al Republicii Moldova a fost modificat, devenind "Infracțiuni în domeniul informaticii și telecomunicațiilor". Acest titlu nu a avut o lungă durată, deoarece, prin Legea nr. 278 din 18.12.2008 pentru modificarea și completarea Codului penal al Republicii Moldova, titlul capitolului XI a fost modificat, devenind "Infracțiuni informatice și infracțiuni în domeniul telecomunicațiilor".

Sintagma "tehnologie informațională" caracterizează metoda de comitere a unor infracțiuni care sunt prevăzute de capitole diferite ale Părții speciale a Codului penal al Republicii Moldova. Sintagma dată nu poate desemna factorul de grupare doar a infracțiunilor prevăzute în capitolul XI din Partea special a Codului penal al Republicii Moldova, această opinie o găsim în doctrina de specialitate atât națională, cât și internațională potrivit căreia: "Infracțiunile cibernetice trebuie privite ca fapte intenționate săvârșite prin utilizarea tehnologiei IT".

Într-o altă ordine de idei, se evidențiază că componența infracțiunii este alcătuită dintr-un sistem complex de elemente constitutive, printre care se enumeră: obiectul, latura obiectivă, subiectul şi latura subiectivă. Celor patru elemente constitutive le corespund anumite semne, ce caracterizează aceste elemente constitutive.

Obiectul infracțiunii reprezintă elementul constitutiv al oricărei infracțiuni, el permite disocierea ilicitului penal de ilicitul non-penal, precum și caracterizează în mod clar gradul de pericol social al infracțiunii. Nu în ultimul rând, obiectul are o semnificație decisivă pentru relevare caracterului pericolului social al infracțiunii comise, constituind cel mai relevant criteriu de calsificare și de sistematizare a normelor penale.

Astfel, se relevă că ***obiectul juridic generic*** al infracțiunilor din grupul analizat îl constituie relațiile sociale din domeniul informaticii și al telecomunicațiilor.

Explicit sau implicit, toate infracțiunile, care sunt prevăzute la art. 259 – 261^1 Cod penal al Republicii Moldova, presupun afectarea într-o măsură mai pronunțată sau mai redusă a relațiilor sociale referitoare la securitatea datelor informatice. Lezarea obiectului juridic special al acestor infracțiuni se realizează pe calea influenţării directe asupra datelor informatice. Aceasta o confirmă sintagmele: „informaţia computerizată” (art. 259 și 261 Cod penal); „date informatice” (art. 260^1 – 260^3, 260^5 și 260^6 Cod penal).

În continuare, vom examina în parte fiecare componență de infracțiune prevăzute la capitolul XI Cod penal al Republicii Moldova.

Astfel, infracțiunile, ce sunt prevăzute de **art. 259 Cod penal**, sunt biobiectuale. Despre aceasta ne vorbește structura faptei prejudiciabile prevăzute de acest articol. Fapta prejudiciabilă analizată include două componente:

1) acţiunea principală de acces ilegal la informaţia computerizată;

2) acţiunea adiacentă de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice.

Acţiunea principală aduce atingere obiectului juridic principal al infracțiunilor prevăzute la art. 259 Cod penal, pe când acţiunea adiacentă aduce atingere obiectului juridic secundar al acestor infracțiuni.

Obiectul juridic principal al infracțiunilor ce sunt specificate în art. 259 Cod penal îl formează relaţiile sociale cu privire la accesul permis sau autorizat la informaţia computerizată.

Obiectul juridic secundar al infracțiunilor nominalizate îl constituie relaţiile sociale cu privire la integritatea, autenticitatea, disponibilitatea sau ireproductibilitatea informației computerizate ori funcționalitatea calculatoarelor, a sistemului sau a reţelei informatice, apărate împotriva cauzării de:

1) daune în proporții mari (în cazul infracțiunii prevăzute la alin. (1));

2) daune în proporții deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2)).

Infracțiunile, prevăzute la art. 259 Cod penal, au **obiect imaterial principal** care constă în informația computerizată accesată ilegal.

În cazul acelorași infracțiuni, informația computerizată distrusă, deteriorată, modificată, blocată sau copiată constituie **obiectul imaterial secundar**;

calculatoarele, sistemul informatic sau reţeaua informatică, a căror funcționare a fost dereglată formează **obiectul material secundar**.

Sistemul informatic este un obiect. După domeniile de activitate cărora li se adresează sistemele informatice pot fi: economice, științifice, de documentare, de inginerie tehnologică etc. În funcție de gradul de concentrare/dispersare a capacităților de prelucrare și memorare a datelor, distingem: sisteme concentrate și sisteme distribuite. Indiferent de tipul sistemului informatic, acesta reprezintă obiectul material al infracțiunilor prevăzute la art. 259 Cod penal.

Referitor la celelelte infracțiuni stipulate în capitolul Codului penal supus cercetării, menționăm, că obiectul juridic special simplu reprezintă:

- pentru art. 260 Cod penal – relațiile sociale cu privire la circulația legală a mijloacelor tehnice sau produselor program;
- pentru art. 260^1 Cod penal – relații sociale cu privire la legalitatea interceptării unei transmisii de date informatice care nu sunt publice;
- pentru art. 260^2 Cod penal – relațiile sociale cu privire la integritatea, accesibilitatea și circulația în condiții de legalitate a datelor informatice;
- pentru art. 260^3 Cod penal – relațiile sociale cu privire la buna fucționare a unui sistem informatic sub aspectul inviolabilității domiciliului informatic;
- pentru art. 260^4 Cod penal – relațiile sociale cu privire la încrederea în datele informatice care permit accesul la un sistem informatic, în sensul utilizării corecte și legale a acestora, precum și în desfășurarea corectă și legală a operațiunilor comerciale în legătură cu acestea;
- pentru art. 260^5 Cod penal – relațiile sociale cu privire la încrederea publică în siguranța și fiabilitatea sistemelor informatice, în valabilitatea și autenticitatea datelor informatice, a întregului proces modern de prelucrare, stocare și tranzacționare automată a datelor de interes oficial sau privat;
- pentru art. 260^6 Cod penal – relațiile sociale cu privire la integritatea patrimoniului unei persoane, atunci când prezența respectivei persoane în spațiul cibernetic se cuantifică într-un anumit volum de date stocate într-un sistem informatic sau vehiculate într-o rețea;
- pentru art. 261 Cod penal – relațiile sociale cu privire la securitatea sistemului informatic.

Obiectul material sau imaterial al infracţiunilor sus menționate îl reprezintă:

- informaţia computerizată a calculatoarelor, sistemului informatic sau reţelei informatice (art. 259 Cod penal);
- informaţia protejată de lege (lit. g) alin. (2) art. 259 Cod penal);
- mijloacele tehnice sau produsele program, concepute sau adaptate, în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. art. 237, 259, 260^1 -260^3, 260^5, 260^6 Cod penal;
- transmisia de date informatice (inclusiv a unei emisii electronice) care nu sunt publice şi care sunt destinate unui sistem informatic, ce provin dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic (art. 260^1 Cod penal);

- datele informatice dintr-un sistem informatic, dintr-un mijloc de stocare sau cu acces limitat (art. 260^2 Cod penal);

- datele informatice (art. 260^2, 260^5 şi 260^6 Cod penal);

- parola codului de acces sau datelor similare care permit accesul total sau parţial la un sistem informatic (art. 260^4 Cod penal);

- informaţia computerizată a altor entităţi, inerente pe fundalul provocării unor urmări grave (art. 261 Cod penal).

Latura obiectivă reprezintă unul dintre elementele constitutive ale infracțiunii. Indiferent dacă infracțiunea este formală sau materilă, latura ei obiectivă include ca semn constitutiv fapta prejudiciabilă. Acest semn se referă la manifestarea exterioară a infracțiunii, la comportamentul făptuitorului care se concretizează în acțiune sau inacțiune.

Sub aspectul ***laturii obiective***, este necesar a menţiona că infracţiunile informatice se comit prin acţiune în cazul componenților prevăzute la art. 259, 260, 260^1 – 260^6 Cod penal sau inacţiune, în cazul componenților prevăzute la art. 261 Cod penal; latura obiectivă fiind una materială la componențele art. 259, 260^2 – 260^6, 261 Cod penal) sau formală, în cazul celor prevăzute la art. art. 260, 260^1 Cod penal.

În legătură cu varianta în vigoare a art. 259 Cod penal, are următoarea structură a laturii obiective:

1) fapta prejudiciabilă care constă în acţiunea principală de acces ilegal la informaţia computerizată, însoţită de acţiunea adiacentă de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei, de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice;
2) urmările prejudiciabile, și anume – daunele în proporţii mari;
3) legătura cauzală dintre fapta prejudiciabilă şi urmările prejudiciabile”

După cum rezultă din dispoziția de la alin. (1) art. 259 Cod penal, nu orice acces la informația computerizată intră sub incidența articolului respectiv, condiția obligatorie este ca accesul la informația computerizată să fie ilegal. Astfel, doar accesul ilegal la informația computerizată este insuficient pentru a întregi fapta prejudiciabilă prevăzută la art. 259 Cod penal, acțiunea principală se poate afla în legătură cauzală cu urmările prejudiciabile numai dacă este însoțită de acțiunea adiacentă.

Cu referire la timpul săvârșirii infracțiunilor informatice, potrivit doctrine, de cele mai multe ori, atacurile cibernetice sunt săvârșite în perioada zilelor de odihnă, precum și în orele matinale, atunci când serviciile de securitate sunt mai pasive, iar solicitarea ajutoarelor este mai dificilă, precum și la finele zilei de muncă.

Pentru caracteristica timpului comiterii infracțiunii informatice se folosește timpul astronomic, adică o anumită durată de timp în limita căreia se realizează modalitatea de comitere a faptei de la începutul ei până la survenirea consecințelor socialmente periculoase. Marea parte a acțiunilor infracționale se comit pe timp de noapte datorită scăderii încărcării și randamentului de lucru al dispozitivelor

informaționale. Condițiile și împrejurările comiterii infracțiunii sunt influențate de starea mijloacelor de apărare și protecția a tehnicii informaționale.

Practica organelor de drept din domeniul cercetării și prevenirii infracțiunilor informatice ne demonstrează că în marea majoritate a cazurilor infractorii, de sine stătător, creează condițiile necesare pentru comiterea faptei. Astfel, pot fi creați viruși și programe speciale de acces neautorizat cu scop de diminuare a nivelului de apărare a tehnicii informaționale. Condițiile și împrejurările comiterii infracțiunilor informatice sunt categorii dinamice. Chiar și cel mai experimentat infractor din domeniul tehnologiilor informaționale nu de fiecare dată este capabil să aprecieze schimbarea lor sub aspect favorabil sau nefavorabil în procesul comiterii infracțiunii. În rezultatul acțiunilor urgente sau greșite rămân urme ale infracțiunii care reprezintă unica posibilitate reală de restabilire a mecanismului infracțiunii comise.

Latura subiectivă a infracțiunii se exprimă în atitudinea psihică a făptuitorului față de fapta prejudiciabilă și față de urmările prejudiciabile, precum și în motiv, scop și emoții.

În privința ***laturii subiective*** se menţionează, că forma de vinovăţie la infracţiunile analizate se exprimă prin intenţie – la art. art. 259, 260, 260^1 – 260^6 Cod penal și prin intenţie sau imprudenţă în raport cu fapta prejudiciabilă şi numai imprudenţă în raport cu urmările prejudiciabile survenite - la art. 261 Cod penal.

În componența infracțiunilor prevăzute de lit. f) alin. (2) art. 259; art. art. 260; 260^4 – 260^6 Cod penal, legiuitorul stabilește în calitate de semn obligatoriu scopul special, și anume:

- scopul comiterii uneia dintre infracţiunile specificate la alin. (1) art. 259, art. 260^1 -260^3, 260^5 și 260^6 – la art. 259 alin. (2) lit. f) Cod penal;
- scopul săvârșirii uneia dintre infracţiunile specificate la art. art. 237, 259, 260^1 – 260^3, 260^5 şi 260^6 – la art. art. 260, 260^4 Cod penal;
- scopul de utilizare a datelor necorespunzătoare adevărului în vederea producerii unei consecinţe juridice – la art. 260^5 Cod penal);
- scopul de a obţine un beneficiu material – la art. 260^6 Cod penal.

Totodată, motivul infracțiunii ca semn secundar al laturii subiective se exprimă prin interesul material, fiind obligatoriu în cazul componențelor prevăzute la art. 260^3 alin. (2) lit. a) şi la art. 260^4 alin. (2) lit. a) Cod penal.

Potrivit art. 21 Cod penal, prin „subiect al infracțiunii” se înțelege doar persoana care săvârșește infracțiunea.

Subiect al infracţiunilor comise prin intermediul tehnologiilor informaționale poate fi orice persoană fizică responsabilă, care la momentul săvârșirii infracţiunii a împlinit vârsta răspunderii penale: 14 ani (art. 260 Cod penal) sau 16 ani (în celelalte cazuri).

Subiectul special în cazul art. art. 259, 260, 260^1, 260^3, 260^4, 261 Cod penal îl reprezintă persoana juridică (cu excepția autorității publice).

La fel, subiectul componenței art. 259 Cod penal are o calitate specială și anume, persoana care nu este autorizată în temeiul legii sau al unui contract şi care depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic.

De asemenea, subiect special există și în cazul componenței de infracțiune prevăzută la art. 261 Cod penal, adică persoana în ale cărei obligaţii intră respectarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic.

Clasificarea categoriilor de infractori în cyberspaţiu, depinde atât de o combinaţie de factori sociali, tehnologici şi legali, cât şi de modul în care aceste categorii de infractori sunt definite.

O clasificare succintă a acestora poate fi următoarea:

- Utilizatorii neglijenţi care violează politicile de securitate sau nu respectă practicile de securitate, şi prin urmare, datele care se află în reţea pot fi afectate;
- Infractorii tradiţionali care comit infracţiuni convenţionale, aceştia folosind computere sau alte tipuri de dispozitive electronice pentru comunicaţii şi care păstrează înregistrările în sprijinul activităţilor lor infracţionale;
- Şarlatanii şi hoţii incluzând pe cei care practică activităţi de phishing, spoofing, spimming (mesaje comerciale nesolicitate trimise printr-un sistem de mesagerie instantanee), sau „*înşală*" oamenii în alte moduri în vederea obţinerii de câştiguri financiare;
- Hacker-ii, computer trespassers (intruşii informatici) şi password crackers (spărgătorii de parole) cunoscuţi şi sub numele de hackeri white hat sau gray hat, care urmând tradiţia eticii originale a *hacker-ilor,* folosesc computerele pentru a explora ilegal, pentru a învăţa şi pentru a prelua controlul asupra sistemelor ca să facă pozne, şi care ar putea să găsească, să exploateze, sau să expună vulnerabilităţile de securitate ș.a. Această categorie de infractori pot fi experţi în domeniul noilor tehnologii, cum sunt, de exemplu, hackerii, experţii în securitatea sistemelor informatice, programatorii şi alţi specialişti în domeniul Internetului.

De asemenea, infractorii din cyberspaţiu pot acţiona ca un grup organizat prin schimbul de informaţii fără a dezvălui identitatea lor pe Internet, îngreunând activităţile de investigare ale organelor de urmărire penală. De multe ori infractorul informatic este departe de locul unde se săvârşeşte fapta ilicită. Infractorii pot alege locul unde ei se vor afla în momentul săvârşirii infracţiunii, întrucât criminalitatea din spaţiul informatic nu necesită prezenţa fizică a făptuitorului la locul săvârşirii faptei ilicite.

Conform prevederilor Convenției Consiliului Europei privind criminalitatea informatică, sunt distinse trei tipuri ale infracțiunilor examinate: a) infracțiuni contra confidențialității și integrității datelor și sistemelor informatice; b) infracțiuni informatice în accepțiune strictă; c) infracțiuni în domeniul telecomunicațiilor.

Nivelul comiterii infracțiunilor săvârșite prin intermediul tehnologiilor informaționale în Republica Moldova în perioada raportată

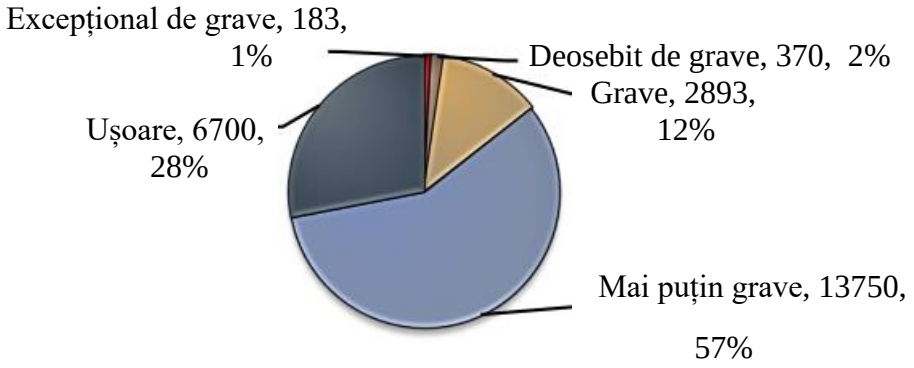
Potrivit informației Biroului Național de Statistică privind nivelul infracționalității în anul 2022, numărul infracţiunilor înregistrate este în scădere față de anul precedent.

Conform datelor Ministerului Afacerilor Interne, în anul 2022, pe teritoriul Republicii Moldova au fost înregistrate 23896 infracțiuni, dintre care 34,29% revenind municipiului Chișinău. Fenomenul infracțional a înregistrat o descreștere cu -1,97%, comparativ cu perioada analogică a anului precedent.

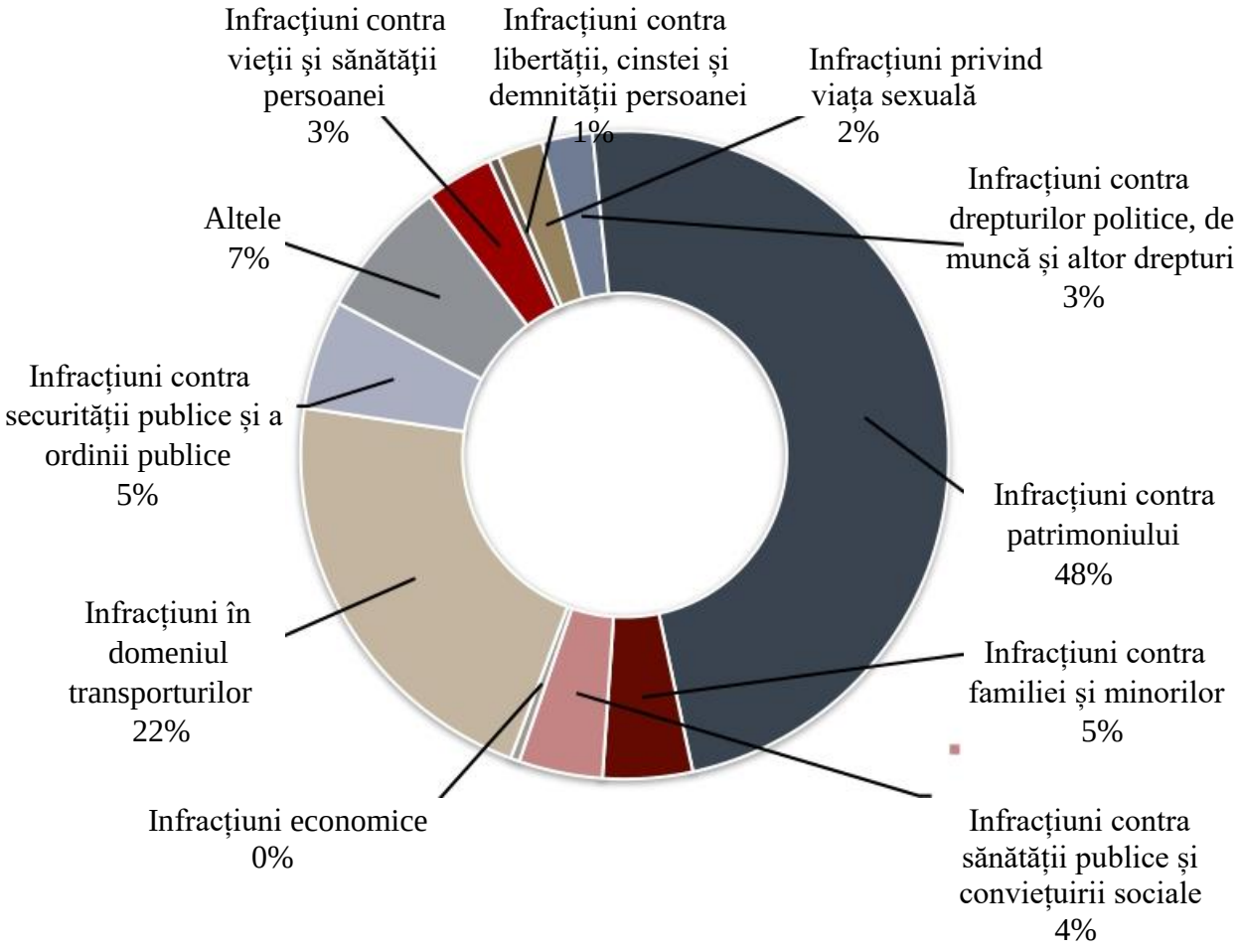
Din numărul total de infracțiuni, au fost trimise procurorului 15784 cauze penale *(66,05%)*, pe 13639 cauze penale a fost finisată urmărirea penală *(57,08%)*, dintre care 10437 cauze penale au fost trimise în judecată *(43,68%)*.

În perioada anului 2022 criminalitatea a înregistrat diminuare a infracțiunilor din categoriile celor deosebit de grave cu -6,8% *(370/397)*, grave cu -20,8% *(2893/3651)* și ușoare cu -3,83% *(6700/6967)*.

Creștere au înregistrat infracțiunile din categoria celor excepțional de grave cu +10,91% *(183/165)*, mai puțin grave cu +4,19% *(13750/13197)*.



Din numărul total de infracțiuni, 48% revin infracțiunilor patrimoniale, 22% (5 062 infracțiuni) se atribuie celor în domeniul transporturilor, 5% (1 274 infracțiuni) celor contra securității și ordinii publice, 5% (1 047 infracțiuni) celor contra familiei și minorilor și 4% (982 infracțiuni) contra sănătății publice și conviețuirii sociale.



În cadrul activităților de urmărire penală și investigare a infracțiunilor, Poliţia a reușit stabilirea autorilor în proporţie de:

- *93,17 % pe cauzele în domeniul transporturilor;*
- *84,32% pe cauzele penale contra vieţii şi sănătăţii persoanelor;*
- *83,57% pe cauzele contra familiei și minorilor;*
- *82,63% pe cauzele contra drepturilor politice;*
- *78,72% pe cauzele contra sănătății publice;*
- *75,35% pe cauzele contra securității publice;*
- *65,53% pe cauzele penale privind viaţa sexuală;*

- *62,91% pe cauzele penale contra justiției.*

Genurile de infracțiuni în care există cele mai multe fapte cu autori neidentificați:

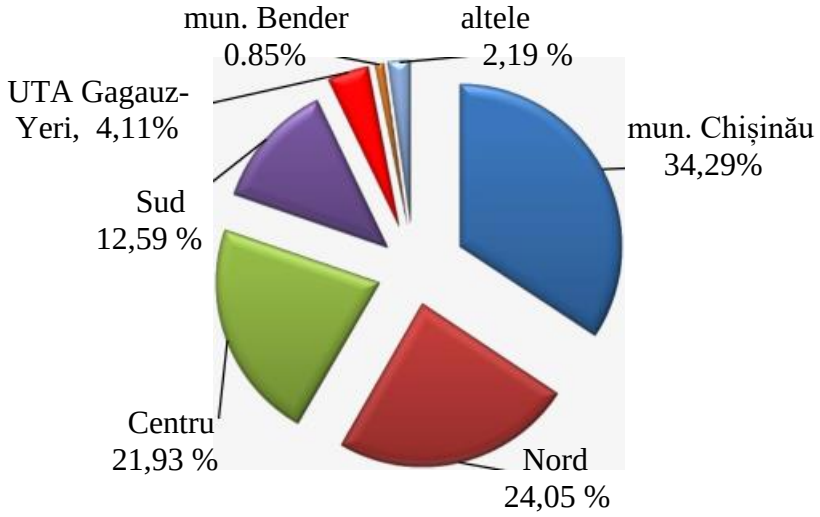
- *infracțiuni contra libertății (50,83)%;*
- *infracțiuni contra patrimoniului (48,83%);*
- *infracțiuni contra bunei desfășurări a activității în sfera publică (51,11%);*
- *infracțiuni economice (25,71%);*
- *infracțiuni ecologice (30%).*
- *infracțiuni informatice (20%).*

În perioada 12 luni ale anului 2022 se atestă creșteri la unele genuri de infracțiuni, comparativ cu perioada analogică a anului 2021:

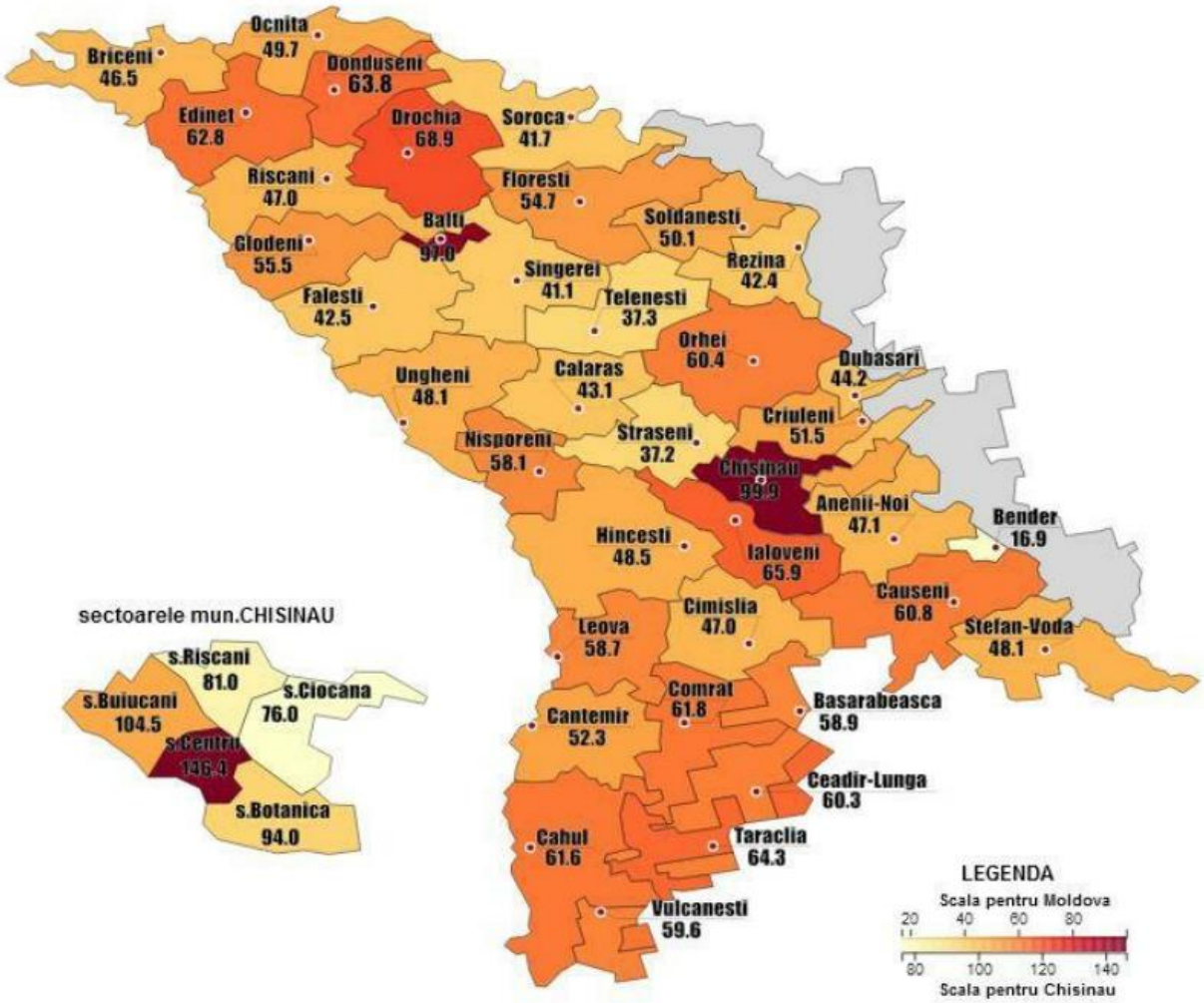
- contra bunei desfășurări a activității în sfera publică cu 109,3%;
- infracțiuni informatice cu 105,9%;
- infracțiuni economice cu 32,91%;
- contra sănătății publice cu 16,35%;
- contra securității publice cu 4,6%;
- contra libertății cu 2,56%;
- contra drepturilor politice cu 2,24%.

Conform criteriului de divizare regională a infracționalității, se atestă că fenomenul infracțional este concentrat în mediul urban, în proporție de 60%.

Pe criteriul regional, cele mai multe infracțiuni au fost înregistrate în mun. Chișinău – 8194, urmat de subdiviziunile regiunii Nord – 5747, Centru – 5241, Sud – 3008, DP UTA Găgăuzia – 981 și mun. Bender – 202 infracțiuni.



Rata criminalităţii la nivel national în perioada analizată, conform Recensământului Populației și al Locuințelor 2014, constituie 70,99 infracțiuni la 10 mii locuitori.



Cele mai afectate unități administrativ-teritoriale din punct de vedere a ratei criminalității sunt municipiile Chișinău, Bălți, precum și raioanele Drochia, Dondușeni, Edineț, Cahul, Comrat, Ialoveni, Căușeni, Taraclia, Orhei, Ceadîr-Lunga.

Conform informațiilor extrase din Sistemul informațional automatizat, în perioada de raport în comiterea infracțiunilor au fost stabilite 13 482 persoane. Din numărul total de persoane care au săvârșit infracţiuni, 306 nu sunt la prima abatere. Totodată 277 persoane sunt străini şi/sau persoane fără cetăţenie.

În perioada 12 luni ale anului 2022, pentru săvârșirea infracțiunilor informatice și infracțiunilor din domeniul comunicațiilor electronice, au fost pornite 206 cauze penale, comparativ cu 221 cauze penale înregistrate în perioada analogică a anului 2021.

În perioada raportată, numărul infracțiunilor săvârșite cu utilizarea sistemelor informatice prin escrocherie înregistrând 78 cauze, a cunoscut o dinamică ascendentă față de perioada analogică a anului trecut unde au fost înregistrate 16 cauze.

Totodată, se atestă o descreștere esențială a fraudelor cu utilizarea cardurilor bancare a clienților mai multor bănci din Republica Moldova (art. 186 Cod penal), în anul 2022 fiind înregistrate 49 cauze penale, comparativ cu 141 cauze penale înregistrate în anul 2021. Acest lucru se datorează acțiunilor de prevenire și informării societății civile a cazurilor de criminalitate informatică și a riscurilor acestora. Dar, totuși fraudele cu cardurile bancare rămân a fi un trend, cu un un risc major.

Dacă ne referim la evoluția în perioada ultimilor ani în special infracțiunea de fraudă informatică (art. 260/6 CP RM), anul curent se atestă o descreștere fiind înregistrate 5 cauze penale comparativ cu 7 cauze penale înregistrate în perioada anului 2021.

Date statistice privind activitatea Curții de Apel Bălți, pe cauzele ce vizează infracțiunile comise prin intermediul tehnologiilor informaționale

Conform datelor statistice, în perioada nominalizată în cadrul Curţii de Apel Bălţi **s-au aflat în procedură 8 cauze penale** privind infracțiunile comise prin intermediul tehnologiilor informaționale prevăzute la art. art. 190; 206; 208^1 Cod penal, pe 8 persoane, dintre care **au fost examinate 7 cauze** pe 7 persoane **(87,5 %).**

Restul dosarelor neîncheiate la sfârşitul perioadei raportate şi care se regăsesc în procedură de examinare pentru perioada anului 2023, **constituie 1 cauză** pe 1 persoană **(12,5 %).**

În procedura Curții deApel Bălți în perioada anului 2022 nu s-au examinat și nu au parvenit nici o cauză penală privind infracțiunile stipulate la capitolul XI din Codul penal al Republicii Moldova, și anume Infracțiuni informatice și infracțiuni în domeniul telecomunicațiilor (art. art. 259 – 261^1).

Din totalul de 7 cauze examinate privind infracțiunile comise prin intermediul tehnologiilor informaționale pe 7 persoane, au fost emise următoarele soluții:

- Hotărâre nouă – 4 cauze pe 4 de persoane (57,14 %);
- Fără modifiări – 3 cauze pe 3 de persoane (42,85 %).

Din totalul de 7 cauze examinate pe 7 persoane:
- pe art. 190 Cod penal au fost examinate 4 cauze pe 4 persoane;
- pe art. 206 Cod penal au fost examinate 1 cauză pe 1 persoană;
- pe art. 208^1 Cod penal au fost examinate 2 cauze pe 2 persoane.

Judecătorii Colegiului Penal al Curții de Apel Bălți în perioada raportată au soluționat:

1. Ion Talpa - 1 cauză aflată în procedură pe 1 persoană, care a fost examinată:
- hotărâre nouă - 1/1 persoană (100 %).

2. Svetlana Șleahtițki - 2 cauze aflate în procedură pe 2 persoane, dintre care au fost examinată 1 cauză pe 1 persoană:
- hotărâre nouă - 1/1 persoană (50 %).

3. Gheorghe Scutelnic - 1 cauză aflată în procedură pe 1 persoană, care a fost examinată:
- fără modificări – 1/1 persoană (100 %).

4. Oleg Moraru - 1 cauză aflată în procedură pe 1 persoană, care a fost examinată:
- hotărâre nouă - 1/1 persoană (100 %).

5. Viorel Pușcaș - 1 cauză aflată în procedură pe 1 persoană, care a fost examinată:
- fără modificări – 1/1 persoană (100 %).

6. Ala Rotaru - 1 cauză aflată în procedură pe 1 persoană, care a fost examinată:
- hotărâre nouă - 1/1 persoană (100 %).

7. Ruslana Burdeniuc - 1 cauză aflată în procedură pe 1 persoană, care a fost examinată:
- fără modificări – 1/1 persoană (100 %).

În tabelul de mai jos, reflectăm, care sunt indicii statistici privind examinarea cauzelor penale pe art. art. 190, 206, 208[1] Cod penal, împotriva sentințelor instanțelor de fond din raza de activitate a Curții de Apel Bălți, pentru perioada anului 2022.

Instanța de judecată	**Total cauze parvenite/ persoane**	**Cauze examinate/ persoane**	**Fără modificări**	**Casat, hotărâre nouă**	**Rest 2023**
Jud. Bălți (sediul Central)	3/3	3/3	1/1	2/2	-
Sediul Sângerei	-	-	-	-	-
Sediul Fălești	-	-	-	-	-
Total Jud. Bălți	**3/3**	**3/3**	**1/1**	**2/2**	-
Jud. Soroca (sediul Central)	2/2	2/2	1/1	1/1	-
Sediul Florești	-	-	-	-	-
Total Jud. Soroca	**2/2**	**2/2**	**1/1**	**1/1**	-
Jud. Drochia (sediul Central)	-	-	-	-	-
Sediul Glodeni	1/1	1/1	-	1/1	-
Sediul Râșcani	2/2	1/1	1/1	-	1/1
Total Jud. Drochia	**3/3**	**2/2**	**1/1**	**1/1**	**1/1**
TOTAL	**8/8**	**7/7**	**3/3**	**4/4**	**1/1**

Practica judiciară de examinare a cauzelor ce vizează infracţiunile comise prin intermediul tehnologiilor informaţionale de către Curtea de Apel Bălţi

Ca urmare a analizei şi studierii deciziilor adoptate de către Colegiul penal al Curţii de Apel Bălţi, în cauzele penale privind infracțiunile comise prin intermediul tehnologiilor informaționale, s-a concluzionat că sentinţele primelor instanţe au fost casate, în cea mai mare parte, în latura pedepsei pe motivul ***adoptării Legii nr. 243 din 24.12.2021 privind amnistia în legătură cu aniversarea a XXX-a de la proclamarea independenței Republicii Moldova,*** la fel și din cauza aplicării incorecte a actului respectiv.

Amnistia, este actul de clemenţă al puterii legiuitoare, care, conform art. 107 Cod penal, are ca efect înlăturarea răspunderii penale sau a pedepsei fie reducerea pedepsei aplicate sau comutarea ei. Aplicarea amnistiei faţă de inculpat nu constituie temei de reabilitare a acestuia.

Potrivit prevederilor art. 389 alin. (4) Cod de procedură penală sentinţa de condamnare se adoptă: 2) cu stabilirea pedepsei şi cu liberarea de executarea ei în cazul amnistiei conform art. 107 din Codul penal.

Cu titlu de exemplu poate fi adusă decizia Curții de Apel Bălți din 20.09.2022 prin care a fost casată parțial sentința instanței de fond în cauza penală prin care a fost încetat procesul penal în privința lui C. D. învinuit de comiterea infracțiunilor prevăzute de art. art. 190 alin. (1); 190 alin. (1); 190 alin. (1) Cod penal al RM, în temeiul art. 2 alin. (1) din Legea nr. 243 din 24 decembrie 2021 privind amnistia în legătură cu aniversarea a XXX-a de la proclamarea independenței Republicii Moldova.

Prin aceiași sentință a fost admisă integral acţiunea civilă înaintată de R. N., P. I. și B. V. împotriva lui C. D., cu încasarea de la ultimul a prejudiciului material în beneficiul lui R. N. în sumă de 20 700 lei, în beneficiul lui P. I. în sumă de 68 392 lei și în beneficiul lui B. V. în sumă de 23 000 lei.

În fapt, instanța de fond a reținut că C. D. la data de 14.04.2019 având scopul dobândirii ilicite a bunurilor altei persoane, manifestând un comportament dolosiv, prin prezentarea ca adevărată a faptei mincinoase în privința naturii, calității substanțiale ale obiectului, aflându-se în XX, l-a indus în eroare pe P. I. solicitând prin intermediul rețelei de socializare „vkontakte”, suma de 300 euro, sub pretextul de a repara automobilul său, cu condiția că va întoarce banii timp de 7 zile, drept urmare comportamentului dolosiv a dobândit ilicit suma solicitată de 300 euro, ceia

ce conform ratei de schimba valutar constituie 6046 lei, pe care i-a însușit, eschivându-se, fără a recepționa apelurile telefonice și sms efectuate de către P. I., cauzându-i daune în proporții considerabile.

Tot el, continuându-și acțiunile sale criminale, îndreptate la dobândirea ilicită a bunurilor altei persoane, în intervalul de timp de la 11.01.2019 până la 14.01.2020 aflându-se în XX acționând din interes material, manifestând un comportament dolosiv, prin prezentarea ca adevărată a faptei mincinoase în privința naturii, calității substanțiale ale obiectului, l-a indus în eroare pe R. N., sub pretextul că, are nevoie de bani pe un termen scurt, l-a determinat pe ultimul să transfere diferite sume de bani prin intermediul bancomatului pe numele său, în vederea folosirii la jocurile pe internet cu obținerea unui profit și transmiterea unei părți către partea vătămată, ca urmare a dobândit ilicit în mai multe rate suma totală de 1000 euro echivalentul a 20 700 lei, pe care i-a însușit, cauzându-i părții vătămate daune în proporții considerabile.

Tot el, continuîndu-și acțiunile sale criminale, îndreptate la dobândirea ilicită a bunurilor altei persoane, la 28.11.2020 în jurul orei 17:00, aflându-se în XX acționând din interes material, manifestând un comportament dolosiv, prin prezentarea ca adevărată a faptei mincinoase în privința naturii, calității substanțiale ale obiectului, l-a indus în eroare pe B. V., sub pretextul că dorește să închirieze pe o perioadă de 24 ore, consola de jocuri de model „Sony Playstation 4 Pro” cu 2 djoystick-rui la preț total de 10000 lei, usby har „HDD” extern cu capacitate de 4 TB, la preț de 2000 lei și jocurile înscrise în discul intern și extern al consolei, la preț de 11 000 lei, în schimbul sumei de 200 lei, cu condiția că, după 24 ore va întoarce consola, însușind consola de jocuri, drept urmare comportamentului dolosiv a dobândit ilicit consola de jocuri, prin ce a cauzat lui B. V., o daună materială considerabilă în sumă totală de 23000 lei.

Prin decizia Colegiului penal al Curții de Apel Bălți din 20.09.2022 ce a soluționat cauza în ordine de apel, a fost admis apelul procurorului în Procuratura xx, casată parțial sentința în latura pedepsei și emisă o hotărâre nouă prin care C. D. a fost recunoscut vinovat de săvârșirea infracțiunilor prevăzute la art. art. 190 alin. (1); 190 alin. (1); 190 alin. (1) Cod penal, și condamnat cu aplicarea prevederilor art. 84 alin. (1) Cod penal la pedeapsa definitivă de 2 ani închisoare, cu executare în penitenciar de tip semiînchis. În temeiul art. 389 alin. (4) pct. 2) Cod de procedură penală și art. 2 din Legea privind amnistia în legătură cu aniversarea a XXX-a de la proclamarea Independenței Republicii Moldova nr. 243 din 24.12.2021, C. D. a fost

liberat de la executarea pedepsei stabilite, cu menținerea în rest a dispozițiilor sentinței instanței de fond.

În motivarea soluției adoptate, Colegiul penal a reținut, că instanța de fond a dat o apreciere corectă probelor și circumstanțelor cauzei penale, examinând probele administrate din punctul de vedere a utilității și veridicității lor, sub toate aspectele, complet și în mod obiectiv, încadrând just acțiunile inculpatului C. D. la art. 190 alin. (1) Cod penal, însă soluția primei instanțe prin care a fost încetat procesul penal pe motivul intervenirii amnistiei este nefondată, or, art. 107 Cod penal stabilește că amnistia este actul care are ca efect înlăturarea de pedeapsă penală, în speţă obligatoriu urma a fi stabilită pedeapsă inculpatului vizat în comiterea faptelor încriminate în baza art. 190 alin. (1); 190 alin. (1) și art. 190 alin. (1) Cod penal cu absolvirea de la executarea pedepsei, fapt care nu ar fi posibil în cazul încetării procesului penal. La fel, art. 389 Cod de procedură penală este unica normă procesuală care permite recunoașterea persoanei culpabile de comiterea unei infracțiuni (art. 285 alin. (2), 275 pct. 4) Cod de procedură penală).

Colegiul s-a expus în privința pedepsei penale, ținând cont de prevederile art. 61 Cod penal, conform căruia pedeapsa penală este o măsură de constrângere statală şi un mijloc de corectare şi reeducare a condamnatului şi respectiv la rândul său are drept scop restabilirea echităţii sociale, corectarea condamnatului, precum şi prevenirea săvârşirii de noi infracţiuni atât din partea condamnatului, cât şi a altor persoane. La fel și de prevederile art. 75 Cod penal, potrivit cărora persoanei recunoscute vinovate de săvârşirea unei infracţiuni i se aplică o pedeapsă echitabilă în limitele fixate în Partea specială a prezentului cod în strictă conformitate cu dispoziţiile Părţii generale a prezentului cod.

Astfel, instanța de apel în temeiul art. 84 alin. (1) Cod penal pentru concurs de infracțiuni, prin cumul parțial al pedepselor aplicare a stabilit inculpatului C. D. pedeapsa definitivă sub formă de 2 ani închisoare. Ținând cont de cumulul circumstanțelor cauzei, Colegiul a considerat că reeducarea și corijarea inculpatului va fi posibilă prin stabilirea pedepsei sub formă de închisoare, astfel va fi atins scopul pedepsei de restabilire a echităţii sociale, corectarea inculpatului, precum şi prevenirea săvârşirii de noi infracţiuni din partea acestuia, cât şi a altor persoane.

Conform art. 389 alin. (4) Cod de procedură penală, sentința de condamnare se adoptă cu stabilirea pedepsei și cu liberarea de executarea ei în cazul amnistiei conform art. 107 din Codul penal și în cazurile prevăzute în art. 89 alin. (2) lit. a), b), c), e), f) și g) din Codul penal. În situația stabilită pe caz, ținând cont de prevederile enunțate, Colegiul penal a considerat că anumite interdicții în vederea

aplicării actului de amnistie nu sunt, inculpatul neîncadrându-se sub interdicţia reglementată la art. 6 din prezenta lege.

Drept urmare, fiind verificată baza de date a hotărârilor Colegiului penal al Curții Supreme de Justiție, nu s-a atestat contestarea cu recurs ordinar a deciziei Curții de Apel Bălți din 20.09.2022.

În cadrul judecării cauzelor penale în ordine apel privind infracțiunile comise prin intermediul tehnologiilor informaționale, Colegiul penal a reținut ***temeinicia sentințelor primelor instanțe*** în ce privește constatarea ca fiind dovedită a vinovăției și încadrarea juridică a acțiunilor potrivit normelor dreptului penal, printr-o apreciere obiectivă a probatoriului conform art. 93-101 Cod de procedură penală, cât și aplicarea pedepselor echitabile inculpaților.

Astfel, prin sentința judecătoriei XXX sediul XXX din 29.12.2021 C. V. a fost condamnat pe art. 208/1 Cod penal la 1 (unu) an închisoare, cu privarea de dreptul de a exercita o activitate în domeniul tehnologiilor informaționale pe un termen de 2 (doi) ani. În temeiul art. 90 Cod penal, pedeapsa stabilită lui C. V. a fost suspendată condiționat pe perioada de probațiune de 1 (unu) an.

Pentru a se expune, instanța de fond a reținut, că C. V. în perioada de timp cuprinsă între 18.07.2020 - 14.04.2021, aflându-se la domiciliul său amplasat în YY, acționând cu intenția unică de a descărca, folosi şi deține din spațiul Internet imagini foto/video sau alte reprezentări ale unui sau mai mulți copii implicați în activități sexuale explicite, reale sau simulate, imagini sau alte reprezentări ale organelor sexuale ale unui copil, reprezentate de manieră lascivă sau obscenă, utilizând sisteme informatice ce erau conectate la rețeaua internet inclusiv cu adresa IP xx, ce i-a fost alocată ultimului de compania de telecomunicații ZZ, cu adresa conectării la domiciliul său, intenționat a folosit, deținut şi distribuit în rețeaua Internet, prin intermediul aplicației de tip „Google Drive”, autentificată cu adresa de e-mail zz, numărul de telefonie mobile ww, prin intermediul programei specializate pentru copierea şi distribuirea fișierelor de internet ce utilizează protocolul de partajare a fișierelor în rețea de tip „Bittorent” în baza principiului „de la egal la egal” - 38 de fișiere grafice, care potrivit bazei de date internaționale „ICACCOPS” (Internet Crymes Againts Children Child Online Protection System) se atribuie la categoria pornografiei infantile, printre care şi următoarele fișiere cu valoarea HASH de tip SHA1: cu valoarea HASH de tip SHA1:

1. Fișierul „93ba9650e41828168a805e2fda2b1fcf7a7c6875”;
2. Fișierul „f890bf7c457c62bfl478b98a9fc679920cbl851”;
3. Fișierul „7fl 3af8daa7fldf8985da6bc021f3454ffc646ef”.

Potrivit procesului-verbal de examinare din 16.08.2021, fiind examinate rapoartele ce conțin informația cu privire la fișierele foto/video extrase în cadrul examinării de către Secția nr. Operațional tehnică al Direcției investigații infracțiuni

informatice al INI al ICJP CU utilizarea aplicației criminalistice „Magnet Axiom” din blocul de sistem „Gamemax”, s/n: ridicat la 27.07.2021 în cadrul efectuării percheziției la domiciliul cet. C. V. în YY, au fost stabilite 28102 foto fișiere foto şi 661 fișiere video atribuite la categoria „pornografiei infantile”, 311863 fișiere foto şi 690 fişiere video atribuite la categoria „Interes Investigativ” pe care ultimul le-a vizualizat şi deținut până la 27.07.2021, care există şi sunt înregistrate în Baza de date specializată în identificarea victimelor pornografiei infantile, abuzului şi exploatării sexuale a copiilor administrate de OIPC „Interpol” - ICSE ca fiind material din categoria pornografiei infantile. La examinarea DSI-ul de tip HDD de model „Transcend” cu capacitatea de 1.5 Tb (1 500 Gb), s/n: ridicat în cadrul efectuării percheziției din 27.07.2021 la domiciliul lui C. V. s-au stabilit 3874 fișiere foto şi 140 fișiere video atribuite la categoria „pornografiei infantile”, 118878 fișiere foto şi 777 fișiere video la categoria „Interes Investigativ” pe care ultimul le-a vizualizat şi deținut până la 27.07.2021, care există şi sunt înregistrate în Baza de date specializată în identificarea victimelor pornografiei infantile, abuzului şi exploatării sexuale a copiilor administrată de OIPC „Interpol” - ICSE ca fiind material din categoria pornografiei infantile.

Prin decizia Colegiului penal al Curții de Apel Bălți din 17.05.2022 apelul declarat de către procurorul în Procuratura pentru Combaterea Criminalității Organizate și Cauze Speciale oficiul Nord Sergiu Railean împotriva sentinței Judecătoriei Soroca sediul Central din 29 decembrie 2021 în cauza lui C. V. a fost respins ca nefondat, cu menținerea acesteia fără modificări.

Colegiul penal, examinând cauza în procedură simplificată potrivit art. 364^1 Cod de procedură penală, adică în baza probelor administrate la faza urmăririi penale, acceptate de către inculpat în corespundere cu alin.(3) a normei vizate prin cererea depusă până la începerea cercetării judecătorești, potrivit căreia el a recunoscut în totalitate faptele indicate în rechizitoriu.

Atât la faza urmăririi penale, cât și în instanța de fond și cea de apel inculpatul C. V. a recunoscut faptele săvârșite, depunând sub jurământ declarații consecvente referitor la cele comise, acestea coroborând întru tot cu restul probelor administrate pe caz.

Colegiul penal a constatat că, instanța de fond a stabilit corect starea de fapt și de drept, ce corespunde probelor din dosar, care au fost apreciate just, încadrând just acțiunile inculpatului C. V. pe art. 208^1 Cod penal, cu semnele calificative: *pornografie infantilă, adică distribuirea, folosirea şi deținerea de imagini sau alte reprezentări ale unui sau mai mulți copii implicați în activități sexuale explicite, reale sau simulate, imagini sau alte reprezentări ale organelor sexuale ale unui copil, reprezentate de manieră lascivă sau obscenă, în formă electronică.*

Colegiul a considerat că, instanța de fond a emis o sentință legală şi întemeiată, apreciind fiecare probă din punct de vedere al pertinenței, concludenții, utilității și veridicității, iar toate probele în ansamblu - din punct de vedere al coroborării lor, în conformitate cu prevederile art. 101 Cod de procedură penală.

În decizia emisă s-a invocat că, instanța de fond a stabilit în mod corect situația de fapt și de drept, vinovăția inculpatului, care a fost dovedită cu certitudine și fără echivoc, apreciind faptele săvârșite de acesta, încadrarea juridică corespunzătoare materialului probator administrat, cercetarea judecătorească fiind efectuată cu respectarea dispozițiilor procesual-penale privind administrarea probelor.

Referitor la individualizarea pedepsei inculpatului, Colegiul penal a constatat că, instanța de fond a acordat deplină eficiență prevederilor art. art. 6, 7, 61, 75 Cod penal, respectiv, a ținut cont de gravitatea infracțiunii săvârșite, de motivul acesteia, de persoana celui vinovat, de circumstanțele care atenuează ori agravează răspunderea penală, de influența pedepsei aplicate asupra corectării și reeducării vinovatului, precum și de condițiile de viață ale familiei acestuia. Ca urmare just considerând că în privința inculpatului C. V. este echitabilă aplicarea unei pedepse cu închisoarea cu suspendarea condiționată a executării pedepsei pe un termen de probă de 1 (unu) an, aceasta va atinge scopul legii penale de restabilire a echității sociale, corectare a condamnatului, precum şi prevenirea săvârșirii de noi infracțiuni atât din partea condamnatului, cât şi a altor persoane.

Suspendarea condiționată este o măsură de individualizare a executării pedepsei numite de către instanțele de judecată prin hotărâre de condamnare de a suspenda pe o perioadă anumită executarea pedepsei aplicate, dacă sunt îndeplinite anumite condiții, care se referă la: pedeapsa aplicată şi natura infracțiunii; circumstanțele cauzei şi persoana infractorului; aprecierea instanței că scopul poate fi atins şi fără executarea acesteia.

Astfel Colegiul penal a menționat că, nu este rațional ca inculpatul C. V. să ispășească real pedeapsa cu închisoare, or, pericolul de a fi anulată suspendarea condiționată a executării pedepsei cu închisoare, în cazul încălcării condițiilor termenului de probă, va îndrepta comportamentul inculpatului la corectare, la respectarea ordinii stabilite în societate, precum și la respectarea legilor.

Analizând personalitatea inculpatului s-a stabilit că, acesta anterior nu a fost în conflict cu legea penală, a comis pentru prima dată o infracțiune mai puțin gravă, și-a recunoscut vina, este căsătorit, are la întreținere doi copii minori, la locul de trai se caracterizează pozitiv.

Respectiv, Colegiul penal a statuat că, pedeapsa stabilită de către instanța de fond cu aplicarea prevederilor art. 90 Cod penal, suspendând condiționat executarea ei, este echitabilă, întrucât este capabilă de a contribui la realizarea scopurilor pedepsei penale, cum ar fi restabilirea echității sociale, corectarea condamnatului şi prevenirea săvârșirii de noi infracțiuni atât de către condamnat, precum şi de alte persoane. Or, practica judiciară demonstrează că o pedeapsă prea aspră generează apariția unor sentimente de nedreptate, jignire, înrăire şi de neîncredere în lege, fapt ce poate duce la consecințe contrare scopului urmărit. La fel, o pedeapsă prea blândă generează dispreț față de ea şi nu este suficientă nici pentru corectarea infractorului şi nici pentru prevenirea săvârșirii de noi infracțiuni.

La verificarea bazei de date a hotărârilor Colegiului penal al Curții Supreme de Justiție, s-a atestat contestarea cu recurs ordinar a deciziei Curții de Apel Bălți din 17.05.2022, care a fost menținută fără modificări.

CONCLUZII

Panorama juridică a lumii este în continuă modificare datorită performanţelor tot mai accelerate a tehnologiei informatice, iar cooperarea internaţională este în faţa unei provocări continue cauzată de creşterea criminalităţii informatice transnaţionale.

Statele s-au văzut nevoite a purcede la armonizarea activă a propriilor legislaţii în vederea combaterii fenomenului enunţat, însă consecinţele sunt doar satisfăcătoare, dar în rezultat nu se poate reţine eradicarea în totalitate a fenomenului propriu-zis.

Datorită specificul său, criminalitatea informatică a devenit o varietate a problemei de criminalitate transnaţională, imposibilă a fi soluţionată de către un singur stat, doar cu cooperarea celorlalte state implicate. Graţie noilor tehnologii, făptuitorul poate comite infracţiunea stând comod în faţa monitorului său într-o locaţie situată la kilometri de locul survenirii daunelor acestei fapte. În esenţă, infracţiunea din domeniul informatic a ieşit din limitele dreptului penal şi procesual-penal tradiţional, a generat oportunitatea nu doar a unor instrumente juridice inedite adecvate de luptă împotriva acesteia, dar a şi impus statele să adopte reglementări cu un grad mai eficace, ce ţin de cooperarea internaţională între organele judiciare penale.

Sistemele informatice, care au schimbat radical modul de viaţă al oamenilor, au oferit noi ocazii, mult mai sofisticate, prin care legea poate fi încălcată; în acelaşi timp, au oferit mijloace noi de comitere a unor delicte tradiţionale care până acum nu au mai fost experimentate. Într-o societate care suportă repercusiunile economice şi sociale ale criminalităţii informatice, zilnic se face uz de calculatoare în aproape toate domeniile, de la controlul traficului aerian, feroviar şi circulaţia autobuzelor şi până la coordonarea serviciilor medicale şi securitatea naţională. Reţelele de telecomunicaţii permit efectuarea tranzacţiilor în regim real de timp, viteza de procesare a sporit considerabil, iar companiile sunt capabile să păstreze şi să prelucreze masive enorme de date. Cea mai măruntă dificultate în funcţionarea acestor sisteme poate pune în pericol mii de vieţi omeneşti, fapt care ne demonstrează incidenţa noilor tehnologii asupra fiinţei umane, pe de o parte, şi, pe de altă parte, dependenţa societăţii faţă de noile sisteme informatizate.

Generalizând cele menționate supra, menționăm că fenomenul criminalității informatice este unul aflat în continuă dezvoltare, se diversifică ca urmare a dezvoltării continue a tehnologiilor ce generează la rândul lor apariția de noi aplicații

și dispozitive, permițând infractorilor să-și remodeleze tehnicile de operare și să creeze noi oportunități de săvârșire a infracțiunilor informatice.

Consiliul Europei precizează că atacurile cibernetice și criminalitatea informatică sunt tot mai numeroase și mai sofisticate în întreaga Europă. Se preconizează că această tendință va continua să crească, date fiind previziunile conform cărora 22,3 miliarde de dispozitive la nivel mondial vor fi conectate la rețeaua Internet până în 2024.

Spațiul cibernetic va fi mereu animat de cursa continuă dintre atacatori și cei care sunt afectați de aceste atacuri. Din nefericire, așa cum precizează Agenția Europeană pentru Securitate Cibernetică (ENISA), în acest moment, infractorii cibernetici sunt cu un pas înainte.

Riscurile din spațiul cibernetic sunt direct proporționale cu gradul de informatizare a societății, iar combaterea fenomenului de criminalitate cibernetică trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi. Respectiv, în societatea digitalizată, unde amenințările la adresa securității cibernetice sunt în continuă creștere, protejarea datelor, infrastructurii, afacerilor, drepturilor omului, în special ale copiilor, este una dintre cele mai mari provocări cu care se confruntă atât cetățenii, cât și autoritățile.

Pornind de la creșterea rolului pe care îl au tehnologiile informaționale în domeniul securității statului, instituțiile abilitate întreprind și urmează să înreprindă în continuare acțiuni pentru asigurarea securității și administrării eficiente a sistemelor informaționale naționale, atât la nivel juridic, cât și la nivel functional, prin reducerea principalilor factori de risc, precum sunt: atacurile pe rețea (cyber-crimes), virușii informatici, vulnerabilitatea softurilor, neglijența sau rea-voința utilizatorilor, conectarea neautorizată a persoanelor terțe. La fel, prezența bazei legislative corespunzătoare în materia incriminării și combaterii infracțiunilor din domeniul informaticii reprezintă una din componentele de bază ale luptei eficiente cu aceste fapte socialmente periculoase. Or, imperfecțiunea legislației favorizează și înlesnește regenerarea și creșterea continuă a criminalității informatice.

Potrivit statisticii internaționale, un număr considerabil de atacuri informatice împotriva persoanelor fizice sau juridice rămân deseori nedeclarate, nedetectate sau nedescoperite, astfel, făptuitorii fiind încurajați să continue activitatea infracțională, inclusiv și datorită nesancționării la timp a ilegalităților săvârșite.

Cooperarea internațională joacă un rol din ce în ce mai important în consolidarea securității cibernetice, prin legislația, politicile și strategiile care necesită adaptare la contextul local.

Țările trebuie să găsească și să mențină o abordare coerentă a problemelor de securitate informațională, care ar presupune: facilitarea armonizării standardelor internaționale legate de securitatea cibernetică, sprijinirea statelor să definească strategii de securitate cibernetică și crearea de echipe de răspuns la incidente informatice, protecția online a copiilor, dezvoltarea capacității umane și promovarea dialogului politic.

Totodată, persoanelor fizice l-ar fi recomand să:

- investească în securitate, utilizarea de software licențiate și protecție antivirus eficientă pe toate dispozitivele;
- protejeze datele prin stocarea celor mai importante fișiere nu numai pe hard disk-ul sistemului informatic, ci și pe medii amovibile, hard disk-uri externe sau în stocarea în cloud și utilizând autentificarea cu doi factori acolo unde este posibil;
- utilizeze parole complexe constând din combinații nesemnificative de litere, cifre și semne, de cel puțin 8 caractere și schimbarea parolelor cel puțin o dată la șase luni;
- verifice atașamentele primite prin e-mail folosind software antivirus;
- prezinte maximă vigilență la site-urile accesate, îndeosebi când urmează a fi efectuate plați on-line, ș.a.

Conștientizarea securității cibernetice trebuie să devină o parte utilă a culturii organizaționale de zi cu zi. Astfel, în vederea consolidării culturii în domeniul securității cibernetice în contextul transformării digitale Consiliul Europei propune:

- investițiile în tehnologii, să fie corespunzătoare/să aibă ca bază și investiții în sisteme de securitate;
- dezvoltarea unui plan de eliminare a potențialelor amenințări care ar putea afecta securitatea cibernetică și stabilirea canalelor de comunicare internă clare între infrastructură (în cadrul instituțiilor/organizațiilor/companiilor);
- informarea și educarea populației privind implementarea măsurilor minime de protecție a sistemelor informaționale, inclusiv protecție on-line, prin desfășurarea măsurilor/campaniilor de informare privind amenințările și vulnerabilitățile generate de tehnologii, precum și familiarizarea cu mecanismele de raportare a incidentelor;
- desfășurarea de lecții/seminare/cursuri gratuite în instituții/organizații/companii în cadrul cărora să fie abordată securitatea cibernetică.

Doar cunoscând mai bine pericolele la care se expune, utilizatorul va analiza mai minuțios acțiunile. Consolidarea capacităților digitale trebuie să fie orientată pe nevoi și adaptată circumstanțelor individuale, naționale și în special să fie coordonată la nivel global.

Pentru redresarea situației atestate, sunt necesare dotarea cu echipamente și instrumente moderne, armonizarea cadrului normativ ce reglementează fenomenul criminalității informatice, inclusiv mediatizarea și sensibilizarea societății privind infracțiunile informatice şi celor conexe, comise prin utilizarea sistemelor informaționale și a mijloacelor tehnice moderne.

Reieșind din situațiile descrise, urmează ca populația să prezinte prudență și să evite neglijența în cazurile unde este posibil, în sesnsul prevenirii comiterii infracțiunilor săvârșite prin intermediul tehnologiilor informaționale, și astfel, cu siguranță vor avea de suferit mult mai puțini, iar numărul infracțiunilor nominalizate va descrește.

Ca măsură de prevenire a comiterii acestor infracțiuni ar servi aplicarea corectă de către instanțele judecătorești a pedepsei penale, care urmează a fi individualizată just în raport cu toate circumstanțele cauzei, cu persoana inculpatului și comportamentul acestuia, astfel ca sancțiunea să nu genereze dispreț față de ea, nici să nu fie insuficientă pentru corectarea infractorului și pentru prevenirea săvârșirii de noi infracțiuni.

Disproporționalitatea dintre gravitatea infracțiunii și pedeapsă ar trebui evitată, iar practica de aplicare a pedepselor ar trebui să fie supusă reevaluării critice pentru a evita o severitate nejustificată. În cazul în care o instanță judecătorească dorește să ia în considerare, ca circumstanțe agravante, unele aspecte care nu fac parte din definiția infracțiunii, trebuie să se asigure că circumstanța agravantă este probată dincolo de orice îndoială rezonabilă și, înainte ca o instanță judecătorească să refuze să țină cont de o circumstanță atenuantă, ar trebui să se asigure că circumstanța respectivă nu există.

Legea spune clar că, adoptând o soluție, aceasta trebuie să ducă la restabilirea echității sociale, să corecteze comportamentul condamnatului, iar pedeapsa să nu determine nici pe cel condamnat și nici pe altcineva din societate să mai comită din nou aceeași infracțiune.

Priopitatea națională de integritate europeană propulsează spre dezvoltarea conceptului unei justiții penale umanizate și racordate la înaltele standarde de responsabilizare și exigență profesională a organelor de ocrotire a normelor de drept care devin instituții-garanții ale statului de drept și protecție a individului.

Astfel, principiile enunțate de Convenția Europeană a Drepturilor Omului devin din ce în ce mai mult partea integrantă a metodologiei de lucru a judecătorului, procurorului și ofițerului de urmărire penală – fapt care duce ca sistemul penal din Republica Moldova să devină treptat unul care să răspundă cu adevărat necesităților societății.

Ca finalitate a procesului judiciar, o importanță primordială are calitatea actului de justiție – act ce va asigura autoritatea de lucru judecat. Calitatea actului de justiție are un impact nu numai asupra intereselor justiției, ce derivă din dreptul la un proces echitabil, dar și pentru garantarea nereluării arbitrare a urmăririi penale sau a judecării persoanei pentru aceeași faptă.

Dacă o eroare judiciară în alte materii poate fi reparată eventual prin despăgubire pecuniară, erorile procesului penal provoacă de cele mai multe ori consecințe iremediabile, fiind în joc soarta omului.

Drept urmare, efectuând o analiză obiectivă şi multiaspectuală a practicii judiciare cu privire examinarea cauzelor penale ce vizează infracțiunile comise prin intermediul tehnologiilor informaționale asupra sentințelor primelor instanțe din raza de activitate a Curţii de Apel Bălţi, se atestă respectarea normelor legale a Codului penal şi Codului de procedură penală a Republicii Moldova la emiterea soluțiilor de către instanțele nominalizate, însă se constată totuşi că în unele situații,

în cadrul judecării cauzelor și adoptării sentințelor pe caz, s-a atestat ne aplicarea corectă a actului amnistiei.

Instanțele de fond urmează să ţină cont de cele menţionate în prezenta notă informativă şi să examineze cauzele efectuând o vastă cercetare, multiaspectuală şi obiectivă a circumstanțelor cu verificarea tuturor aspectelor de drept ce au importanţă pentru justa soluţionare a spețelor penale, pentru adoptarea şi pronunţarea sentinţelor legale şi motivate, în scopul efectuării unei justiţii echitabile şi imparțiale.

Pentru a întruni obiectivul diminuării erorilor judiciare asemenea celor sus menţionate, spre pronunţarea unor hotărâri judecătoreşti legale şi întemeiate, şi în scopul unei practici judiciare uniforme, având în vedere rezultatele generalizării în cauză,

SE PROPUNE:

A se discuta nota informativă în cadrul şedinţei operative a Colegiului penal ale Curţii de Apel Bălţi.

A plasa prezenta notă informativă pe Pagina-Web a Curții de Apel Bălți.

Coordonator,
Judecător al Colegiului penal
al Curţii de Apel Bălţi **Oleg Moraru**

Executor, Specialist principal a
Direcţiei Sistematizare, Generalizare
a Practicii Judiciare şi Relaţii cu publicul **Alina Braga**