**TEMA 6**

***PROBLEMATICA RĂSPUNDERII PENALE ŞI ACALIFICĂRII INFRACŢIUNILOR ÎN DOMENIUL INFORMATIC***

**Unităţi de conţinut:**

1. **Problematica răspunderii penale şi a calificării infracţiunilor contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice**
2. **Problematica răspunderii penale şi a calificării infracţiunilor informatice în accepţiune strictă**

**1. Problematica răspunderii penale şi a calificării infracţiunilor contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice**

Din analiza normelor din Capitolul XI din Partea Specială al Codului penal rezultă că comiterea unei fapte prin intermediul tehnologiilor informaționale sau a sistemelor informatice este susceptibilă să îndeplinească elementele constitutive ale mai multor infracţiuni. Este posibil, spre exemplu, pentru a putea **altera integritatea datelor informatice ţinute într-un sistem informatic**al unei persoane juridice să se intercepteze o transmisie de date informatice pentru a accesa în mod ilegal sistemul informatic al acestei persoane. Prin accesarea sistemul informatic se poate modifica datele informatice, care generează perturbarea funcționării acestui sistem. Astfel, în ipoteza descrisă se înglobează elementele constitutive ale mai multor infracţiuni informatice. Cum se va califica cele comise (cu sau fără cauzarea daunelor personei juridice)? În cele ce urmează vom încerca să stabilim în ce situații este prezent un concurs de infracțiuni și, respectiv, în care nu.

Dificultatea soluționării dilemei date, adică a problematicii atragerii la răspundere penală şi a încadrării juridice infracţiunilor din domeniul informatic, are originea în structura normelor de incriminare; or, legiuitorul le-a structurat astfel încât a inclus în calitate de semne calificative: prezenţa acţiunilor adiacente; urmare prejudiciabilă sub formă de daune în proporţii mari; scopului special de a comite una sau mai multe infracţiuni enumerate exhaustiv.

Începem analiza acestui paragraf prin studiul problematicii încadrării juridice a infracţiunii prevăzute al art.259 CP RM. Controversele derivă, în primul rând, din structura complexă a laturii obiective a faptei prejudiciabile, şi anume – reținem că acţiunea principală (accesul ilegal la informaţia computerizată) trebuie să fie însoţită, în mod obligatoriu, de acţiunea adiacentă (distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice). Astfel, în lipsa acesteia, aşa cum o specifică şi S.Copeţichi[[1]](#footnote-1), cele comise nu pot fi încadrate potrivit art.259 CP RM. Totuşi, în condiţiile în care făptuitorul doreşte, totodată, să cauzeze şi daune în proporţii mari, cele comise trebuie catalogate drept tentativă la infracţiunea de acces ilegal la informaţia comuterizată, în ipoteza în care făptuitorul realizează acţiunea principală, dar din cauze independente de voinţa lui să nu-i reuşească comiterea uneia din acţiunile adiacente (de exemplu: distrugerea sau copierea).

În asemenea circumstanțe, nu este clar raţionamentul legiuitorului moldav care la incriminarea infracţiunii de acces ilegal la informaţia computerizată reuneşte în cadrul normei de la art.259 CP RM pe lângă fapta prevăzută la art.2 (Accesarea ilegală) din Convenţia Consiliului Europei privind criminalitatea informatică de la Budapesta[[2]](#footnote-2)şi faptele distinse drept infracţiuni de la art.4 (Afectarea integrităţii datelor) precum şi art.5 (Afectarea integrităţii sistemului), fapt ce complică semnificativ calificarea faptei.

O altă dilemă apare şi în cazul determinării prejudiciilor în proporţii mari şi a legăturii de cauzalitate dintrea acestea, ca semne obligatorii ale laturii obiective. Aceasta deoarece nu toate *modus operandi* care duc la distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice prevăzute la art.259 CP RM pot fi estimate în bani (spre exemplu, prin acces ilegal la un calculator, în scop de a împiedica promovarea unei persoane, a fost o distrusă o lucrare ştiinţifică ce reprezintă munca acesteia timp de doi ani). Astfel, apare întrebarea: care este modalitatea de evaluare a informaţiei deţinute întrun sistem informaţional? În asemnea situaţii, prejudiciul cauzat este constituit din prejudiciul moral şi un eventual venit ratat (dacă va fi constatată valoarea propriuzisă a informației), care este stabilită de către instanţă.

Este de menționat că și doctrina rusă consideră discutabilă includerea urmării prejudiciabile în calitate de semn obligatoriu al laturii obiective a infracțiunii de acces ilegal la informația compiuterizată; or, și legiuitorul rus (*n.a.* – ca și cel moldav) nu determină conceptul tipurilor specifice de consecințe prejudiciabile în dispoziția articolului (art.272 CP FR)[[3]](#footnote-3).

În ceea ce priveşte prejudiciul în proporţii mari cauzat, care în corepundere cu art.126 CP RM este acela, valoarea căruia depăşeşte 20 de salarii medii lunare pe economie prognozate, stabilite prin Hotărârea Guvernului în vigoare la momentul săvârşirii faptei (cuantumul salariului mediu lunar pe economie, prognozat pentru anul 2021, este în mărime de 8716 lei[[4]](#footnote-4)), credem că este mult prea mare pentru a criminaliza fapta doar în condiţiile prevăzute la art.259 CP RM.

Pe de de altă parte, din analiza de drept penal comparată efectuată (*a se vedea* Tema 7) și după cum a stabilit și S.Copeţchi,[[5]](#footnote-5) normele din legiuirile penale ale majorităţii statelor europene, ce incriminează accesul ilegal la sisteme informatice, nu prevăd urmarea prejudiciabilă în calitate de semn constitutiv. *Ad similis*, Convenţia privind criminalitatea informatică nu prevede vreo urmare prejudiciabilă la art.2 (Accesarea ilegală) care stabilește, *inter alia*, „incriminarea ca infracţiune, pentru dreptul său intern, accesarea intenţionată şi fără drept a asamblului sau a unei părţi a unui sistem informatic”. Astfel, nu este clar raţionamentul legiuitorului moldav care la incriminarea infracţiunii de acces ilegal la informaţia computerizată reuneşte în cadrul art.259 CP RM şi faptele distinse drept infrcţiuni de către Convenţie prevăzute la art.4 (Afectarea integrităţii datelor) şi art.5 (Afectarea integrităţii sistemului).

Să presupunem că legiuitorul moldav la adoptarea acestei norme s-a condus de pct.37 al Rportului explicativ al Convenţia Consiliului Europei privind criminalitatea informatică[[6]](#footnote-6), care, stabileşte că, *Părţile pot să excludă infracţiunile minore sau nesemnificative din câmpul de aplicare a art.2 până la art.10din Convenţie*. Însă, este greu de conceput că cauzarea unei daune mai mici de 20 de salarii medii lunare pe economie prognozate (pentru anul 2020 – în sumă mai mică de 159 060 lei), poate fi apreciată drept infracţiune minoră sau nesemnificativă. Mai mult, în conformitate cu prevederile Directivei 2013/40/UE referitoare la atacurile împotriva sistemelor informatice[[7]](#footnote-7), un caz poate fi considerat minor în situaţiile în care prejudiciile cauzate de infracţiune şi riscul la adresa intereselor publice sau private este nesemnificativ sau de alta natură încât aplicarea unei sancţiuni penale în cadrul limitelor legale sau angajarea răspunderii penale nu este necesară.

În viziune noastră, atât Raportului explicativ al Convenției, cât şi Directiva 2013/40/UE referinduse la infracțiunile minore sau nesemnificative se referă la faptele care cauzează un prejudiciu în proporții mici; or, în legislaţia națională a statelor ce fac parte la Convenţia de la Budapesta, faptele ilicite sunt clasificate diferit în coraport cu gradul de prejudiciabilite al acestora. De altfel, în conformitate cu dreptul intern al Republicii Moldova, fapta, acţiune sau inacţiune, ilicită, cu un grad de pericol social mai redus decât infracţiunea este contravenţia (art.10 Cod Contravenţional[[8]](#footnote-8)), ceea ce corespunde cu cele prevăzute în Directiva 2013/40/UE.

În acest context, din analiza sistemică a normelor din Codul Contravenţional al Republicii Moldova, deducem că accesul ilegal la informația computerizată nu îşi are existenţa, nici parțială, în calitate de contravenţie. Prin urmare, în cazul comiterii acţiunilor prevăzute la art.259 CP RM şi provocând victimei o daună în valoare de până la 159 060 lei, totodată neurmărind cauzarea de daune în proporţii mari, făptuitorul rămâne nepedepsit. În asemenea împrejurări legiuitorul moldav nu apără pe deplin relaţiile sociale privind accesul legal la informaţia computerizată, şi nici relaţiile sociale privind imixtiunea legală în sistemul informaţional.

Dacă facem o analogie *grosso modo* (necătând că nu este permisă, însă în cazul nostru, raţională) cu infracţiunea prevăzută la art.179 CP RM (Violarea de domiciliu) ce prevede acţiunea (inacţiunea) de pătrundere sau rămânere ilegală în domiciliul sau în reşedinţa unei persoane fără consimţământul acesteia, se observă că aceasta nu reprezintă altceva decât accesul ilegal în domicilul sau reşedinţa personei. Mai mult, cum este recunoscut şi în doctrină[[9]](#footnote-9), sistemul informatic împreună cu datele informatice reprezintă *spaţiul informatic* sau *domiciliul informatic*. În asemenea circumstanţe, se prezumă necesitatea reglementării similară a *spaţiul informatic (domiciliul informatic)* cu cel al domiciliului real. Acest lucru este ineluctabil, având în vedere faptul că cyberspațiul (a se citi – mediul online – *n.a.*) devine, după cuvintele lui Gh. Reniță, tot mai mult o „a doua natură umană”[[10]](#footnote-10).

Axându-ne pe raționamentele invocate *supra* considerăm oportun ca legiuitorul nostru să reevalueze propunerea *de lege ferenda* consemnată în Proiectul de Lege pentru modificarea şi completre unor acte legislative[[11]](#footnote-11), înregistrat la data de 13.04.2016 şi retras la 14.06.2018, susţinută de către doctrină[[12]](#footnote-12), şi anume: 1) excluderea urmării prejudiciabile sub formă de daune în proporţii mari din dispoziţia de la alin.(1) art.259 CP RM; şi 2) prevederea accesteia în calitate de circumstanţă agravantă la lit.h) alin.(2) art.259 CP RM.

Într-un al vector al cercetării, remarcăm că problematica calificării faptelor este reprezentată de faptul că, uneori, infracțiunea comisă poate atenta şi la alte relaţii sociale, care ies din aria de acoperire a valorilor protejate doar prin norma de la alin.(1) art.259 CP RM. Atestăm o situație în cazul în care se accesează ilegal informaţia computerizată, protejată de lege, despre viaţa personală ce constituie secret personal sau familial al altei persoane, culegerea ilegală sau răspândirea cu bună-ştiinţă în acest mod a informaţiilor, atrage răspunderea penală în conformitate cu una dintre faptele de **încălcare a inviolabilităţii vieţii personale**. Însă, în cazul în care făptuitorul accesând informația ce constituie secret personal sau familial al altei persoane, totodată distruge, deteriorează, modifică, blochiază sau copie informaţia computerizată ori dereglează funcţionarea calculatoarelor, a sistemului informatic sau a reţelei informatice, cauzează prin aceasta daune în proporţii mari, cum menționează și autorii S.Brînza și V.Stati, nu este exclus concursul dintre infracţiunea prevăzută la lit.g) alin.(2) art.259 CP RM şi una din infracţiunile specificate la alin.(1) sau (11) art.177 CP RM[[13]](#footnote-13).

De asemenea, putem menționa și cazul de violare a dreptului la secretul corespondenţei electronice întreţinute prin *e-mail*, cum menționeză și doctrina[[14]](#footnote-14), în contextul în care legiuitorul nu face referire la tipul corespondenței, fapta comisă se va califica în conformitate cu art.178 CP RM. Iar dacă prin această accesare aplicaţia de poştă electronică se cauzează un prejudiciu (calculatorului, sistemului informatic etc.) în proporții mari, atunci infracțiunea comisă reprezintă acces ilegal la informația computerizată (alin.(1) art.259 CP RM). Cazuri similare mai există în Codul penal (spre exemplu: art.1851, 24510, 24512, 337, 338, 344 CP RM) calificarea cărora se face în conformitate cu algoritmul de mai sus. De remarcat că în cazul **obţinerii ilegale şi/sau divulgării informaţiilor ce constituie secret comercial sau bancar** (art. 24510 CP RM) legiuitorul a prevăzut expres folosirea tehnicilor speciale în calitate de modalitate a activității infracționale.

În ceea ce privește comiterea infracțiunii de aces ilegal la informația computeriztă ca mijloc de hărţuire a unei persoane prin acţiuni repetate, încdrarea juridică poate forma un concurs de infracțiuni a celei incriminate la art.259 cu cea de la prevăzută la art.173 CP RM. Aceasta deoarece totodată sunt prejudiciate și relaţiile sociale cu privire la inviolabilitatea sexuală sau libertatea sexuală a persoanei, în calitate de obiect șuridic principal al hărțuirii sexuale.

De asemnea, prin intermediul internetului sau a altor tehnologii informaționale, pot fi săvârșite și acțiunile perverse (art.175 CP RM), în care a lipsit contactul fizic nemijlocit cu corpul victimei, totodată fiind îndreptate spre satisfacerea poftelor sexuale a făptuitorului, spre apariția dorinței sexuale la victimă sau spre trezirea interesului acesteia față de relații sexuale. În asemnea circumstanțe, infracțiunea prevăzută la art.259 CP RM poate intra, în prezența tuturor semnelor necesare ale componențelor de infracțiune respective, în concurs cu infracțiunea prevăzută la art.175 CP RM.

Întrebarea controversată din literatura juridico-penală[[15]](#footnote-15) constă în posibilitatea aplicării răspunderii penale pentru infracțiunea de acces ilegal la informația computerizată, în cazul în care se sustrage dispozitivul extern de păstrare a informației, după care făptuitorul copiază sau distruge informația ce se conține pe dispozitiv. Este cert faptul că, în astfel de cazuri este temei pentru calificarea celor comise de către făptuitor în conformitate cu art.186 CP RM în concurs cu infracțiunea prevăzută de art. 259 CP al RM (în caz de cauzare a unui pregudiciu în proporții mari).

În alt registru, la prima vedere, accesul ilegal la informaţia computerizată presupune etapa premergătoare de comitere a infracţiunile specificate la art.2601-2603  CP RM. Totuşi, constatăm că interceptarea ilegală se poate realiza şi prin interceptarea emisiei electromagnetice (art.2601 CP RM), fapt ce poate fi realizat fără accesul ilegal la informaţia computerizată. De altfel, atât alterarea integrităţii datelor informatice dintr-un sistem informatic (art.2602 CP RM) cât și perturbarea funcţionării sistemului informatic (art.2603 CP RM) se pot comite şi în situaţia în care accesul la informaţia computerizată este licit, adică de către o persoană care este autorizată în temeiul legii sau al unui contract, acționează în limitele autorizării ori 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 în cadrul sistemului informatic. Astfel, cum relatează şi autorii S.Brînză şi V.Stati, accesul ilegal la informaţia computerizată nu constituie neapărat o situaţie premisă a săvârşirii infracţiunilor prevăzute la art.2601-2603 CP RM[[16]](#footnote-16). Totodată, potrivit aceloraşi autori, opinie susținută și de noi, în ipoteza în care se accesează ilegal informaţia computerizată în scopul comiterii vreuneia din infracţiunile specificate la art.2601-2603  CP RM (inclusiv în scopul comiterii unei alte infracțiuni), iar acest scop îşi găseşte realizarea, ne vom afla în prezenţa unui concurs între infracţiunea prevăzută la alin.(1) art.259 CP RM şi una dintre infracţiunile specificate la art.2601-2603  CP RM[[17]](#footnote-17).

În alt context, observăm că legiuitorul moldav a redat infracţiunile prevăzute la lit.f) alin.(2) art.259, art.260 şi 2604 CP RM ca activităţi de pregătire a altor infracţiuni. Astfel, scopul special al faptei incriminate la lit.f) alin.(2) art.259 CP RM este de a comite infracţiunile prevăzute la alin.(1) art.259, art. 2601−2603, 2605 şi 2606 CP RM, iar cel de la art.260 şi 2604 CP RMeste de a comite faptele incriminate la art.237, 259, 2601−2603, 2605 şi 2606 CP RM. Astfel, în ipoteza în care făptuitorul îşi realizează scopul, cele comise trebuie să fie încadrate ca concurs de infrcţiuni, adică infracţiunea prevăzută la lit.f) alin.(2) art.259 (art.260 sau art.2604 CP RM) şi una dintre infracţiunile de la alin.(1) art.259, art. 2601−2603, 2605 şi 2606 CP RM (art.237, 259, 2601-2603, 2605 şi 2606 CP RM).

De consemnat că, în cazul în care: utilizarea ilegală a calculatorului, sistemului sau reţelei informatice (lit.f) alin.(2) art.259 CP RM); *ori* producerea, importul, comercializarea sau punerea la dispoziţie, sub orice altă formă, în mod ilegal, a mijloacelor tehnice sau produselor program, concepute sau adaptate (art.260 CP RM); *ori* producerea, importul, comercializarea sau punerea la dispoziţie, sub orice altă formă, în mod ilegal, a unei parole, a unui cod de acces sau a unor date similare care permit accesul total sau parţial la un sistem informatic (art.2604 CP RM) sunt comise în scopul unei alte infracţiuni decât celei specificate în normele de incriminare (spre exemplu: comiterea infracţiunii de pornografie infrantilă (art.2081 CP RM), sau în cazul accesrii ilegale a informaţiei computerizate, protejată de lege, despre viaţa personală ce constituie secret personal sau familial al altei persoane (una din infracţiunile specificate la alin.(1) sau (11) art.177 CP RM)), fapta se califică ca pregătire (art.26 CP RM) de infracţiune scop. Iar în contextul realizării scopului propus, vom fi în prezenţa infracţiunii unice, şi anume a unei dintre infracţiunile prevăzute la art.2081, 177 CP RM etc., doar în cazul accesului ilegal la informația computerizată (când se întrunesc toate semnele componenței de infracțiune), se va reține concursul între infracțiunea incriminată la alin.(1) art.259 CP RM și după caz, art.2081 ori art.177 CP RM. Aceasta deoarece, actele de pregătire a infracțiunii sunt incriminate de către legiuitor ca infracţiune de sine stătătoare, iar raționamentul reținerii concursului rezidă în pericolul social al faptelor comise, ce se datorează valorilor sociale protejate de lege prejudiciate în cazul dat (nu se are în vedere gravitatea faptei; or, este alogică catalogarea infracțiunii prevăzute la alin.(1) art.259 CP RM ca una ușoară în momentul existenței daunelor în proporții mari în calitate de urmare prejudiciabilă, pe când aceași daună în cazul infracțiunii de furt plasează fapta în rândul infracțiunilor grave), precum și faptul că, faptele incriminate la art.2081 și art.177 CP RM pot fi comise și fără accesarea ilegală informația computerizată. Astfel, sutem în prezența unui concurs de infracțiuni cu conexitate etiologică, când persoana săvârșește infracțiunea-mijloc pentru pregătirea unei alte infracțiuni-scop. O soluție contrară ar încălca principiul legalității incriminării.

Reglementarea propusă de legiuitorului nostru se justifică prin cerinţele prezente în Convenţia de la Budapesta (art.6). Însă, în ipoteza în care faptele prevăzute la lit.f) alin.(2) art.259, art.260 şi 2604 CP RM sunt comise în scopul unei alte infracţiuni decât cele din norma de incriminre, periculozitatea acestora nu este diminuată. Astfel, pentru uniformizarea aplicabilităţii normelor penale este raţional de a exclude enumerarea exhaustivă a infracţiunilor ce reprezintă scopul pentru care se comit faptele pervăzute la lit.f) alin.(2) art.259, art.260 şi 2604 CP RM.

De altfel, este ambiguă poziţia legiuitorului de a include la art.2604 CP RM cauzarea de daune în proporţii mari în calitate de urmare prejudiciabilă, urmare absentă în cazul infracţiunii incriminată la art.260 CP RM, doar acestea se aseamănă după *modus operandi* (producerea, importul, comercializarea sau punerea la dispoziţie, sub orice altă formă, în mod ilegal) şi scop (de a comite o infracţiune prevăzută de art.237, 259, 2601−2603, 2605 şi 2606 CP RM) însă se deosebesc prin obiectul material (imaterial) al infracţiunii, iar în cazul acţiunii de producere prin produsul infracţiunii, şi anume: mijloacele tehnice sau produsele program (art.260CP RM) şi parole, coduri de acces sau datele similare (art.2604 CP RM).

Mai mult, considerăm inaplicabilă în practică modalitatea de producere în mod ilegal, a unei parole, a unui cod de acces sau a unor date similare care permit accesul total sau parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile prevăzute la art.237, 259, 2601−2603, 2605 şi 2606 CP RM, şi totodată această acţiune să cauzeze daune în proporţii mari. În context, din momentul că producerea reprezintă acea activitate care se finalizează cu un produs, rațional apare întrebarea în ce mod și cui i se cuzează daune? Este de subliniat că, în acest caz produsul propriuzis al infracţiunii nu poate provoca daune decânt în ipoteza că aceste sunt folosite la: **accesul ilegal la informaţia computerizată; interceptarea ilegală a unei transmisii de date informatice; alterarea integrităţii datelor informatice ţinute într-un sistem informatic**etc.

În această conjunctură, suntem de acord cu opinia lui S.Copeţchi[[18]](#footnote-18) care menţionează că, în vederea lichidării carenţelor legislative, dar şi întru asigurarea unei coerenţe dintre reglementările interne cu cele înscrise în art.6 din Convenţia de la Budapesta recomandăm legiuitorului moldav: a) să stabilească în cadrul unei singure norme răspunderea penală pentru manipulările ilegale realizate cu mijloacele tehnice sau produsele program (art.260CP RM) şi parole, coduri de acces sau datele similare (art.2604 CP RM); b) să ecludă urmarea prejudiciabilă din structura laturii obiective a infracţiunii prevăzută la art.2604 CP RM.

O problemă similară, adică existenţa semnului constitutiv daune în proporţii mari, este prezentă şi în cazul infracţiuniilor prevăzute la art.2602 şi 2603 CP RM.

De altfel, în cazul comiterii unor modalităţi faptice prevăzute de norma de incriminare a infracţiunii de **alterare a integrităţii datelor informatice ţinute într-un sistem informatic (**art.2602 CP RM**)**, cum ar fi: transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, punerea la dispoziţie, sub orice formă, a datelor informatice cu acces limitat nu în mod obligatoriu cauzează victimei un prejudiciu. Însă, din specificul datelor informatice, care după natura sa sunt cu „acces limitat”, periculozitatea faptei nu se diminuiază, iar pentru lezarea relaţiilor sociale cu privire la accesibilitatea şi circulaţia în condiţii de legalitate a datelor informatice este suficient ca făptuitorul în mod ilegal să le transfere, dobândească sau să le pună la dispoziţia unei terţe persoane.

Este de constatat că Convenţia de la Budapesta prevede la alin.(2) art.4 dreptul Părţilor de a condiţiona în dreptul său intern comportamentul care afectează integritatea datelor de producerea cu unele următi grave. Însă, norma incriminatoare-cadru din Convenţie prevede doar fapta *comisăintenţionatşi fără drept* de distrugere, ştergere, deteriorare, modificare sau eliminare a datelor informtice, comportament prin care se poate cuza o daună. Mai mult, Directiva 2013/40/UE la art.5 distinge necesitatea adoptării măsurilor necesare pentru a asigura că fapta care constă în ştergerea, periclitarea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau în a le face inaccesibile, cu intenţie şi fără drept, este incriminată, *cel puţin atunci când nu reprezintă un caz minor* (situație identică cu cea prezentă la analiza infracțiunii prevăzute la art.259 CP RM). Aceeaş specificre este prezentă şi în caz de afectare ilegală a integrităţii sistemului (art.4 al Directivei).

Astfel, întru înlăturarea normelor „moarte” (sau partea din normă neaplicabilă) şi protecţia relaţiilor sociale cu privire la accesibilitatea şi circulaţia în condiţii de legalitate a datelor informatice cu acces limitata propunem de a exclude urmarea prejudiciabilă sub formă de daune în proporţii mari din dispoziţia de la art.2602 CP RM, şi completarea acestuia cu un nou aliniat, care va fi alin.(2) care va prevederea daunele în proporţii mari în calitate de circumstanţă agravantă a faptei incriminate la art.2602 CP RM. Din raţionamente similare, formulăm următoarea recomandare: de a exclude urmarea prejudiciabilă sub formă de daune în proporţii mari din dispoziţia de la alin.(1) art.2603 CP RM, şi prevederea accesteia în calitate de circumstanţă agravantă la lit.d) alin.(2) art.2603 CP RM.

**2. Problematica răspunderii penale şi a calificării infracţiunilor informatice în accepţiune strictă**

Analizând infracţiunea de fals informatic (art. 2605 CP RM) menționăm că aceasta nu este prezentă în oricare caz în care se produc date necorespunzătoare adevărului, apte să genereze consecinţe juridice. Deci, nu poate fi aplicată răspunderea în baza art.2605 CP RM în situaţia în care accesul la sistemul informatic este legal, iar subiectul care introduce, modifică, şterge datele sau restricţionează accesul la acestea are dreptul să o facă. În acest caz, putem fi în prezența comiterii faptei prevăzute la art.2602 CP RM, în ipoteza modificării, ştergerii sau deteriorării intenţionate a datelor informatice ţinute într-un sistem informatic ori restricţionării ilegale a accesului la aceste date.Însă, dacă rezultă date necorespunzătoare adevărului, se poate reţine o altă infracţiune de fals, dar din cele specificate la art.332 sau 361 CP RM, dacă sunt întrunite toate semnele şi elementele acestor componenţe de infracţiune; or, cum este menționat de către pct.81 din Raportului Consiliului Europei[[19]](#footnote-19) scopul incriminării falsului informatic este de a crea o infracţiune paralelă cu falsificarea de documente tangibile pentru acoperirea lacunelor în dreptul penal legate de falsificarea tradiţională, care necesită lizibilitatea unui text încorporat într-un document şi care nu se aplică datelor stocate pe suport electronic.

Următorul caz din practica judiciară ne confirmă faptul că în cazul comiterii infracțiunii incriminate la art. 2605 CP RM, făptuitorul acționează fără drept de acces la datele informatice, deși activează în cadrul instituției: la 16 decembrie 2011, în temeiul încheierii executorului judecătoresc M.S., lui A.I. i-a fost transmis în proprietate privată bunul imobil cu nr.cadastral 0000 amplasat în or.Ialoveni.

La 03 ianuarie 2012, Ţ.A. fiind specialist în evidenţă a documentelor al OCT Ialoveni, aflându-se în biroul său de serviciu amplasat în or. Ialoveni, contrar atribuţiilor sale de serviciu, neavând acces la datele Registrului Bunurilor Imobile, cunoscând parola registratorului OCT Ialoveni C.V., intenţionat a introdus date informatice cu privire la punerea interdicţiei pe imobilul cu nr.cadastral 0000 amplasat în or. Ialoveni, ce se află în proprietatea lui A.I., fără documente justificate acestei i proceduri.

Tot ea, Ţ.A., în continuarea acţiunilor sale infracţionale a restricţionat ilegal accesul la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a limita dreptul de dispoziţie a proprietarului A.I. asupra bunului imobil menţionat. Această interdicţie falsă introdusă în datele informatice a Registrului Bunurilor Imobile, de către Ţ.A., s-a menţinut pînă la 13.01.2012, când a fost prezentată încheierea din 13.01.2012 a Judecătoriei Ialoveni cu privire la sechestru asupra bunului dat. În urma acţiunilor specialistului în evidenţa documentelor al OCT Ialoveni, Ţ.A., proprietarul bunului imobil A.I. a fost ilegal lipsită de dreptul de dispoziţiei în perioada 03-13.01.2012 asupra imobilului, prin ce i s-a cauzat consecinţe juridice.*[[20]](#footnote-20)*

Cu titlu de excepție, se va reţine infracţiunea de fals în acte publice (art.332 CP RM), iar nu infracţiunea de fals informatic, în cazul în care o persoană publică falsifică pe calculatorul de la locul de muncă un document oficial, de exemplu, prin desenarea ştampilei autorităţii publice emitente. În acest caz, accesul la sistemul informatic este legal, iar datele informatice sunt modificate de o persoană care are dreptul să facă acest lucru, atât sistemul informatic, cât şi datele conţinute de acesta aparţinându-i.

În contextul în care infracțiunea de fals informatic în legislația României (art.325) este similară cu cea prevăzută la art.2605 CP RM, provoacă interes problematica ridicată de către D.Pârgău cu referire la faptul *„d*acă fapta de a deschide și utiliza un cont pe o rețea de socializare deschisă publicului (rețea care nu solicită dovezi din care să reiasă folosirea numelui real de către deținătorul unui cont), furnizând ca nume de utilizator numele unei alte persoane și introducând date reale vizând această persoană (informații, fotografii, imagini video etc.) realizează condițiile de tipicitate ale infracțiunii de fals informatic prevăzută de art.325 CP, cu referire la cerințele ca acțiunea de introducere a unor date informatice să fie realizată fără drept și, respectiv, să aibă ca rezultat date necorespunzătoare adevărului”.[[21]](#footnote-21)

Într-adevăr, cum se observă din speță, făptuitorul a introdus ilegal date reale vizând o altă persoană. Cu toate acestea, în jurisprudența din România existentă decizii care nu confirmă aceasta. Astfel, Curtea de Apel București a decis că în cazul care *„inculpatului i se impută faptul că a săvârșit infracțiunea de fals informatic în modalitatea introducerii de date informatice, reținându-se în sarcina sa că a creat o pagină de facebook, purtând în mod ilegal, numele și sigla părții civile, într-un context negativ, pe care a postat ulterior texte denigratoare la adresa acesteia, care au avut drept consecință inducerea neîncrederii opiniei publice cu privire la activitatea societății”[[22]](#footnote-22)*, a stabilit: *pentru a fi îndeplinită tipicitatea prevăzută de lege pentru infracțiunea de fals informatic, elementul material al laturii obiective ar fi trebuit să se realizeze prin simularea contului de facebook; or, în practică și doctrină s-a amintit că elementul material al acestei infracțiuni se comite de cele mai multe ori prin: simularea hyperconexiunilor, simularea poștei electronice, simularea Web-ului. În ceea ce privește* ***cerința esențială „fără drept”,*** *Curtea a constatat că aceasta ar fi fost îndeplinită dacă inculpatul și-ar fi însușit paternitatea sau proprietatea numelui sau a siglei. De altfel, trebuie făcută o diferență între eventualul prejudiciu de imagine, moral sau/și material, pe care l-a suferit partea civilă și consecințele juridice ale săvârșirii acestei infracțiuni care apar dacă, datele astfel modificate, alterate sau șterse sunt apte să dea naștere, să modifice sau să stingă raporturi juridice, creând drepturi și obligații. În primul caz este vorba de prejudiciu, ca element al răspunderii civile delictuale, iar în cel de-al doilea caz reprezintă o cerință a laturii subiective, care face ca intenția, în cazul acestei infracțiuni, să fie calificată prin scop.[[23]](#footnote-23)*

Din cele menționate, putem conchide că pentru aplicarea normei prevăzute de la art.2605 CP RM este necesar de stabilit:

* + ilegalitatea introducerii, modificării sau ştergerii datelor informatice, ori ilegalitatea restricţionării accesului la aceste date;
	+ rezultatul realizării uneia sau a mai multor acțiuni ale elementului material trebuie să fie datele informatice ce nu corespund adevărului;
	+ prezența scopului, cel de a produce efecte juridice.

În alte cazuri, vom fi în prezența unei alte infracțiuni, sau chiar a unei contravenții (spre exemplu, calomnia).

În alt registru, conform unei opinii din literatura de specialitate, este greu de înțeles de ce restricționarea accesului la date informatice a fost asimilată cu falsificarea unui înscris, când în realitate corespunde mai degrabă sustragerii sau distrugerii unui înscris.[[24]](#footnote-24) Ar fi cazul când în calitate de un document falsificat se prezintă situația în care rezultatul acțiunii de restricționarea este ca *datele informatice să nu mai fie afișate* (de exemplul, persoana criptează accesul la datele informatice referitorare la venitul său sau poate a datoriilor sale, în așa mod, când solicită un împrumut bancar, datele referitoare la insuficiența venitului, ori prezența datoriilor nu se identifică în precesul de verificare.).

Aceași problematică este prezentă și în *modus operandi* ștergerea datelor informtice; or, aceasta poate fi prezentă doar în cazul ștergerii parțiale a datelor. În caz contrar, „este greu de conceput cum ar rezulta date necorespuzătoare adevărului, creându-se mai degrabă o situație identică celei în care un înscris este sustrs sau distrus”[[25]](#footnote-25).

În cele din urmă, făcând o cercetare a infracțiunii de fraudă informatică (2606 CP RM) s-a constata că, dificultatea aplicării în practică a tuturor operațiunilor financiare comise comise în mod fraudulos prin utilizarea tehnologiilor informaționale este dictată de faptul că, legiuitorul moldav a indicat exaustiv *modus operandi* al faptei (*a se vedea* paragraful 5.2). Acest lucru exclude atragerea la răspundere penală pentru ale acțiuni infracționale, cum ar fi, utilizarea, fără consimţămantul titularului, a unui instrument de plată electronică (efectuarea unei operaţiuni de retragere de numerar, incărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri), însă în practică se întâlnesc astfel de cazuri.

În acest sens, propunem un caz din practica judiciară rusă, la care a făcut referire autorul Ragulina A.V.[[26]](#footnote-26), unde se fundamentează faptul că infracțiunea de fraudă informatică (art. 159.6 CP FR) este comisă nu atât prin introducerea datelor informatice, ci prin utilizarea acestora: *N.L.S. a fost condamnată în temeiul art. 159.6 CP FR în următoarele circumstanțe: N.L.S., prin intermediul serviciul „Mobile Bank”, după ce a primit un e-mail la telefonul mobil despre limita disponibilă de bani în sumă de ... pe un cont bancar care nu îi aparține, deschis pe numele Ș. având intenția de a sustrage suma specificată a realizat-o, utilizând telefonul său mobil Samsung și o cartelă SIM cu un număr de abonat înregistrat pe numele lui D., pe care din greșeală a fost instalat serviciul „Mobile Bank” al Sberbank din Federația Rusă, care acordă dreptul de a gestiona banii din contul curent a lui Ș. Astfel, prin introducerea datelor informatice sub formă de semnale electronice – „mesaje SMS” la numărul „900”, prin rețeaua de telecomunicații a operatorului de telefonie mobilă „Beeline”, a transferat (sustras), în mai multe rate, bani în suma de ... din contul curent care aparține lui Sh. în contul unei cartele SIM cu număr de abonat ..., cauzându-i lui Ș. daune materiale în valoare totală de ... ruble.* Deci, cum se observă *N.L.S*. a avut posibilitatea să extragă banii din contul bancar, doar datorită utilizării informației primite pe *e-mail,* în așa mod fiind atrasă la răspundere penal pentru frauda informatică, normă prevăzută la art.1596 din Codul penal al Federației Ruse (în continuare CP FR) (sustragerea bunurilor străine sau obținerea dreptului de proprietate asupra bunurilor străine, prin intermediul introducerii, modificării, blocării sau ștergerii datelor informatice sau prin intermediul altor intervenții în funcționarea unui sistem informatic).

Aparent prevederile din legislația rusă al infracțiunii de fraudă informatică sunt echivalentul celor de la art.2606 CP RM, totuși deosebirea semnificativă este reprezentată de predederile „*sustragerea bunurilor străine sau obținerea dreptului de proprietate asupra bunurilor străine”* (art.1596 CP CP FR) și „*scopul de a obţine un beneficiu material pentru sine sau pentru altul”*(art.2606 CP RM). Astfel, în conformitate cu prevederile legale autohtone realizarea scopului pentru care se introduce, modifică sau se şterge datelor informatice, se restricţionează accesul la aceste date ori se împiedică în orice mod funcţionarea unui sistem informatic poate fi și prin sustracerea bunurilor ori altfel obținerea dreptului de proprietate. Deci, în conformitate cu regulele de calificre, vom fi în prezența unui concurs de infracțiuni dintre fapta prevăzută la art.2606 CP RM și una de la art.art.186, 187, 189, CP RM etc.

Datorită faptului că legiuitorul a limitat modalitățile faprice ale infracțiunii de fraudă informatică, rezultă faptul că alte forme de imixtiune la datele informatice sau la sistemului informatic în scopuri cupidante, face inaplicabilă norma prevăzută la art.2606 CP RM. De exemplu, acțiunile făptuitorului, care a copiat loghinul și parola victimei, iar după aceasta a folosit datele obținute pentru a se autoriza în sistemul plaților *online* și a sustras bani, formează semnele componențelor de infracțiune, prevăzute la art. 186 și 259 CP RM (în caz că daunile cauzate sunt proporții mari).

De altfel, frauda informatică este comisă prin influența (introducerea, modificarea sau ştergerea ilegală ori restricţionarea ilegală a accesului) cu ajutorul tehnologiilor informaționale asupra informației computerizate, mijloacelor de păstrare, prelucrare sau transmitere a acestora, asupra rețelelor informaționale și de telecomunicații. Prin urmare, frauda informatică, comisă prin accesul ilegal la informație computerizată sau prin producerea, folosirea sau răspândirea programelor dăunătoare (cu respectarea tutror elementelor componenței de infracțiune), necesită o calificare suplimentară în conformitate cu una din infracțiunile incriminate la art. 259 și 260 CP RM.

În ceea ce privește infracțiunea de escrocherie și cea de cauzare de daune prin înșelăciune sau abuz de încredere, este relevantă opinia autorului R.Cojocaru, conform căreia, „extinderea conceptului de escrocherie informaţională la alte fapte penale săvârşite prin intermediul reţelelor informaţionale (cum ar fi, de exemplu, delapidarea averii străine, cauzarea de pagube materiale prin înşelăciune sau abuz de încredere, frauda informatică) poate fi acceptată doar în limitele unui studiu criminologic. Din perspectiva dreptului penal, menționează autorul, o asemenea lărgire de concept nu poate fi acceptată, întrucât legiuitorul la art.190 CP RM fixează un cadru legal bine definit al escrocheriei, care nu poate fi extins la alte conduite ilicite cu caracter penal. De fapt, din raţiuni de tehnică legislativă, în vederea asigurării unei interpretări uniforme a normativului penal, nu poate fi acceptată ideea atribuirii unor înţelesuri diferite expresiilor şi termenilor folosiţi în legislaţia penală la descrierea componenţelor de infracţiune”.[[27]](#footnote-27) În susținerea poziției sale autorul subliniază că, în vederea asigurării aplicării corecte a legii penale, în strictă consonanţă cu principiul legalităţii, este necesar de a stabili cu claritate normele cu caracter incriminator ce devin incidente în raport cu diferitele forme pe care le pot îmbrăca sustragerile din reţelele infromaţionale şi prin aceasta – limitele aplicării normei privitoare la escrocherie. Punctul de reper în acest sens, fără doar şi poate, îl constituie norma prevăzută la art.190 CP RM, care stabileşte extremităţile de incidenţă a legii penale în ceea ce priveşte posibilitatea încadrării unei fapte ca escrocherie. În acest sens, se concluzionează că fapta incriminată la art.190 CP RM devine aplicabilă când calculatorul şi informaţia computerizată sunt utilizate de către făptuitor pentru influenţarea voinţei victimei de a transmite benevol bunul sau dreptul asupra acestuia, sub dominaţia înşelăciunii sau abuzului de încredere.[[28]](#footnote-28)

Totuși, așa cum o menționează și autorii S.Brînza și V.Stati, în raport cu infracţiunile prevăzute la art.190 şi 196 CP RM, infracţiunea specificată la alin.(1) art.2606 CP RM se distinge prin recurgerea la mijloace informatice (*e-mail*, mesagerie instantă, pagină *Web* etc.), aplicate într-un mediu informatic. Tocmai aceste mijloace speciale de săvârşire a infracţiunii au ca efect că alin.(1) art.2606 CP RM reprezintă o normă specială faţă de art.190 şi 196 CP RM. În consecinţă, aplicarea alin.(1) art.2606 CP RM exclude reţinerea la calificare a uneia dintre infracţiunile prevăzute la art.190 sau 196 CP RM.[[29]](#footnote-29)

În acest context, susținem opinia lui Crijanovschi S.,[[30]](#footnote-30) care în procesul analizei comparate a infracțiunii de fraudă informatică a subliniat că, „efectuand o comparare simplă a legii penale autohtone şi a legii penale române, se scoate în evidenţa un domeniu cibernetic suficient de larg, care rămane a fi neacoperit de legea penală a Republicii Moldova, şi anume – domeniul efectuării operaţiunilor financiare frauduloase *„prin utilizarea, fără consimţămantul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia”*, sau *„prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimţămantul titularului său”*, sau *„prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive”*.

Având în vedere cele menționate *supra*, conchidem că legea penală a Republicii Moldova urmează a fi ajustată, pentru a conferi relațiilor sociale din domeniul analizat o protecție corespunzătoare.

**Bibliografie:**

Brînza S., Stati V. Tratat de Drept penal. Partea Specială. Volumul II. Chişinău: Tipografia Centrală, 2015.

Codul contravențional al Republicii Moldova, adoptat de Parlamentul Republicii Moldova la 24.10.2008. În: Monitorul Oficial al Republicii Moldova, 2017, nr.78-84

1. Cojocaru R. Escrocherii informaţionale: forme şi clarificări conceptuale ale cadrului normativ-penal de incriminare. În: Probleme de prevenire şi combatere a criminalităţii de către organele afcerilor interne în perioada recesiunii economice. Chişinău, 2010.

<http://academy.police.md/assets/files/pdf/2009_15_octombrie_Recesiunea_economica.pdf>

Copetchi, S.Infracţiunile informatice potrivit legii penale moldave: studiu de drept penal comparat şi propuneri de lege ferenda. În: Culegerea comunicărilor Conferinţa ştiinţifică naţională cu participare Internaţională: “Realităţi şi perspective ale învăţământului juridic naţional”, Volumul II, 01-02 octombrie 2019.

Convenţia Consiliului Europei privind criminalitatea informatică de la Budapesta din 23.11.2001 [Accesat 20.08.2020] Disponibil: <http://legislatie.just.ro/Public/DetaliiDocumentAfis/51289>

Crijanovschi S. Unele aspecte privind analiza juridico-penală comparativă a infracţiunilor informatice în legea penală a Republicii Moldova şi cea a României. În: Studia Universitatis Moldavia. Seria „Ştiinţe Sociale”, 2016, nr.3(93).

Decizia Curții de Apel București, nr.1044/A din 08.08.2017<http://www.rolii.ro/hotarari/59b88c86e49009740e000093>

Decizia Curții Supreme de Justiție din 25 iunie 2014. Dosarul nr.1ra-1113/2014<http://jurisprudenta.csj.md/search_col_penal.php?id=2653>

Dobrinoiu, M. Infracțiuni în domeniul informatic. București: C.H.Beck, 2006.

Directiva 2013/40/UE a Parlamentului European şi a Consiliului privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului din 12 august 2013. <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=RO>

Explanatory Report to the Convention on Cybercrime. Budapest, 23.XI.2001. European Treaty Series, No.185 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b>

Hotărârea Guvernului Republicii Moldova privind aprobarea cuantumului salariului mediu lunar pe economie, prognozat pentru anul 2020, nr.678 din 27.12.2019. În: Monitorul Oficial al Republicii Moldova, nr.400-406 din 31.12.2019

Pârgău D. Despre limitele falsului informatic în cazul rețelelor de socializare. Opinie cu privire la dezlegarea unei chestiuni de drept în materie penală. <https://www.juridice.ro/699938/despre-limitele-falsului-informatic-in-cazul-retelelor-de-socializare-opinie-cu-privire-la-dezlegarea-unei-chestiuni-de-drept-in-materie-penala.html#_ftn1>

Proiectul legii pentru modificarea şi completarea unor acte legislative (Legea privind Serviciul de Informaţii şi Securitate al RM – art.7; Codul penal – art.178, 2081, 259, ş.a.; ş.a.). <http://www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/3183/language/ro-RO/Default.aspx>

Rotru C., Trandafir A.-R., Cioclei V. Drept penal. Partea specială II. Curs tematic. București: C.H.Beck, 2019.

Лысак Е.А. Проблемы квалификациипреступлений в сферекомпьютерной информации. În: Научный журнал КубГАУ, №90(06), 2013, p.4 <http://ej.kubagro.ru/2013/06/pdf/48.pdf>

Рагулина А.B. Компьютерноемошенничество. În: Пробелы в российском законодательстве, nr.5, 2016, p.42.

1. Copetchi, S.Infracţiunile informatice potrivit legii penale moldave: studiu de drept penal comparat şi propuneri de lege ferenda. În: Culegerea comunicărilor Conferinţa ştiinţifică naţională cu participare Internaţională: “Realităţi şi perspective ale învăţământului juridic naţional”, Volumul II, 01-02 octombrie 2019, p.33 [↑](#footnote-ref-1)
2. Convenţia Consiliului Europei privind criminalitatea informatică de la Budapesta din 23.11.2001 [Accesat 20.08.2020] Disponibil: <http://legislatie.just.ro/Public/DetaliiDocumentAfis/51289> [↑](#footnote-ref-2)
3. Лысак Е.А. Проблемы квалификации преступлений в сфере компьютерной информации. În: Научный журнал КубГАУ, №90(06), 2013, p.4 <http://ej.kubagro.ru/2013/06/pdf/48.pdf> [↑](#footnote-ref-3)
4. #### Hotărârea Guvernului Republicii Moldova privind aprobarea cuantumului salariului mediu lunar pe economie, prognozat pentru anul 2021, nr.923 din 22.12.2020. În: Monitorul Oficial al Republicii Moldova, nr.359-923 din 31.12.2019

 [↑](#footnote-ref-4)
5. Copeţchi S. Op. cit., p.35 [↑](#footnote-ref-5)
6. Explanatory Report to the Convention on Cybercrime.Budapest, 23.XI.2001. European Treaty Series, No.185 <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016800cce5b> [↑](#footnote-ref-6)
7. Directiva 2013/40/UE a Parlamentului European şi a Consiliului privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului din 12 august 2013. <https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=RO> [↑](#footnote-ref-7)
8. Codul contravențional al Republicii Moldova, adoptat de Parlamentul Republicii Moldova la 24.10.2008. În: Monitorul Oficial al Republicii Moldova, 2017, nr.78-84 [↑](#footnote-ref-8)
9. Dobrinoiu, M. Infracțiuni în domeniul informatic. București: C.H.Beck, 2006, p.159 [↑](#footnote-ref-9)
10. Reniță Gh. *Controverse legate de răspunderea penală pentru manipularea unui eveniment și pariurile aranjate săvârșite în cyberspațiu*. În: Revista științifică a USM „Studia Universitatis Moldaviae”, Seria „Științe sociale”, 2017, nr. 8(108), p. 234. [↑](#footnote-ref-10)
11. Proiectul legii pentru modificarea şi completarea unor acte legislative (Legea privind Serviciul de Informaţii şi Securitate al RM – art.7; Codul penal – art.178, 2081, 259, ş.a.; ş.a.). <http://www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/3183/language/ro-RO/Default.aspx> [↑](#footnote-ref-11)
12. Copetchi, S. Op.cit., p.36 [↑](#footnote-ref-12)
13. Brînza S., Stati V. Tratat de Drept penal. Partea Specială. Volumul II. Chişinău: Tipografia Centrală, 2015, p. 358. [↑](#footnote-ref-13)
14. Brînza S., Stati V. Tratat de Drept penal. Partea Specială. Volumul I. Chişinău: Tipografia Centrală, 2015, p. 657 [↑](#footnote-ref-14)
15. Ibidem, p.56 [↑](#footnote-ref-15)
16. Brînza S., Stati V, p. 354. [↑](#footnote-ref-16)
17. *Ibidem.* [↑](#footnote-ref-17)
18. Copeţchi S. Op.cit., p.38 [↑](#footnote-ref-18)
19. Explanatory Report to the Convention on Cybercrime.Budapest, 23.XI.2001. European Treaty Series, No.185 <https://rm.coe.int/16800cce5b> [↑](#footnote-ref-19)
20. Decizia Curții Supreme de Justiție din 25 iunie 2014. Dosarul nr.1ra-1113/2014<http://jurisprudenta.csj.md/search_col_penal.php?id=2653> [↑](#footnote-ref-20)
21. # Pârgău D. Despre limitele falsului informatic în cazul rețelelor de socializare. Opinie cu privire la dezlegarea unei chestiuni de drept în materie penală. <https://www.juridice.ro/699938/despre-limitele-falsului-informatic-in-cazul-retelelor-de-socializare-opinie-cu-privire-la-dezlegarea-unei-chestiuni-de-drept-in-materie-penala.html#_ftn1>

 [↑](#footnote-ref-21)
22. Decizia Curții de Apel București, nr.1044/A din 08.08.2017http://www.rolii.ro/hotarari/59b88c86e49009740e000093 [↑](#footnote-ref-22)
23. Idem [↑](#footnote-ref-23)
24. Rotru C., Trandafir A.-R., Cioclei V. Drept penal. Partea specială II. Curs tematic. București: C.H.Beck, 2019, p.409 [↑](#footnote-ref-24)
25. Idem [↑](#footnote-ref-25)
26. Рагулина А.B. Компьютерноемошенничество. În: Пробелы в российском законодательстве, nr.5, 2016, p.42 [↑](#footnote-ref-26)
27. Cojocaru R. Escrocherii informaţionale: forme şi clarificări conceptuale ale cadrului normativ-penal de incriminare. În: Probleme de prevenire şi combatere a criminalităţii de către organele afcerilor interne în perioada recesiunii economice. Chişinău, 2010. p.19

<http://academy.police.md/assets/files/pdf/2009_15_octombrie_Recesiunea_economica.pdf> [↑](#footnote-ref-27)
28. Ibidem, p.20 [↑](#footnote-ref-28)
29. Brînza S., Stati V, Op.cit., p. 391 [↑](#footnote-ref-29)
30. Crijanovschi S. Unele aspecte privind analiza juridico-penală comparativă a infracţiunilor informatice în legea penală a Republicii Moldova şi cea a României. În: Studia Universitatis Moldavia. Seria „Ştiinţe Sociale”, 2016, nr.3(93), p. [↑](#footnote-ref-30)