APROBAT

Preşedintele Curţii de Apel Bălţi

_____

Ion Talpa

Notă informativă

Generalizarea practicii judiciare cu privire la examinarea cauzelor penale comise prin intermediul tehnologiilor informaționale.

Conform planului de activitate a Colegiului Penal al Curţii de Apel Bălţi pentru anul 2021, ţinînd cont de importanţa şi actualitatea problemei legate de judecarea cauzelor penale comise prin intermediul tehnologiilor informaționale, **Direcţia sistematizare, generalizare a practicii judiciare şi relaţii cu publicul, a efectuat prezenta notă informativă, care cuprinde generalizarea practicii judiciare şi analiza datelor statistice cu privire la examinarea cauzelor penale comise prin intermediul tehnologiilor infromaționale, pentru perioada anului 2020.**

La tratarea tematicii nominalizate a fost studiată legislaţia naţională și internațională care reglementează respectiva problemă, şi anume:

1) Constituţia Republicii Moldova;
2) Constituţia Republicii Moldova; COMENTARIU, Editura ARC;
3) Codul Penal al Republicii Moldova Nr.985-XV din 18 aprilie 2002;
4) Codul penal al Republicii Moldova, COMENTARIU, cu modificările de pînă la 08 august 2003, Centrul de Drept al Avocaţilor, Chişinău 2003;
5) Codul de procedură penală al Republicii Moldova Nr.122-XV din 14 martie 2003;
6) 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”;
7) Convenţia Europenă pentru Apărarea Drepturilor Omului şi a Libertăţilor Fundamentale;
8) Legea R.M. privind prevenirea şi combaterea criminalităţii informatice nr. 20-XVI din 03.02.2009 Monitorul Oficial nr.11-12/17 din 26.01.2010.

Prezenta 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 asupra infracțiunilor comise prin intermediul tehnologiilor infromaționale, pe perioada anului 2020.

Aspecte generale asupra infracţiunilor comise prin intermediul tehnologiilor informaţionale.

Revoluţia Informaţiei din a doua jumătate a secolului al XX-lea a fost motorul care a dus societatea actuală la un progres nesperat. Înalta tehnologie a permis strîngerea unor cantităţi imense de date pe suporturi magnetice, aproape imposibil de perceput pentru simţul uman. Informaţia mereu a fost un atribut al puterii, cel ce o deţinea putea să conducă şi să supună. Ea fiind o istorie, o muncă intelectuală adunată şi cunoscută cu greu, trebuia şi era protejată pe parcursul anilor, uneori şi cu preţul vieţii, secolul XXI — fiind considerat „era informaticii".

Criminalitatea informatică reprezintă fenomenul social caracterizat prin comiterea infracţiunilor în domeniul informaticii. Din cauza diversităţii săvîrşirii lor, lipsei unei idei clare despre ceea ce constituie infracţiune în domeniul informaticii, precum şi din cauza inexistenţei unui termen unic ce ar caracteriza aceste fapte, în literatura de specialitate se întîlnesc următoarele noţiuni: infracţiune computerizată; infracţiune în domeniul comunicaţiei; ciberban-ditism; infracţiune informaţională; infracţiune în domeniul informaticii etc. Toate aceste noţiuni în esenţă caracterizează aceleaşi fapte, cu mici diferenţe stabilite de legislaţia penală a fiecărui stat.

Pentru prima dată noţiunea de infracţiune computerizată a fost întîlnită în legislaţia S.U.A., unde în anii '70 autorităţile au depistat o serie de încălcări comise în perioada anilor '50—'70 ai sec. XX. Primul infractor din Statele Unite ale Americii, care a comis o infracţiune prin intermediul MEC, a fost Alifonce Konfessore. În 1969, prin acţiunile sale, a prejudiciat statul cu 620.000, 00 USD şi a fost găsit vinovat de comiterea infracţiunii computerizate de către 20 de instanţe judecătoreşti.

Iniţial, orice infracţiune comisă prin intermediul MEC era calificată drept infrac- ţiune computerizată, astăzi deja făcîndu-se o diferenţiere dintre infracţiunile, unde MEC serveşte drept mijloc de comitere şi infracţiunile unde informaţia computerizată este obiectul atentării.

Deoarece anume în S.U.A. au avut loc primele progrese tehnologice în dezvoltarea tehnicii de calcul, această ţară a şi fost prima care s-a confruntat cu acest fenomen negativ nou. Organele de drept luptau cu acest fenomen, după metodele clasice, calificînd acţiunile drept furt, delapidarea averii străine, alte componenţe de infracţiuni. Însă timpul a demonstrat ineficienţa metodelor tradiţionale şi necesitatea elaborării unor metode noi şi adecvate fenomenului.

Astfel în 1973, Suedia a făcut primele modificări în legislaţie prin adoptarea legii privind răspunderea penală pentru modificarea neautorizată, distrugerea sau accesarea înscrisurilor de pe suporţii materiali informaţionali. Aceleaşi măsuri, în anul 1985, au fost întreprinse de S.U.A., M.B., Austria, Canada, Danemarca. Australia, Franţa şi Portugalia au urmat exemplul celorlalte state şi în 1992 au efectuat modificările respective.

După cum a fost reţinut, S.U.A. a fost prima ţară care s-a confruntat cu acest feno- men, dar după cum putem observa ea nu a fost prima care a reacţionat „legislativ". Noul fenomen criminogen înregistrat a trezit spaima autorităţilor de stat, sectorului bancar şi altor sectoare unde tehnica de calcul era un element indispensabil

pentru desfăşurarea activităţii lor, astfel în anii 70' a fost ridicată problema protecţiei juridice a informaţiei.

În 1977, Senatului S.U.A. i-a fost prezentat proiectul „legii cu privire la protecţia sistemelor federale de computere", însă actul respectiv a fost adoptat de Congres abia în 1984. Ulterior, după analiza mai amplă a problemei, precum şi după încercarea combaterii acestui fenomen, au fost efectuate careva modificări în legea dată şi astăzi ea este întîlnită sub denumirea de „Legea anului 1986 privind înşelăciunea şi abuzul, ce ţine de computer". În 1985 deja 47 de state din S.U.A. au adoptat astfel de legi. Statul Florida a fost cel care a adoptat una din cele mai reuşite legi în domeniu, după cum a demonstrat practica, - „legea cu privire la infracţiunile computerizate". Conform acestui act normativ, categoria dată de infracţiuni poate fi divizată în 3 grupe: infracţiuni contra proprietăţii intelectuale, care include efectuarea inten- ţionată şi ilegală a modificărilor, distrugerea sau furtul de date, programe şi documente ce ţin de computer; infracţiuni ce prejudiciază utilajul computerului, care duc la distrugerea sau deteriorarea sistemelor computerizate, indicatoarelor, etc.; infracţiuni, ce atentează la utilizatorii computerului, orice folosire neautorizată a computerului străin, precum şi tentativa de a prelucra careva date, îngrădirea accesului utilizatorului legal la computerul său.

Modificări radicale în legislaţia penală au fost efectuate şi în Germania, unde la mijlocul anilor 70' s-a pus problema despre necesitatea şi raţionalitatea elaborării normelor legale pentru încriminarea acţiunilor infracţionale săvîrşite prin intermediul MEC. Dezbaterile pe marginea problemei date s-au finisat cu adoptarea, de către Bunderstag, a legii a doua la număr, privind combaterea infracţiunilor economice, care a introdus în Codul Penal al R.F.G. 8 paragrafe noi ce conţineau descrierea infracţiunilor computerizate.

Codul Penal al Franţei, în 1992, a completat sistemul infracţiunilor contra patri- moniului, cu un capitol nou „privind atentarea la sistemele automatizate de prelucrare a datelor", unde se prevedea răspunderea pentru: accesul neautorizat la întregul sau la o parte din sistemul automatizat de prelucrare a datelor; împiedicarea sau încălcarea funcţionării corecte a unui astfel de sistem, precum şi introducerea pe calea înşelăciunii a informaţiei, distrugerea sau modificarea bazei de date.

Urmează a fi menţionat şi rolul Consiliului Europei, care a elaborat o serie de Convenţii ce urmează să stabilească criterii unice de delimitare a infracţiunilor in- formaţionale de alte categorii de infracţiuni, în care sunt indicate măsurile ce trebuie întreprinse de state pentru combaterea comiterii lor, astfel îndemnînd statele la aducerea în conformitate cu necesităţile sociale noi formate a legislaţiei. Astfel de convenţii sunt: „Convenţia pentru Protecţia Particularilor privind Procesarea Automatizată a Informaţiei Personale" din 1981; Budapesta, 23 noiembrie 2001, „Convenţia Europeană cu privire la criminalitatea informatică" precum şi o serie de Recomandări.

Din cele relatate mai sus se conchide că, criminalitatea informatică s-a dezvoltat odată cu progresul ştiinţific. Potenţialul distrugător al acestui fenomen fiind unul enorm. Unii analişti ruşi, precum Сервин И.А., a considerat că terenul dezvoltării şi răspîndirii fenomenului dat reprezintă doar statele cu o industrie bine

dezvoltată. Trebuie să reamintim că specificul criminalităţii informatice este lipsa unor hotare, mobilitatea cu care ea se săvîrşeşte, lipsa necesităţii deplasării pentru comiterea ei şi mulţi alţi factori.

Acest fenomen loveşte ferm şi provoacă daune considerabile în statele unde:

1) lipsesc organe specializate în acest domeniu;
2) lipseşte baza juridico-penală pentru încriminarea acestor acţiuni;
3) nivelul slab de informatizare despre urmările acestui fenomen;
4) existenţa unor lacune în legislaţie;
5) factor important este existenţa unei reţele informaţionale la nivel naţional.

O primă noţiune dată faptelor penale de natură informatică de către grupul de experţi ai OECD în 1983 este: ”Orice comportament ilegal, neetic sau neautorizat ce priveşte un tratament automat al datelor şi/sau o transmitere de date.” Această definiţie, deşi formulată în urmă cu două decenii, îşi dovedeşte utilitatea în primul rând prin faptul că permite integrarea dezvoltărilor ulterioare ale tehnicii în domeniul informatic.

În prezent funcţionează alte două definiţii. Astfel, prin infracţiune informatică în sens larg se înţelege: *”Orice infracţiune în care un calculator sau o reţea de calculatoare este obiectul unei infracţiuni, sau în care un calculator sau o reţea de calculatoarea este instrumentul sau mediul de înfăptuire a unei infracţiuni.”* Prin infracţiune informatică în sens restrâns se înţelege: ”*Orice infracţiune în care făptuitorul interferează, fără autorizare, cu procesele de prelucrare automată a datelor.”*

Republica Moldova a întreprins o serie de măsuri în prevenirea şi combaterea criminalităţii informaţionale. Cel mai însemnat eveniment reprezentându-l cu siguranţă semnarea Convenţiei de la Budapesta din 2001, care a avut loc la 23 noiembrie 2001 şi care a fost ratificată prin Legea nr. 6 din 02.02.2009. Convenţia a intrat în vigoare pentru Republica Moldova la 01.09.2009.

De fapt, îndată după ratificarea Convenţiei de la Budapesta, a fost adoptată Legea Nr. 20 din 03.02.2009 privind prevenirea şi combaterea criminalităţii informatice, care reglementează raporturile juridice privind prevenirea şi combaterea infracţiunilor informatice:

a) cadrul de asistenţă mutuală în prevenirea şi combaterea criminalităţii informatice, în protecţia şi acordarea de ajutor furnizorilor de servicii şi utilizatorilor de sisteme informatice;
b) colaborarea autorităţilor administraţiei publice cu organizaţii neguvernamentale şi cu alţi reprezentanţi ai societăţii civile în activitatea de prevenire şi de combatere a criminalităţii informatice;
c) cooperarea cu alte state, cu organizaţii internaţionale şi regionale avînd competenţe în domeniu.

Reglementarea infracțiunilor informatice în legislația națională a venit ca o adaptare firească a legislației la realități ce nu puteau fi ignorate.

Astfel, în Codul penal al Republicii Moldova, adoptat prin Legea nr. 985 din 18.04.2002, în vigoare din 12.06.2003 în premieră a fost introdus capitolul ”*Infracțiuni informatice și Infracțiuni în domeniul telecomunicațiilor*”, care cuprindea

inițial trei articole: art. 259 – Accesul ilegal la informația computerizată; art. 260 – Producerea, importul, comercializarea sau punerea ilegală la dispoziție a mijloacelor tehnice sau produselor program și art. 261 – Încălcarea regulilor de securitate a sistemului informatic.

După ratificarea Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23.11.2001, prin Legea nr. 6 din 02.02.2009, Codul penal al R.Moldova, fiind armonizat în conformitate cu prevederile Convenției prin Legea nr.278 din 18.12.2008, ambele publicate în M.O. la 20.02.2009, a fost suplinit cu articole noi 260^1-260^6, care prevedeau noi tipuri de infracțiuni cum ar fi interceptarea ilegală a unei transmisii de date, perturbarea funcționării sistemului informatic, falsul informatic, frauda informatică, etc.

Astfel, Codul Penal al Republicii Moldova la moment reglementează următoarele categorii de crime informaţionale ce constituie 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).

Un studiu realizat de FBI zugrăveşte gravitatea crimelor informatice prin faptul că circa 69 % din cei interogaţi sunt mult mai îngrijoraţi de atacurile informatice decît de furturi sau fraude obişnuite. Cercetările criminologice asupra infracţiunilor realizate prin sistemele informatice se află încă în la o etapă fragilă.

Este de menţionat faptul că doar o mică parte din faptele penale legate de utilizarea sistemelor informatice ajung la cunoştinţa organelor de cercetare penală, fiindcă este dificil de monitorizat infracţiunile informatice. Chiar şi dacă este posibil să se efectueze o descriere certă a tipurilor de fapte penale în domeniul sistemului informatic, este foarte dificilă prezentarea unei sinteze asupra întinderii pierderilor cauzate de acestea, precum şi a numărului real de infracţiuni comise. Numărul cazurilor de infracţiuni informatice este în continuă creştere. O companie independentă de sondaje GO-Gulf arată că în anul 2013 s-au înregistrat circa 2,402,722 de crime informatice în Rusia; 907,102 in Taiwan; 780,425 în Germania; 566,531 în Ucraina etc. Cu referire la prejudiciile cauzate de crimele informatice, un sondaj efectuat Internet Crime Complaint Center (IC3) şi Federal Bureau of Investigation (FBI) în 2013 indica pierderi de circa 781 de milioane dolari SUA din cauza crimelor cibernetice, în 2001 fiind doar 17 milioane dolari SUA.

Conform Global Security Map, Moldova se clasează pe locul 9 dintre alte 219 state în dependenţă de indicele de gravitate a securităţii în domeniul informatic, pe o scară de la 0 la 1000 Republica Moldova obţine 225.5.

Potrivit studiului Business Software Alliance din 2013 cu privire la pirateria software pentru computere personale, Republica Moldova face parte din grupul de state cu cea mai mare rată a pirateriei. Se constată că, ponderea produselor program ilegale din totalul software-ului utilizat este de 91%, ceea ce constituie, în opinia BSA, 57 milioane de dolari SUA, şi, totodată, cel puţin 140 milioane de lei venit naţional (reieşind din achitarea TVA şi a taxelor de import).

Cea mai răsunătoare crimă informatică începând cu anul 2011, a fost atunci când cinci persoane suspecte au comercializat prin reţeaua Internet, softul maliţios „CITADEL", destinat infectării sistemelor informatice şi culegerii datelor despre conturile bancare şi a datelor cu caracter personal, infectând peste 5 milioane de computere la nivel mondial, astfel cauzându-le instituţiilor financiare din SUA şi Europa daune materiale, estimate la mai bine de 10 milioane USD.

Un alt caz a fost în sectorul bancar, atunci când în decursul anului 2013, persoanele au favorizat suplinirea conturilor numerelor de telefon ale operatorilor de telefonie mobilă din Republica Moldova la un preţ redus, şi anume, în valoare de 50-70% din valoarea tranzacţiei, favorizând procurarea echipamentelor GSM, a sistemelor informatice, precum şi altor mijloace electronice la preţ redus, de pe unele website-uri care prestează servicii de vînzări on-line, utilizând la efectuarea acestor tranzacţii, datele cardurilor bancare străine, fără ştirea şi acordul titularilor, efectuând operaţiuni de plată online în suma de peste 250 mii lei moldoveneşti.

Trăsăturile caracteristice ale infracţiunilor din domeniul infromatic.

Infracțiunile din domeniul informatic prevăzute în Capitolul XI „*Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor*" din Partea Specială a Codului penal, sunt mult mai complexe decât ceea ce apare la prima vedere, de aceea în cele ce urmează li se va face o generalizare a trăsăturilor comune și distincte.

Astfel, obiectul juridic al infracţiunilor visate din domeniul informațional, prevăzute la art. 259 CP este format din:

- *obiectul juridic principal*, ce rezultă din relaţiile sociale cu privire la accesul legal la informaţia computerizată;

- *obiectul juridic secundar,* care reprezentă relaţiile sociale cu privire la intervenţia legală în sistemul informaţional.

În cazul infracțiunilor prevăzute la art.art.260-261 Cod penal, obiectul juridic special simplu se referă la relațiile sociale cu privire la:

- circulaţia legală a mijloacelor tehnice sau produselor program (art.260 CP);

- legalitatea interceptării unei transmisii de date informatice care nu sunt publice (art.260^1 CP);

- integritatea, accesibilitatea şi circulaţia în condiţii de legalitate a datelor informatice (art. 260^2 CP;

- buna funcţionare a unui sistem informatic sub aspectul inviolabilităţii domiciliului informatic (art. 260^3 CP);

- încrederea în datele informatice care permit accesul la un sistem informatic, în sensul utilizării corecte şi legale a acestora, precum şi în desfăşurarea corectă şi legală a operaţiunilor comerciale în legătură cu acestea (art.260 [4] CP);

- încrederea publică în siguranţa şi fiabilitatea sistemelor informatice, în valabilitatea şi autenticitatea datelor informatice, a întregului proces modern de prelucrare, stocare şi tranzacţionare automată a datelor de interes oficial sau privat (art.260 [5] CP);

- integritatea patrimoniului unei persoane, atunci cînd prezenţa respectivei persoane în spaţiul cibernetic se cuantifică într-un anumit volum de date stocate într-un sistem informatic sau vehiculate într-o reţea (art. 260 [6] CP);

- securitatea sistemului informatic (art. 261 CP).

Tot odată, obiectul material sau imaterial al infracţiunii îl reprezintă:

- informaţia computerizată a calculatoarelor, sistemului informatic sau reţelei informatice (art.259 CP);

- informaţia protejată de lege (lit. g) alin. (2) art. 259 CP);

- mijloacele tehnice sau produsele program, concepute sau adaptate, în scopul săvîrşirii uneia dintre infracţiunile prevăzute la art. art. 237, 259, 260[1]-260[3], 260[5]; 260 [6] CP;

- 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] CP RM);

- datele informatice dintr-un sistem informatic, dintr-un mijloc de stocare sau cu acces limitat (art.260 [2] CP);

- datele informatice (art.260[2], 260[5] şi 260[6] CP);

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

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

În contextul dat ține de menționat, că datele informatice necorespunzătoare adevărului reprezintă produsul infracţiunii incriminate la art.260 [5] CP.

În calitate de victime ale infracțiunilor supuse cercetării sunt persoanele care întrunesc următoarele caracteristici:

- proprietar sau alt posesor al informaţiei computerizate, calculatorului, sistemului informatic sau reţelei informatice accesate ilegal (art.259 CP RM);

- persoană fizică sau juridică posesoare a mijloacelor tehnice sau a produselor program care au fost în mod fraudulos utilizate pentru a permite accesul într-un sistem informatic (art.260 CP RM);

- persoană fizică sau juridică care este posesorul datelor informatice interceptate (art.260[1]CP RM);

- persoană fizică sau juridică care posedă datele informatice ce constituie obiectul imaterial al infracţiunii (art.260[2]CP RM);

- persoană fizică sau juridică posesoare a sistemului informatic, a cărui funcţionare este perturbată (art.260[3]CP RM);

- persoană fizică sau juridică posesoare a parolelor, codurilor de acces sau a altor asemenea date informatice care au fost în mod fraudulos utilizate pentru a permite accesul într-un sistem informatic (art.260^4CP RM);

- persoană fizică sau juridică prejudiciată în propriile interese şi faţă de care se produc consecinţe juridice (de ordin patrimonial, moral ori social) în urma contrafacerii datelor informatice (art.260^5 CP RM);

- persoană al cărei interes patrimonial a fost prejudiciat prin acţiunea făptuitorului (art.260^6 CP RM);

- proprietar sau alt posesor al resurselor sau al sistemelor informaţionale, al tehnologiilor şi mijloacelor de asigurare a acestora; proprietar sau alt posesor al informaţiei computerizate art.261 CP RM).

Potrivit literaturii de specialitate, latura obiectivă a infracţiunilor informatice se caracterizează prin fapta prejudiciabilă ce poate fi comisă prin acţiune în cazul componențelor prevăzute la art. 259, 260, 260^1-260^6 sau inacţiune, în cazul componențelor prevăzute la art. 261; latura obiectivă fiind una materială la componențele art.259, 260^2-260^6, 261 CP RM) sau formală, în cazul celor prevăzute la art. art. 260; 260^1 CP.

În contextul unor infracțiuni din domeniul informatic ca semn facultativ ale laturii obiective devin obligatorii următoarele mijloacele de săvârşire a infracţiunii:

- mijloacele tehnice speciale: lit. e) alin. (2) art.259 şi lit. d) alin.(2) art. 261^1 CP;

- calculatorul, sistemul informatic sau reţeaua informatică: lit. f) alin. (2) art. 259 CP.

Latura subiectivă a infracțiunilor informatice caracterizându-se prin:

- intenţie, la art.259, 260, 260^1-260^6 CP;

- intenţie sau imprudenţă în raport cu fapta prejudiciabilă şi numai imprudenţă în raport cu urmările prejudiciabile survenite la art. 261 CP.

În componența infracțiunilor prevăzute de lit. f) alin. (2) art. art. 259; 260; 260^4- 260^6 CP, 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; $260^{6;;}$ lit. f) alin. (2) art. 259 CP RM);

- scopul săvârşirii uneia dintre infracţiunile specificate la art. art. 259, 260^1-260^3, 260^5; 260^6 ; 260; 260^4 CP;

- scopul de utilizare a datelor necorespunzătoare adevărului în vederea producerii unei consecinţe juridice - art.260^5 CP);

- scopul de a obţine un beneficiu material - art. 260^6 CP.

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

Subiectul infracţiunilor din domeniul informatic fiind persoana fizică responsabilă care la momentul comiterii faptei a atins vârsta de 16 ani în cazul componențelor art.259, 260^1-260^6, 261 CP sau de 14 ani în cazul celor prevăzute de

art. 260 CP; subiectul special la art.259, 260, 260^1, 260^3, 260^4, 261 CP fiind persoana juridică (cu excepţia autorităţii publice).

În ce privește subiectul componenței art. 259 CP, acesta deține 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. Iar, persoana în ale cărei obligaţii intră respectarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic este subiectul special al infracţiunii prevăzute la art.261 CP RM.

Tipurile infracţiunilor din domeniul informatic.

Orice clasificare este condiționată, iar scopul său este de a facilita tratarea infracțiunilor în cauză, dar nu mai mult. Clasificarea este un instrument natural pentru cunoașterea realității obiective, o sursă specială de cunoaștere a acesteia, o tehnică prin care setul de fenomene observate este împărțit în grupuri principale, clase, tipuri care fac parte dintr-un sistem comun și constituie un singur întreg. În procesul de clasificare, fiecare obiect studiat primește un anumit grad (rating). De aceea, cercetătorii se confruntă, mai devreme sau mai târziu, cu nevoia de a clasifica anumite fenomene ale vieții sociale.

Conţinutul noţiunii de infracțiune din domeniul informatic, cum a fost menționat și în unitatea de conținut anterioară, este deosebit de variat, abordarea căruia este diferită din perspectivele viziunilor doctrinare, determinând și o clasificare (tipologia) diferită a acestor infrațiuni.

Astfel, în raportul Comitetului European pentru probleme criminale, infracţiunile informatice sunt sistematizate în următoarele categorii: infracţiunea de fraudă informatică; infracţiunea de fals în informatică; infracţiunea de prejudiciere a datelor sau programelor informatice; infracţiunea de sabotaj informatic; infracţiunea de acces neautorizat la un calculator; infracţiunea de interceptare neautorizată; infracţiunea de reproducere neautorizată a unui program informatic protejat de lege; infracţiunea de reproducere neautorizată a unei topografii; infracţiunea de alterare fără drept a datelor sau programelor informatice; infracţiunea de spionaj informatic; infracţiunea de utilizare neautorizată a unui calculator; infracţiunea de utilizare neautorizată a unui program informatic protejat de lege.

Manualul Naţiunilor Unite pentru prevenirea şi controlul infracţionalităţii informatice sintetizează 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.

În studiul "Aspectele legale ale infracţionalităţii informatice în cadrul societăţii informaţionale", realizat pentru Comisia Europeană de către prof. dr. Ulrich Sieber, de la Universitatea din Wurzburg, Germania, sunt prezentate următoarele categorii şi sub-categorii de infracţiuni informatice:

- atingeri aduse dreptului la viaţa privată;

infracţiuni cu caracter economic:

- penetrarea sistemelor informatice în scopul depăşirii dificultăţilor tehnice de securitate (“hacking”);
- spionajul informatic;
- pirateria programelor pentru calculator;
- sabotajul informatic;
- frauda informatică;
- distribuirea de informaţii cu caracter ilegal sau prejudiciabil (propagandă rasistă, difuzare de materiale pornografice, etc.);

alte infracţiuni:

- infracţiuni contra vieţii;
- infracţiuni legate de crima organizată;
- război electronic.

În doctrina românească unii autori disting categoriile de infracţiuni cibernetice în conformitate cu prevederile Legii penale speciale nr.161/2003 după cum urmează:

1. Infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice:

- infracţiunea de acces ilegal la un sistem informatic;
- infracţiunea de interceptare ilegală a unei transmisii de date informatice;
- infracţiunea de alterare a integrităţii datelor informatice;
- infracţiunea de perturbare a funcţionării sistemelor informatice;
- infracţiunea de a realiza operaţiuni ilegale cu dispozitive sau programe informatice.

2. Infracţiuni informatice:

- infracţiunea de fals informatic;
- infracţiunea de fraudă informatică.

3. Pornografia infantilă prin intermediul sistemelor informatice:

Alții, pentru clasificarea infracţiunilor informatice utilizează criteriul rolului avut de sistemele informatice în comiterea infracţiunii. Din această perspectivă, infracţiunile informatice se clasifică în:

- infracţiuni săvîrşite cu ajutorul sistemelor informatice, în care sistemele informatice constituie un instrument de facilitare a comiterii unor infracţiuni. Este vorba de infracţiuni “tradiţionale” perfecţionate prin utilizarea sistemelor informatice; şi
- infracţiuni săvîrşite prin intermediul sistemelor informatice, în care sistemele informatice, incluzînd şi datele stocate în acestea, constituie ţinta infracţiunii. Aceste infracţiuni pot fi săvarşite doar prin intermediul sistemelor informatice. Ele au făcut obiect de reglementare în ultimii ani.

În dependență de atitudinea făptuitorului față de infracțiunea comisă, in concreto, de motivul care îl determină pe acesta, se distinge următoarea clasificare: 1) săvîrșită din motive egoiste: săvârșită din răzbunare; din interes material; comise de intenții huliganice; terorismul; 2) neintenționat: săvârșită din curiozitate; în scop de auto-afirmare.

De asemnea, se distinge și tipologia infracțiunilor din domeniul informatic stipulate în Convenţia Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001, și anume:

- Infracțiuni împotriva confidențialității, integrității și disponibilității unui sistem computerizat sau datelor în format electronic: accesul ilegal; interceptarea ilegală; modificarea datelor; accesul neautorizat într-un sistem computerizat; utilizarea metodelor ilicite.
- Infracțiuni în domeniul sistemelor computerizate: falsuri în domeniul sistemelor computerizate; fraude în domeniul sistemelor computerizate.
- Infracțiuni legate de conținutul datelor în format electronic: infracțiuni legate de pornografia infantilă.
-Infracțiuni legate de încălcarea drepturilor de proprietate intelectuală și a drepturilor conexe.

În cele din urmă, făcând o retrospectivă a clasificărilor propuse supra și prin corelație cu prevederile Codului penal al Republicii Moldova, putem stabili două tipuri ale infracţiunilor din domeniul informatic:

1) infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice (prevăzute la art.259, 260, 260 [1]-260 [4], 261 CP RM);

2) infracţiuni informatice în accepţiune strictă (prevăzute la art.260 [5]şi 260 [6] CP RM).

Analiza statisticii judiciare cu privire la examinarea cauzelor penale privind infracțiunile comise prin intermediul tehnologiilor informaționale.

În perioada anului 2020 în procedura Curții de Apel Bălți s-au aflat 7 cauze penale în ordine de apel privind infracțiunile comise prin intermediul tehnologiilor informaționale, dintre care au fost examinate 5 cauze, 2 cauze au rămas în rest pentru perioada anului 2021. Rezultatele generalizării privitoare la acest compartiment relevă, că din cele 5 cauze examinate, 2 cauze au rămas fără modificări, în alte 3 cauze fiind adoptate hotărâri noi.

Datele privind examinarea cauzelor penale privind infracțiunile comise prin intermediul tehnologiilor informaționale de către judecătorii Colegiului penal al Curții de Apel Bălți, sunt următoarele:

1. **Gh. Scutelnic** - 1cauză aflată în procedură, 1 cauză examinată, hotărîre nouă – 1 cauză.
2. **O. Moraru** - 1 cauză aflată în procedură, 1 cauză examinată, hotărîre nouă - 1 cauză.
3. **A.Revenco -** 1 cauză aflată în procedură,1 cauză examinată, hotărîre nouă - 1 cauză.
4. **Gh. Liulca** - 1 cauză aflate în procedură, 1 cauză examinată, fără modificări - 1 cauză.
5. **E. Rățoi -** 1 cauză aflate în procedură, 1 cauză examinată, fără modificări - -1 cauză

6. **A. Rotaru** - 1 cauză aflată în procedură, 1 cauză rest.
7. **R.Burdeniuc** - 1 cauză aflată în procedură, 1 cauză rest.

În procedura judecătorilor Colegiului penal al Curții de Apel Bălți: I.Talpa, O.Mironov, S.Șleahtiţki, D.Pușca, V.Pușcaș nu au fost înregistrate cauze penale privind infracțiunile comise prin intermediul tehnologiilor informaționale în perioada anului 2020.

Examinarea cauzelor penale privind infracțiunile comise prin intermediul tehnologiilor informaționale de către Judecătoriile din circumscripția Curții de Apel Bălți.

1. ***Judecătoria Bălţi sediul Central***: total cauze aflate în procedură - 4; 3 cauze examinate, 1cauză - fără modificări; 2 cauze - hotărîri noi, 1 cauză – rest.
2. ***Judecătoria Bălţi sediul Sîngerei***: total cauze aflate în procedură -1; rest -1 cauză.
3. ***Judecătoria Drochia sediul Central***: total cauze aflate în procedură -1; 1cauză examinată; 1 cauză - hotărîre nouă.
4. ***Judecătoria Soroca sediul Central*** : total cauze aflate în procedură -1; 1cauză examinată; 1 cauză - fără modificări.

PRACTICA JUDICIARĂ

Ca urmare a analizei şi studierii deciziilor adoptate şi pronunţate de către Colegiile penale ale 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 latura pedepsei penale pe motivul ***blândeții ei*** **în** raport cu caracterul și gradul prejudiciabil al faptei comise și urmările survenite, acordându-se insuficientă relevanță prevederilor art. 61 CP ce se referă la scopul pedepsei penale, precum și celor de la art. 75 CP referitor la criteriilor generale de individualizarea ei.

Astfel, prin sentința judecătoriei xxx, sediul xxx din 23 aprilie 2018, adoptată în ordinea art. 364/1 alin. (8) Cod pr. penală, XXX a fost condamnată pentru, că acționând cu intenţie directă unică în scopul răspândirii cu bună-ştiinţă a informaţiilor ocrotite de lege despre viaţa personală ce constituie secret personal al altei persoane, fără consimţământul ei, prin mass-media, în perioada lunilor mai-iunie 2017, ilegal a cules informaţia ce constituie secret personal a minorei xxxx , şi cu bună-ştiinţă, fără consimţământul ultimei, deținînd în formă electronică imagini sexuale reale şi simulate cu reprezentarea organelor sexuale ale minorei date, reprezentată de maniera lascivă şi obscenă, le-a răspîndit în massmedia prin intermediul reţelei de socializare „xxxxx" grupa „xxxxx".

Tot ea, acționînd cu intenţie directă unică în scopul distribuirii de imagini sexuale reale şi simulate cu reprezentarea organelor sexuale ale unui copil, reprezentată de maniera lascivă şi obscenă, inclusiv în formă electronică, pe parcursul lunilor mai-iunie 2017, cu bună-ştiinţă fără consimțământul minorei xxxx, deținînd în formă electronică imagini sexuale reale şi simulate cu reprezentarea organelor sexuale ale victimei, le-a răspîndit în massmedia prin intermediul reţelei de socializare „xxxxx ” grupa „xxxxx.”.

Tot ea, acționînd cu o intenţie unică şi urmărind scopul de profit, amenințînd-o pe minora xxxx, cu răspîndirea unor ştiri defăimătoare, prin intermediul sms-urilor de pe telefonul său mobil cu nr.xxxx şi a unei pagini WEB de pe reţeaua de socializare „xxxx” cu denumirea „ xxxx”, pe reţeaua de socializare „xxxx ”, a cerut şi primit de la xxxx bani în sumă totală de 500 lei, fiindu-i stabilită pedeapsa, după cum urmează:

- art. 177 alin. (2) lit. a) Cod penal, amendă în mărime de 413 unităţi convenţionale, echivalentul a 20 650 lei;
- art. 208[1] Cod penal - un an închisoare;
- art.189 alin. (3) lit. e) Cod penal - 4 ani 5 luni 10 zile închisoare cu amendă în mărime de 1 175 unităţi convenţionale, echivalentul a 58 750 lei.

Potrivit art. 84 alin. (1) Cod penal, pentru concurs de infracţiuni, prin cumul parţial al pedepselor aplicate, s-a stabilit pedeapsa definitivă de 5 (cinci) ani închisoare, cu amendă în mărime de 1 200 unităţi convenţionale, echivalentul a 60 000 lei, cu executare în penitenciar pentru femei de tip semiînchis, dispunându-se prin aplicarea prevederilor art.90 Cod penal, suspendarea condiționată a executării pedepsei închisorii pentru perioada de probaţiune de 4 (patru) ani.

Prin decizia Colegiului penal al Curții de Apel Bălți din 31 octombrie 2018 ce a soluționat cauza în ordine de apel, s-a admis apelul procurorului în Procuratura xxxx, xxxx, cu casarea sentinței din 23 aprilie 2018 în latura pedepsei penale și pronunţată o nouă hotărâre potrivit modului stabilit pentru prima instanţă, după cum urmează:

- art. 177 alin. (2) lit. a) Cod penal, coroborat cu art. 70 alin. (3^1) Cod penal și art.364 [1] alin. (8) Cod de procedură penală, la amendă în mărime de 500 unităţi convenţionale;
- art. 189 alin. (3) lit. e) Cod penal, coroborat cu art. 70 alin. (3^1) Cod penal și art.364 [1] alin.(8) Cod de procedură penală, la 4 (patru) ani 5 (cinci) luni 10 (zece) zile închisoare, cu amendă în mărime de 1 388 unităţi convenţionale;
- art. 208 [1] Cod penal, coroborat cu art.70 alin.(3^1) Cod penal și art. 364^1 alin. (8) Cod de procedură penală, la 1 (unu) an închisoare;

Pentru concurs de infracțiuni, prin aplicarea prevederilor art. 84 alin.(1) Cod penal, s-a stabilit pedeapsa de 5 (cinci) ani închisoare, cu amendă în mărime de 1400 unităţi convenţionale, echivalentul a 70 000 lei, cu executarea pedepsei închisorii în penitenciar pentru femei de tip semiînchis.

Respectiva decizie a fost casată de către CP al CSJ din 16 iulie 2019, cu remiterea cauzei la rejudecare în ce privește pedeapsa penală.

Prin decizia CP al CAB din 10.09.2020 s-a aplicat pedeapsa în aceleași limite ca și în precedenta decizie din 31.10.2018, doar că prin aplicarea art. 90 Cod penal

s-a dispus suspendarea condiţionată a executării pedepsei sub formă de închisoare pentru perioada de probațiune 4 (patru) ani, dacă în termenul de probă nu va săvîrși o nouă infracțiune și prin comportare exemplară și muncă cinstită va îndreptăți încrederea ce i-a fost acordată.

În motivarea soluției adoptate, Colegiul penal a reținut, că la examinarea cauzei penale s-a dat deplină eficiență art.93-101, art.26-27 Cod de procedură penală, fiind apreciate probele din punct de vedere al pertinenţei, concludenţei, utilităţii şi veridicităţii lor, iar toate în ansamblu din punct de vedere al coroborării lor, corect ajungîndu-se la concluzia privind încadrarea juridică a faptelor și vinovăția lui XXX în comiterea infracțiunilor prevăzute de art. 177 alin.(2) lit.a), art. 208 [1] și art. 189 alin.(3) lit.e) Cod penal. Mai mult ca atît, cauza penală a fost examinată în baza art.364 [1] Cod de procedură penală, în cadrul căreia inculpata a depus o cerere de examinare în procedura simplificată, prin care a recunoscut vina, a fost de acord cu învinuirea formulată în rechizitoriu și a acceptat toate probele administrate la urmărirea penală, care a fost acceptată de instanța de fond.

Prin urmare, instanța de apel reținând caracterul întemeiat al soluției judecătorești referitor la încadrarea juridică a faptelor penale și vinovăția inculpatei în comiterea infracțiunilor imputate, a constatat însă erori de drept material la aplicarea pedepsei penale, rezultate dintr-o interpretare și aplicare eronată a prevederilor art. 70 alin. (3^1) Cod penal, referitor la pedeapsa amenzii, deși acestea sunt aplicabile doar în cazul închisorii.

Respectiv, casând sentința în latura pedepsei penale, Colegiul a dispus aplicarea prevederilor art. 364 [1] alin. (8) Cod de procedură penală, stabilindu-i XXX pe art. 189 alin. (3) lit. e) Cod penal pedeapsa închisorii pe termen de 4 (patru) ani 5 (cinci) luni 10 (zece) zile, prin reducerea cu 1/3 a limitelor maximă și minimă a sancțiunii, prevăzute de legiuitor, precum și cu ¼ a amenzii, calculată în mărime de 1388 u.c..

La fel, Colegiul a stabilit, aplicarea incorectă de către instanța de fond, sub limita minimă, prevăzută de art. 64 alin. (3) Cod penal, a pedepsei amenzii pe art. 177 alin. (2) lit. a) Cod penal, fără a ține cont de faptul, că potrivit legiuitorului, *mărimea amenzii pentru persoanele fizice se stabileşte în limitele de la 500 la 3000 unităţi convenţionale (...) luîndu-se ca bază mărimea unităţii convenţionale la momentul săvîrşirii infracţiunii*.

Respectiv, în situația în care limitele amenzii pe art. 177 alin. (2) lit. a) Cod penal constituie de la 550 la 850 u. c., instanța nu putea aplica amendă sub limita de 500 u.c., ceea ce impune stabilirea ei în mărime de 500 u.c.

În contextul celor menționate, Colegiul, ținând cont de gravitatea infracţiunilor comise de XXX, de recunoașterea vinei, de căința sinceră, de acceptarea procedurii simplificate de examinare a cauzei penale, de caracteristica inculpatei, de vîrsta ei tînără, de prezența la întreținere a unui copil minor, de lipsa evidenței la medicul narcolog și psihiatru, modul și condiţiile acesteia de viaţă, conștientizarea faptelor săvîrșite, influenţa pedepsei asupra corectării şi reeducării ei, a conchis asupra suspendării condiționate a executării pedepsei cu închisoarea respingând solicitarea apărării referitor la aplicarea art. 96 Cod penal.

Atacată cu recurs, decizia instanței de apel a fost păstrată neschimbată prin decizia Colegiului penal al Curții Supreme de Justiție din 03 februarie 2021 ce a dispus inadmisibilitatea recursului.

În cadrul judecării cauzelor penale în ordine apel privind infracțiunile comise prin intermediul tehnologiilor informaționale, Colegiile penale au 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.

Astfel, prin sentința judecătoriei XXX sediul XXX din 28.12.2018 XXX și ZZZ au fost condamnați pentru faptul că, inculpatul XXX împreună cu ZZZ, în perioada de timp cuprinsă între 06.03.2018 și 14.03.2018, acționând prin înțelegere prealabilă și de comun acord, intenționat, având scopul accesului ilegal la rețelele și serviciile de telecomunicații ale companiei SA ”xxx”, în vederea obţinerii unui beneficiu material pentru sine și pentru altul, sub pretextul prestării serviciilor de ”Call Centru”, au fondat întreprinderea “xxxx” SRL, cu sediul în mun.xxx, str. xxx, al cărei administrator este ZZZ, utilizând fraudulos numărul ”111111” din numerotația de telefonie fixă ”1111111”, atribuită de către compania de telecomunicații SA ”xxxx”, au închiriat camera nr.x a imobilului situat pe str.xxxx din mun.xxxx, unde au instalat un sistem informatic de model ”Lenovo ideapad Z500”, interconectat la un dispozitiv ”Raspberry Pi” și router ”MikroTik”, având setate programe utilizate pentru generarea traficului voce în rețeaua de telefonie ca ”Asterisk” și ”PuTTY Configuration”, fiind conectați la rețeaua internet a furnizorului de servicii SA ”xxxxx”, prin intermediul IP adresei 93.116.45.87, au accesat neautorizat reţelele şi serviciile de telecomunicaţii ale companiei SA ”xxxx”, au restricţionat accesul la datele informaţionale internaţionale şi au efectuat terminaţii neautorizate ale traficului voce local şi internațional, generând ilegal 40687,9 minute, cauzând astfel companiei SA ”xxxx” daune în proporții mari în sumă de 183790,25 lei.

Tot el, XXX, împreună cu ZZZ, în vederea realizării intențiilor lor infracționale, acționînd prin înțelegere prealabilă și de comun acord, intenționat, urmărind scopul obţinerii unui beneficiu material pentru sine și pentru altul, sub pretextul prestării serviciilor de ”Call Centru”, au fondat întreprinderea “xxxx” SRL, cu sediul pe str.xxx, mun.xxxx, al cărei administrator esteZZZ, utilizând fraudulos numărul ”11111” din numerotația de telefonie fixă ”11111”, atribuită companiei date de către compania de telecomunicații SA ”xxxx”, au închiriat camera nr.xx a imobilului situat pe str.xxx din mun.xxxx, unde au instalat un sistem informatic de model ”Lenovo ideapad Z500”, interconectat la un dispozitiv ”Raspberry Pi” și router ”MikroTik”, având setate programe utilizate pentru generarea traficului voce în rețeaua de telefonie ca ”Asterisk” și ”PuTTY Configuration”, fiind conectați la rețeaua internet a furnizorului de servicii SA ”xxx”, prin intermediul IP adresei 93.116.45.87, au accesat neautorizat reţelele şi serviciile de telecomunicaţii ale companiei SA ”xxxx”, au restricţionat accesul la datele informaţionale internaţionale şi au efectuat terminaţii neautorizate ale traficului voce local şi internațional, împiedicând funcţionarea sistemelor informatice ale companiei SA

”xxxx”, au generat ilegal 40687,9 minute, cauzând astfel companiei SA ”xxxx” daune în proporţii mari în sumă de 183790,25 lei, fiindu-le stabilite pedeapsa după cum urmează:

- art. 260^6 alin. (1) CP, amendă în mărime de 1350 unităţi convenţionale pentru fiecare;
- art. 261^1 alin. (2) lit. b), d) CP, amendă în mărime de 1350 unităţi convenţionale pentru fiecare;
- în baza art. 84 alin. (1) CP, pentru concurs de infracţiuni, prin cumul parţial al pedepselor aplicate, l-i s-a stabilit definitiv pedeapsa de amendă în mărime de 1400 unităţi convenţionale, echivalentul a 70000 lei pentru fiecare.

Prin decizia Colegiului penal al Curții de Apel Bălți din 23.01.2020 apelul comun declarat de inculpaţii XXX şi ZZZ împotriva sentinței Judecătoriei xxx sediul xxx 28.12.2018 s-a respins ca nefondat, cu menținerea ei fără modificări.

Colegiul penal a reținut, că la examinarea cauzei s-a dat deplină eficiență prevederilor art. art. 26-27; 93-101, CPP**,** cauza a fost cercetată multe aspectual, în baza probelor acumulate just a fost reținută starea de fapt și de drept, corect ajungînd la concluzia privind vinovăţia inculpaţilor XXX şi XXX în baza art. 260^6 alin. (1) CP – *frauda informatică, adică restricţionarea accesului la date informatice şi împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, acţiuni care au cauzat daune în proporţii mari*, şi art. 261^1 alin. (2) lit. b), d) CP – *accesul neautorizat la reţelele şi serviciile de telecomunicaţii cu utilizarea reţelelor şi serviciilor de telecomunicaţii ale altor operatori, acţiuni ce au cauzat daune în proporţii mari, săvârşită de două persoane, cu folosirea mijloacelor tehnice special.*

Instanța de apel a notat, că temeinicia sentinței a fost verificată reieșind din argumentele aduse de către autorii apelului în raport cu materialul probant acumulat şi cu cadrul legal existent, iar la demersul părţii apărării, a fost reluată cercetarea judecătorească în scopul audierii inculpaţilor, reprezentantului părții vătămate, martorilor şi cercetarea suplimentară a probelor administrate conform regulilor generale prevăzute pentru prima instanţă, cît și a probelor scrise.

Fiind constatată vinovăția inculpaților, la stabilirea pedepsei ultimilor s-a ținut cont de prevederile art. 61 CP, la fel şi de criteriile generale de individualizare a pedepsei prevăzute de art.art. 7 şi 75 CP, pedeapsa stabilită lui XXX şi ZZZ a fost numită în limitele sancţiunilor prevăzute la articolele corespunzătoare din Codul penal, ajungîndu-se la conluzia, că corectarea şi reeducarea inculpaţilor este posibilă fără izolarea lor de societate, stabilindu-se o pedeapsă sub formă de amendă.

Atacată cu recurs, decizia instanței de apel a fost păstrată fără modificări prin decizia Colegiului penal al Curții Supreme de Justiție din 05 august 2020 ce a dispus inadmisibilitatea recursului.

Prin urmare a celor menționate, *sub aspectul legalităţii şi temeiniciei soluţiei instanței de fond asupra infracţiunilor comise prin intermediul tehnologiilor informaţionale*, Colegiul penal al Curții de Apel Bălți a reținut și sentința judecătoriei XXX sediul XXX din 22.11.2019 prin care ZZZ a fost condamnat pentru faptul că, în intervalul de timp, începând cu data de 26.01.2019 pînă la data de 28.01.2019, având

intenția de distribuire, folosire sau deţinere de imagini sau alte reprezentări ale unui sau mai mulţi copii implicaţi în activităţi sexuale explicite, reale sau simulate, ori de imagini sau alte reprezentări ale organelor sexuale ale unui copil, reprezentate de manieră lascivă sau obscenă, în formă electronică, utilizând sistemul informatic ”laptop de model ”Asus X552C” cu număr de serie ”DBNOCV244266463” cu dispozitiv de stocare a informației HDD de model ”WDC WD5000LPVX-22V0TT0” cu numărul de serie WXQ1E34LDLK7, cu capacitatea de 500 Gb și rețeaua internet cu IP adresa: 89.149.74.191, cu adresa conectării la domiciliul său situat în municipiul xxxx, strada xxx, nr.xx, ap.xxx, prin intermediul programei specializate pentru copierea și distribuirea fișierelor în internet ”eMule”, ce utilizează rețeaua ”ED2K” în baza principiului „de la egal la egal”, a distribuit 74 fișiere grafice și video cu conținut de pornografie infantilă, care conform bazei de date specializate în identificarea victimelor pornografiei infantile, abuzului și exploatării sexuale a copiilor „ICSE”, administrată de OIPC „Interpol”, reprezintă pornografie infantile, precum și a folosit și a deținut 3207 fișiere foto, dintre care cu valoarea hash MD: MA05A81269145CABCCF3D2127121E5EBD,8A50C752F6C43E2FE0AE1F7F8E07690,AD4CDB6ABD9A0F595FB60BEBF5F2C970,8454BC77049C99BAF194D261785DD2F5,E951E03845CF7E978F9E9B5C03905D73, care conform bazei internaționale de date „GRIDCOP”, reprezintă pornografie infantilă, fiindu-i stabilită pedeapsa în baza art.208 [1] CP la 8 luni închisoare, iar în baza art.90 CP, executarea acestei pedepse a fost suspendată condiționat pe o perioadă de probațiune de 1 an, în temeiul art. 65 alin. (3) CP, în privința lui ZZZ a fost aplicată pedeapsa complementară sub formă de privare de dreptul de a exercita activitate în domeniul tehnologiilor informaționale pe un termen de 3 ani.

Contestată cu apel, sentința primei instanțe a fost menținută fără modificări prin decizia Colegiului penal al Curții de Apel Bălți din 04.03.2020.

Astfel, Colegiul penal a reținut, că cauza a fost judecată în prima instanță în ordinea prevăzută de art. 364[1] CPP, în baza probelor administrate de către organul de urmărire penală, care au fost cercetate în ședința instanței de fond, asupra cărora inculpatul nu a obiectat și nu a solicitat administrarea unor probe noi, iar prin prisma probatoriului administrat instanța a stabilit ca fiind dovedită pe deplin vinovăția inculpatului ZZZ în comiterea infracțiunii prevăzute de art. 208[1] CP - *pornografia infantilă, adică distribuirea, folosirea, și 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 eletronică*.

Prin prisma criteriilor complementare ce vizează personalitatea inculpatului, gravitatea faptei comise, precum și reținând circumstanțele comiterii infracțiunii și comportamentul lui ZZZ după săvârșirea faptei, s-a conchis că corectarea lui ZZZ poate avea loc și fără privarea lui de libertate, stabilindu-i pedeapsa sub formă de închisoare cu suspendarea executării acesteia pe o perioadă de probațiune, totodată, în temeiul art.65 alin.(3) CP, aplicând și pedeapsa complementară rezultând din caracterul și specificul faptei infracționale comise.

În opinia instanței de apel, pedeapsa astfel cum a fost individualizată de către prima instanță răspunde atât principiului proporționalității, cât și scopului prevăzut în art.61 CP, cuantumul acesteia este dozată corespunzător, iar față de natura și gravitatea faptei comise, a circumstanțelor reale de săvârșirea acesteia, pedeapsa aplicată inculpatului este aptă să conducă la realizarea scopurilor sancțiunii.

Drept urmare, fiind verificată baza de date a hotărîrilor Colegiului penal al Curții Supreme de Justiție, nu s-a atestat contestarea cu recurs ordinar a deciziei Curții de Apel Bălți din 04.03.2020.

Concluzii:

Edificarea şi consolidarea statului de drept în Republica Moldova impune cu insistenţă crearea unui mecanism complex chemat să asigure libertatea individuală şi siguranţa persoanei.

Dreptul penal, prin reglementările sale, are în calitate de sarcină ocrotirea valorilor sociale importante în societate. Domeniul tehnologiilor informaţionale a devenit cu timpul un domeniu important pentru societate, astfel, că se înscrie în valorile sociale ocrotite de dreptul penal.

Actualmente, practic toate legislaţiile penale ale statelor cuprind norme cu privire la protecţia domeniului informatic. Deosebirile existente între legislaţiile penale ale statelor în ceea ce priveşte modul de reglementare al protecţiei domeniului informatic se explică, pe de o parte, prin faptul că infracţiunile din domeniul activităţilor informatice nu au fost recunoscute pe plan mondial, decît în ultimii ani şi au avut evaluări diferite, iar, pe de altă parte, prin nivelul scăzut de dezvoltare al domeniului tehnologiilor informatice şi al sistemelor de telecomunicaţii în anumite state, introducerea reglementărilor în această materie nu era oportună.

Gradul de dezvoltare a tehnologiilor informaţionale depinde direct de dezvoltarea resurselor informaţionale, de cultura informaţională a membrilor societăţii, de competenţa cadrelor corespunzătoare ce activează în domeniul dat. Paralel cu dezvoltarea tehnologiilor informaţionale se dezvoltă infracţiunile în acest domeniu, iar succesul depistării infractorului şi aducerea acestuia la răspundere juridică în instanţă nu depinde de oamenii care utilizează sistemele informatice, asta este datoria primară a statului.

Republica Moldova se află la o etapă fragilă de dezvoltare a ramurii respective şi întâmpină greutăţi în prevenirea şi combaterea crimelor de genul dat. De asemenea se reține a fi fragilă politica de stat în domeniul securităţii informaţionale, care ar unifica măsurile juridice, organizatorice, tehnice, tehnologice şi fizice de protecţie a spaţiului cibernetic al Republicii Moldova, precum şi reglementarea clară a rolurilor şi competenţelor autorităţilor de resort.

Prin urmare, pentru a construi o societate informaţională sănătoasă, statul, în primul rând, trebuie să i-a toate măsurile necesare pentru a asigura securitatea subiecţilor participanţi la relaţiile informaţionale şi acestea ar fi:

1) Reglementarea tranzacţiilor electronice. Elaborarea unui cadru legal adecvat pentru afaceri, care să reglementeze nu numai comerţul electronic şi

semnătura electronică, ci şi aspectele referitoare la banii electronici, fiscalitatea şi modul de încheiere a contractelor în Internet;

2) Elaborarea tehnicilor şi metodologiilor de cercetare a infracţiunilor informatice. Datorită caracterului transfrontalier al criminalităţii informatice, armonizarea legislaţiei cu cea internaţională trebuie să vizeze, în principal: dreptul de autor, confidenţialitatea datelor, prevenirea şi combaterea criminalităţii informatice, precum şi promovarea standardelor tehnice care să asigure intercomunicarea noilor reţele de comunicaţii.
3) Crearea programelor de studiu şi pregătirea specialiştilor în domeniul securităţii informatice.

În Republica Moldova este elaborată Strategia securității informaționale pentru anii 2019-2024, fiind elaborat în anul 2019 raportul de monitorizare și evaluare a implimentării strategiei vizate. Raportul de monitorizare şi evaluare a Strategiei securităţii informaţionale pentru anii 2019-2024 reprezintă o analiză a acţiunilor întreprinse, progresul înregistrat şi rezultatele obţinute pe parcursul anului 2019 la realizarea Planului de acţiuni al Strategiei, adoptată prin Hotărîrea Parlamentului nr.257 din 22.11.2018.

Serviciul de Informaţii şi Securitate al Republicii Moldova, conform prevederilor art.art. 2 şi 3 al HP nr. 257 din 22.11.2018 şi a pct.115 din Strategie, este desemnat ca autoritate coordonatoare şi responsabilă de monitorizarea şi coordonarea procesului de implementare a Planului de acţiuni.

Concepţia securităţii informaţionale a Republicii Moldova, aprobată prin Legea nr.299/2017, reprezintă documentul de politici ce stă la baza reglementării procesului de implementare a Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019-2024.

Strategia securităţii informaţionale a Republicii Moldova 2019-2024 are scopul de a corela juridic şi de a integra sistemic domeniile prioritare cu responsabilităţi şi competenţe de asigurare a securităţii informaţionale la nivel naţional, fiind bazat pe rezilienţa cibernetică, pluralismul multimedia şi convergenţa instituţională în materie de securitate, destinate protejării suveranităţii, independenţei şi integrităţii teritoriale a Republicii Moldova.

Planul de acţiuni însumează complexul de acţiuni elaborate de instituţiile de drept public şi privat, care sunt parte a societăţii informaţionale, precum şi acelor care direct sau indirect au competenţe şi atribuţii la domeniul informaţiei, comunicării şi tehnologiilor informaţionale, pentru a realiza obiectivele Strategiei după cum urmează:

1) Pilonul I - Asigurarea securităţii spaţiului informaţional-cibernetic şi investigarea criminalităţii informatice;
2) Pilonul II - Asigurarea securităţii spaţiului informaţional-mediatic;
3) Pilonul III - Consolidarea capacităţilor operaţionale;
4) Pilonul IV - Eficientizarea proceselor de coordonare internă şi de cooperare internaţională în domeniul securităţii informaţionale.

Procesul de monitorizare realizat pe parcursul anului 2019 şi expus în contextul raportul pentru primul an de implementare, denotă relevanţa Strategiei securității

informaționale pentru anii 2019-2024, iar priorităţile de securitate informaţională stabilite în Strategie continuă să fie conforme tendinţelor de dezvoltare a societăţii informaţionale la nivel naţional şi internaţional.

Prin urmare, efectuînd o analiză obiectivă şi multiaspectuală asupra practicii judiciare cu privire examinarea cauzelor penale comise prin intermediul tehnologiilor informaţinale asupra sentinţelor primelor instanţe 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 sentinţelor de către primele instanţe, însă se constată că totuşi instanţele de fond în unele cazuri în cadrul judecării cauzelor și adoptării sentinţelor pe caz, nu au dat aprecierii la justa valoare a tuturor circumstanţelor cauzelor penale în fapt şi de drept. Ca rezultat a aprecierii incorecte și în lipsa cercetării sub toate aspectele a circumstanţelor cauzei s-a admis stabilirea de către primele instanţe a unor pedepse penale pentru faptele comise de către inculpați contrar prevederilor art.61 Cod penal și art.75 Cod penal.

Pe cale de consecinţe, este remarcabil faptul că instanţele de fond urmează să ţină cont de cele menţionate în prezenta notă informativă şi să examineze cauzele efectuînd o vastă cercetare, multiaspectuală şi obiectivă a circumstanţelor cauzei cu verificarea tuturor aspectelor de drept ce au importanţă pentru justa soluţionare a cauzelor 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, care ar avea drept scop pronunţarea unor hotărîri judecătoreşti legale şi întemeiate, şi în scopul unei practici judiciare uniforme, avînd în vedere rezultatele generalizării în cauză,

SE PROPUNE:

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

Coordonator,
Judecător al Colegiului penal
al Curţii de Apel Bălţi **Angela Revenco**

Executor, Specialist principal a
Direcţiei Sistematizare, Generalizare
a Practicii Judiciare şi Relaţii cu publicul **Mariana Alexei**