# INFRACȚIUNILE INFORMATICE POTRIVIT LEGII PENALE MOLDAVE: STUDIU DE DREPT COMPARAT ȘI PROPUNERI *DE LEGE FERENDA*

*CYBERCRIMES IN ACCORDANCE WITH MOLDOVIAN CRIMINAL LAW: COMPARATIVE LAW STUDY AND THE LEGE FERENDA PROPOSALS*

**Stanislav COPEȚCHI,** dr., conf. univ.,
Universitatea de Stat din Moldova

**Abstract:** In the present study are analyzed, from a comparative perspective, some cyber crimes provided in Chapter XI of the Special Part of the Penal Code of the Republic of Moldova (PC RM). The offenses provided in art. 259, 260 and 260[1] PC RM were investigated, in accordance with the Convention of the Council of Europe on cybercrime, signed on 23.11.2001, in Budapest, as well as with the criminal laws of some foreign states: Romania, Russia, Armenia, Georgia, Bulgaria, Albania, Finland, Croatia, France etc. It is concluded that the incrimination norms provided in articles 259, 260 and 260[1] PC RM suffer from serious deficiencies. In this regard, taking into account the good legislative practices in this matter are submitted some proposals for amending these norms.

***Cuvinte-cheie****: infracţiune informatică, acces ilegal, informaţie computerizată, interceptare, sistem informatic, date informatice, perturbare, alterare, parole, coduri de acces, produse program, fals informatic, fraudă informatică, distrugere, modificare, blocare, ştergere, copiere.*

Preliminar consemnăm că, datele statistice demonstrează că Republica Moldova se află la o fază relativ incipientă în combaterea crimelor informatice. Acest lucru rezultă foarte clar reieşind din statistica oferită de Procuratura Generale a Republicii Moldova [1] pentru anul 2018, în corespundere cu care, pe parcursul acestuia an, în baza art.259-261 CP RM [2] (norme care stabilesc răspunderea penală pentru infracţiunile informatice) au fost pornite doar 15 cauze penale.

Mai exact, în baza art.259 CP RM (accesul ilegal la informaţia computerizată) a fost pornită o singură cauză penală; în baza art.260 CP RM (producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau a produselor program) – o cauză penală; în baza art.260[1] CP RM (interceptarea ilegală a unei transmisii de date informatice) – o cauză penală; în baza art.260[2] CP RM (alterarea integrităţii datelor informatice ţinute într-un sistem informatic) – nici o cauză penală; în baza art.260[3] CP RM (perturbarea funcţionării sistemului informatic) – două cauze penale; în baza art.260[4] CP RM (producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similare) – nici o cauză penală; în baza art.260[5] CP RM (falsul

informatic) – două cauze penale; în baza art.$260^6$ CP RM (frauda informatică) – şase cauze penale şi în baza art.261 CP RM (încălcarea regulilor de securitate a sistemului informatic) – două cauze penale.

Considerăm că, una din cauzele vitezei de reacţie a organelor competente ale statului în combaterea infracţiunilor informatice, îl constituie (de ce nu?) cadrul incriminator imperfect consacrat la art.259-261 CP RM. În special, avem în vedere infracţiunile contra confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice (art.259-$260^4$ CP RM). Or, aşa cum se va vedea *infra*, acesta deraiază, în unele privinţe, de la instrumentele juridice internaţionale în această materie. Nu acelaşi lucru remarcăm în legislaţiile penale ale unor state străine care, în reglementarea unor comportamente infracţionale din sfera informatică, ţin să se alinieze la standardele internaţionale.

După această precizare, subliniem că la momentul adoptării noului Cod penal al Republicii Moldova (cel din redacţia anului 2002, în vigoare din 2003) Capitolul XI din Partea Specială a Codului penal stabilea răspunderea penală doar pentru săvârşirea a trei infracţiuni informatice (accesul ilegal la informaţia computerizată (art.259 CP RM), introducerea sau răspândirea programelor virulente pentru calculatoare (art.260 CP RM) şi fapta de încălcare a regulilor de securitate a sistemului informatic (art.261 CP RM)).

Ulterior, prin Legea Republicii Moldova pentru modificarea şi completarea Codului penal al Republicii Moldova, nr.278 din 18.12.2008 (în continuare – Legea RM nr.278/2008) [3] au mai fost introduse şase articole destinate incriminării unor fapte prejudiciabile în domeniul informaticii. Este vorba de: art.$260^1$ CP RM (interceptarea ilegală a unei transmisii de date informatice); art.$260^2$ CP RM (alterarea integrităţii datelor informatice ţinute într-un sistem informatic); art.$260^3$ CP RM (perturbarea funcţionării sistemului informatic); art.$260^4$ CP RM (producerea, importul, comercializarea sau punerea ilegală la dispoziţie a parolelor, codurilor de acces sau a datelor similare); art.$260^5$ CP RM (falsul informatic) şi art.$260^6$ CP RM (frauda informatică).

În acelaşi timp, art.260 CP RM care, până la momentul adoptării Legii RM nr.278/2008 incrimina fapta de „introducere sau răspândire a programelor virulente pentru calculatoare", a fost modificat, apărând în următoarea redacţie: „producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau a produselor program".

Sesizăm că incriminarea celor din urmă fapte infracţionale a fost rodul iniţierii de către Republica Moldova, la acel moment, a procedurii de ratificare a Convenţiei Consiliului Europei privind criminalitatea informatică, semnată la 23.11.2001, la Budapesta (în continuare – Convenţia de la Budapesta) [4], finisată prin adoptarea de către Parlamentul Republicii Moldova a Legii pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică, nr.6 din

02.02.2009 [5]. De menţionat că Convenţia de la Budapesta prevede următoarele infracţiuni în sfera informatică: la art.3 (interceptarea ilegală); la art.4 (afectarea integrităţii datelor); la art.5 (afectarea integrităţii sistemului); la art.6 (abuzurile asupra dispozitivelor); la art.7 (falsificarea informatică) şi la art.8 (frauda informatică).

Deşi asemenea fapte infracţionale nu erau cuprinse în noul Cod penal al Republicii Moldova în redacţia anului 2002, totuşi, unele fragmente incriminatorii erau prezente în vechiul Cod penal al Republicii Moldova (cel din redacţia anului 1961) [6].

Aşadar, Capitolul VI[1] din Partea Specială a Codului penal în redacţia anului 1961 întitulat „Infracţiuni în domeniul tehnologiilor informaţionale" prevedea răspunderea penală pentru săvârşirea următoarelor fapte: 1) accesul ilegal (nesancţionat) la informaţia computerizată; 2) însuşirea ilegală a informaţiei computerizate, precum şi interceptarea acesteia; 3) fabricarea sau desfacerea mijloacelor specifice în scopul obţinerii accesului ilegal (nesancţionat) la sistemul computerizat; 4) modificarea informaţiei computerizate; 5) sabotajul computerizat, adică nimicirea, blocarea, aducerea în stare inutilizabilă a informaţiei computerizate, scoaterea din funcţiune a utilajului computerizat, distrugerea sistemului computerizat; 6) crearea, utilizarea sau răspândirea programelor dăunătoare.

Comparativ cu vechiul model incriminator (cel consemnat în CP RM în redacţia anului 1961) noul model incriminator (cel din CP RM în redacţia anului 2002, dar de după completările operate prin Legea RM nr.278/2008 – atunci când au fost introduse cele şase articole) este mult mai evoluat. *Primo* – conţinutul normelor incriminatoare înscrise la art.259-261 CP RM pornesc de la principiile directoare de reglementare a conduitelor infracţionale din sfera informatică consacrate în textul Convenţiei de la Budapesta. *Secundo* – acesta nu incriminează fragmentar faptele prejudiciabile menite să lezeze integritatea datelor şi sistemelor informatice, aşa cum o făcea vechiul cadru legal, ci mult mai cuprinzător. De exemplu, în corespundere cu vechiul cadru legal nu conta care este scopul sau rezultatul real cauzat în urma modificării informaţiei computerizate. Aplicabil era de fiece dată art.176[4] CP RM (modificarea informaţiei computerizate).

În contrast, în corespundere cu noul cadru legal modificarea datelor informatice poate antrena răspunderea penală cel puţin în baza a patru norme de incriminare: a) alterarea integrităţii datelor informatice ţinute într-un sistem informatic (art.260[2] CP RM); b) perturbarea funcţionării sistemului informatic (art.260[3] CP RM); c) falsul informatic (art.260[5] CP RM); d) frauda informatică (art.260[6] CP RM). Aplicabilitatea uneia sau altei norme depinde de: **1)** scopul urmărit de făptuitor; **2)** rezultatul real cauzat. De exemplu, în ipoteza în care modificarea datelor informatice a generat în perturbarea funcţionării unui sistem informatic cele comise trebuie încadrate în baza art.260[3] CP RM (perturbarea funcţionării siste-

mului informatic). Dacă modificarea datelor informatice nu a dus la perturbarea funcţionării sistemului informatic, cele săvârşite trebuie apreciate drept alterare a integrităţii datelor informatice (art.$260^2$ CP RM). Evident, cu condiţia cauzării unor daune în proporţii mari.

De asemenea, dacă modificarea datelor informatice, rezultând date necorespunzătoare adevărului este făcută în scopul utilizării lor în vederea producerii unei consecinţe juridice cele comise trebuie catalogate drept fals informatic (art.$260^5$ CP RM). În opoziţie, dacă făptuitorul urmăreşte prin modificarea datelor informatice obţinerea unui beneficiu material cele săvârşite trebuie încadrate în baza art.$260^6$ CP RM (frauda informatică).

În altă ordine de idei, consemnăm că Convenţia de la Budapesta face distincţie între: **a)** infracţiunile împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice şi, **b)** infracţiunile informatice propriu-zise. La prima categorie sunt atribuite: accesarea ilegală; interceptarea ilegală; afectarea integrităţii datelor; afectarea integrităţii sistemului; abuzurile asupra dispozitivelor. În categoria infracţiunilor informatice propriu-zise sunt incluse: falsificarea informatică şi frauda informatică.

Observăm că din perspectiva tehnicii legislative legiuitorul moldav a decis să amplaseze toate infracţiunile sunt enunţate în cadrul Capitolului XI din Partea Specială a Codului penal „Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor".

În plan comparat, sesizăm şi alte poziţii legislative. De exemplu: legiuitorul român a decis să aleagă o altă cale. *In concreto*, acesta a decis să localizeze infracţiunile sus-indicate în trei capitole şi titluri diferite din Partea Specială a Codului penal. Mai exact, accesul ilegal la un sistem informatic, interceptarea ilegală a unei transmisii de date informatice, alterarea integrităţii datelor informatice, perturbarea funcţionării sistemelor informatice, transferul neautorizat de date informatice, precum şi operaţiunile ilegale cu dispozitive sau programe informatice (art.360-365 Cod penal) sunt amplasate în cadrul Capitolul VI „Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice" din Titlul VII „Infracţiuni contra siguranţei publice". În acelaşi timp, infracţiunea de fals informatic (art.325 Cod penal) a fost localizată în Capitolul III „Falsuri în înscrisuri" din Titlul V „Infracţiuni de fals", iar infracţiunea de fraudă informatică (art.249 Cod penal) a fost amplasată în cadrul Capitolului IV „Fraude comise prin sisteme informatice şi mijloace de plată electronice" din Titlul II „Infracţiuni contra patrimoniului". Deci, legiuitorul român a instituit un Capitol aparte destinat incriminării unor fapte infracţionale pasibile să lezeze integritatea sistemelor informatice şi a datelor informatice. În acelaşi timp, unele infracţiuni informatice a decis să le amplaseze în alte capitole şi titluri din Partea Specială a Codului penal.

În mod similar, observăm că şi legiuitorul bulgar a mers pe calea instituirii unui Capitol special dedicat infracţiunilor informatice (Capitolul IX „a" – Infracţiuni informatice). Totodată, unele infracţiuni informatice a decis să le înscrie în alte capitole, similar legiuitorului român. De exemplu, răspunderea penală pentru frauda informatică este prevăzută la alin.(2) art.212a Cod penal, norma enunţată fiind amplasată în cadrul Secţiunii IV „Înşelăciunea" din Capitolul V „Infracţiuni împotriva proprietăţii".

De asemenea, potrivit legislaţiei Albaniei infracţiunea de fraudă informatică (art.143b din Codul penal) [7] este amplasată în cadrul Secţiunii II „Despre fraude" din Capitolul III „Infracţiuni aferente proprietăţii sau sferei economice". În acelaşi timp, infracţiunea de fals informatic şi cea de acces ilegal la informaţia computerizată sunt localizate în cadrul Secţiunii VIII „Falsificarea de documente" din acelaşi Capitol III. Celelalte infracţiuni, corespondente celor de la art.260-260$^4$ CP RM (art.293/a-art.293/ç din Codul penal) sunt prevăzute în Secţiunea III „Infracţiuni împotriva ordinii publice şi securităţii publice" din cadrul Capitolului VIII „Infracţiuni împotriva autorităţilor de stat".

În altă ordine de idei, în continuare vom încerca să scoatem în evidenţă unele imperfecţiuni de care suferă (în viziunea noastră) normele înscrise în cadrul Capitolului XI din Partea Specială a Codului penal, şi, în special, normele consemnate la art.259, 260 şi 260$^4$ CP RM, inclusiv, din perspectivă comparată cu legislaţia penală a unor state străine.

Vom debuta cu infracţiunea de *acces ilegal la informaţia computerizată* (art.259 CP RM).

Judecând după structura laturii obiective sesizăm că fapta prejudiciabilă (*alias* – elementul material) a componenţei de infracţiune enunţate este formată din două acţiuni: 1) acţiunea principală constând în accesul ilegal la informaţia computerizată şi, 2) acţiunea secundară care poate lua una din următoarele forme cu caracter alternativ: a) distrugerea informaţiei, b) deteriorarea informaţiei, c) modificarea informaţiei, d) blocarea informaţiei, e) copierea informaţiei, f) dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice.

Pentru a fi în prezenţa acestei infracţiuni este necesar ca acţiunea principală să fie secundată de una din cele şase acţiuni secundare. În caz contrar, cele comise nu pot fi încadrate potrivit art.259 CP RM, drept acces ilegal la informaţia computerizată. Totuşi, cele comise trebuie catalogate drept tentativă la infracţiunea prevăzută la art.259 CP RM în ipoteza în care făptuitorul realizează acţiunea principală sub forma accesului ilegal la informaţia computerizată, dar din cauze independente de voinţa sa nu-i reuşeşte să realizeze acţiunea secundară (de exemplu: să distrugă sau să copieze informaţia etc.). Evident, aceasta dacă făptuitorul urmăreşte cauzarea unor daune în proporţii mari.

În plan comparat lucrurile stau puţin diferit. Mai exact, identificăm mai multe orientări cu privire la structura laturii obiective a infracţiunii de acces ilegal la informaţia computerizată.

Într-o primă orientare, în corespundere cu alin.(1) art.272 din Codul penal al Federaţiei Ruse [8], distrugerea, blocarea, modificarea sau copierea informaţiei formează urmarea prejudiciabilă, nu însă formele cu caracter alternativ de exprimare a acţiunii secundare. Acelaşi lucru e valabil în cazul art.361 din Codul penal al Ucrainei [9], art.251 din Codul penal al Armeniei [10], precum şi art.349 din Codul penal al Republicii Belarus [11].

Într-o altă orientare, remarcăm că distrugerea, modificarea, blocarea etc. a informaţiei computerizate nu apare nici pe post de acţiune secundară, nici în postura de urmare prejudiciabilă. De exemplu, în acord cu art.360 din Codul penal al României [12] răspunderea penală pentru fapta de acces ilegal la un sistem informatic este angajată doar pentru simplul acces, fără drept, la un sistem informatic, nefiind necesar ca fapta de acces ilegal la un sistem informatic să fie succedată de deteriorarea, modificarea, copierea informaţiei etc. sau să aibă drept consecinţă deteriorarea, modificarea, copierea informaţiei etc.

În corespundere cu legislaţia României, remarcăm totuşi că, dacă accesul ilegal la un sistem informatic este însoţit de modificarea sau deteriorarea datelor informatice cele comise vor forma concurs de infracţiuni între art.360 Cod penal şi art.362 (alterarea integrităţii datelor informatice) sau art.363 Cod penal (perturbarea funcţionării sistemelor informatice).

Similar legiuitorului român, cel bulgar şi georgian au decis, la fel, să prevadă răspunderea penală în formă consumată doar pentru simpla faptă de acces ilegal la datele informatice (alin.(1) art.319a din Codul penal al Bulgariei [13] şi, corespunzător, alin.(1) art.284 din Codul penal al Georgiei [14]). Acelaşi model legislativ este înscris la art.2 din Convenţia de la Budapesta.

Susţinem cel din urmă model. Considerăm suficientă simpla accesare ilegală a unui sistem informatic pentru a considera cele comise drept infracţiune consumată. Nu vedem de ce acţiunea de acces ilegal la informaţia computerizată ar trebui să fie succedată de deteriorarea, modificarea, blocarea sau copierea informaţiei ori să fi determinat deteriorarea, modificarea, blocarea sau copierea informaţiei. Or, celor din urmă acţiuni/consecinţe le pot fi atribuite aprecieri juridico-penale distincte. De exemplu: deteriorarea sau modificarea datelor informatice poate antrena răspunderea penală în baza art.$260^2$ CP RM (alterarea integrităţii datelor informatice ţinute într-un sistem informatic), în baza art.$260^3$ CP RM (perturbarea funcţionării sistemului informatic) sau în baza altor norme. În acelaşi timp, copierea informaţiei ar trebui să marcheze momentul epuizării infracţiunii, ci nu să constituie una din acţiunile secundare/urmare prejudiciabilă, aceasta deoarece nu orice acces ilegal la informaţia computerizată este însoţit de copierea acesteia.

În ceea ce ne priveşte, considerăm că pentru a fi lezate relaţiile sociale aflate în derivaţie organică cu confidenţialitatea, integritatea şi disponibilitatea datelor informatice este suficient ca făptuitorul să fi accesat ilegal asemenea date informatice. Realizarea unor acţiuni suplimentare (secundare cu caracter alternativ) nu ar trebui să conteze la încadrare potrivit art.259 CP RM, ci la individualizarea pedepsei sau, eventual, pentru încadrarea celor săvârşite în tiparul unei alte norme de incriminare. Tocmai din aceste raţiuni, considerăm că legiuitorul moldav ar trebui să-şi revadă poziţia sa la construirea conţinutului normei incriminatoare înscrise la art.259 CP RM, prin preluarea bunelor practici în materie. În acest sens, par a fi elocvente modelele legislative din legislaţiile penale ale Georgiei, Bulgariei şi României, aflate în consonanţă perfectă cu cel desprins din textul Convenţiei de la Budapesta.

Tot în conjunctura infracţiunii de acces ilegal la informaţia computerizată merită a fi remarcat şi următorul lucru: urmarea prejudiciabilă, precum şi legătura de cauzalitate dintre faptă şi urmarea prejudiciabilă reprezintă semne obligatorii ale componenţei de infracţiune specificate la art.259 CP RM. Mai exact, pentru a fi în prezenţa infracţiunii sub forma unui fapt consumat este necesar ca acţiunea prejudiciabilă să fi cauzat daune în proporţii mari proprietarului sau posesorului informaţiei computerizate, calculatorului sau sistemului informatic. Potrivit alin. (1) art.126 CP RM se consideră proporţii mari valoarea pagubei pricinuite de o persoană sau de un grup de persoane, care depăşeşte 20 de salarii medii lunare pe economie prognozate, stabilite prin hotărârea de Guvern în vigoare la momentul săvârşirii faptei.

O urmare prejudiciabilă similară identificăm în cazul art.349 din Codul penal al Bulgariei şi cel al art.251 din Codul penal al Armeniei.

Pe de altă parte, normele din legiuirile penale ale majorităţii statelor europene, ce incriminează accesul ilegal la sisteme informatice, nu prevăd urmarea prejudiciabilă în calitate de semn constitutiv. Este cazul legislaţiei României, Georgiei, Albaniei, Bulgariei, Croaţiei [15], Cehiei [16], Danemarcei [17], Ungariei [18], Olandei [19] etc.

La fel, nici norma incriminatoare-cadru din Convenţia de la Budapesta nu conţine vreo referire la cauzarea vreunei urmări prejudiciabile prin săvârşirea accesului ilegal la sisteme informatice. Şi de această dată considerăm mai reuşite cele din urmă modele incriminatorii. Considerăm mult prea blând modelul incriminator moldav, fiind unul mai puţin eficient în prevenirea şi combaterea faptelor de acces ilegal la sisteme informatice, acolo unde momentul consumării infracţiunii este transferat la o fază mult mai târzie – momentul cauzării unor daune în proporţii mari. Rezultă că, potrivit legislaţiei Republicii Moldova cele săvârşite nu pot fi încadrate conform art.259 CP RM ca şi fapt consumat, în ipoteza în care fapta prejudiciabilă nu generează cauzarea unor daune în proporţii mari. În lipsa

unor atare daune cele comise pot fi apreciate drept tentativă la infracţiunea de acces ilegal la informaţia computerizată (cu condiţia că făptuitorul a avut intenţia cauzării unor asemenea daune).

De consemnat că potrivit unui Proiect de Lege pentru modificarea şi completarea unor acte legislative, aflat pe masa Parlamentului Republicii Moldova încă din anul 2016 [20], este înaintată propunerea *de lege ferenda* de a exclude urmarea prejudiciabilă sub forma daunelor în proporţii mari din textul alin.(1) art.259 CP RM, urmând ca aceasta să apară pe post de circumstanţă agravantă la lit.h) alin.(2) art.259 CP RM. Susţinem propunerea legislativă avansată. Este neclară însă, cauza tergiversării transpunerii în realitate a respectivei iniţiative legislative.

În alt registru, subliniem că la art.260 CP RM este prevăzută răspunderea penală pentru „*producerea, importul, comercializarea sau punerea la dispoziţie, sub orice altă formă, în mod ilegal, a mijloacelor tehnice sau produselor program, concepute sau adaptate, în scopul săvârşirii uneia dintre infracţiunile prevăzute la art.237, 259, 260$^{1}$–260$^{3}$, 260$^{5}$ şi 260$^{6}$*”.

În acelaşi timp, la art.260$^{4}$ CP RM este incriminată „*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 în scopul săvârşirii uneia dintre infracţiunile prevăzute la art.237, 259, 260$^{1}$–260$^{3}$, 260$^{5}$ şi 260$^{6}$, dacă aceste acţiuni au cauzat daune în proporţii mari*”.

Din perspectivă comparată, în legislaţia României cele două infracţiuni sunt reunite şi incriminate în cadrul unui singur articol. Este vorba de art.365 din Codul penal întitulat „Operaţiuni ilegale cu dispozitive sau programe informatice”. În mod similar, în conformitate cu legislaţia Albaniei manipulările ilegale cu entităţile sus-indicate cad sub incidenţa uneia şi aceleiaşi norme – art.293/ç din Codul penal. Şi în Codul penal al Croaţiei cele două fapte sunt reunite sub egida unuia şi aceluiaşi articol (art.272 din Codul penal). Acelaşi lucru îl remarcăm în cazul legislaţiei Cehiei (secţiunea 231 din Codul penal), Franţei (art.323-3-1 din Codul penal) [21], Lituaniei (art.198$^{2}$ din Codul penal) [22] şi Olandei (secţiunea 139d din Codul penal).

Şi de această dată constatăm că, cele din urmă modele incriminatorii sunt mai reuşite ca cel moldav. *Infra* ne vom convinge de acest lucru.

*Primo* – nu este clar de ce legiuitorul moldav a decis să separe în cadrul unei norme distincte răspunderea penală pentru anumite operaţiuni ilegale cu mijloace tehnice sau produse program de răspunderea penală pentru anumite operaţiuni ilegale cu parole, cu coduri de acces sau cu alte date similare ce permit accesul total sau parţial la un sistem informatic. Or, instrumentul internaţional de bază în materia infracţiunilor informatice (Convenţia de la Budapesta) stabileşte în

cadrul unei singure norme răspunderea penală pentru operaţiunile realizate în privinţa entităţilor sus-indicate. Surprindem că cadrul legislativ moldav în această materie deviază de la cadrul model consacrat la alin.(1) art.6 din Convenţia de la Budapesta. *Per a contrario*, în cazul legislaţiilor penale române, albaneze, croate, cehe, franceze şi lituaniene nu sesizăm o atare neconcordanţă.

*Secundo* – apare neclar momentul stabilirii urmării prejudiciabile în calitate de semn constitutiv al infracţiunii prevăzute la art.$260^4$ CP RM. Aşadar, sesizăm că pentru a fi în prezenţa infracţiunii respective, în formă consumată, este necesar ca prin 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 în scopul săvârşirii uneia dintre infracţiunile prevăzute la art.237, 259, $260^1$–$260^3$, $260^5$ şi $260^6$, să se fi cauzat daune în proporţii mari. În contrast, o asemenea urmare prejudiciabilă lipseşte în cazul infracţiunii prevăzute la art.260 CP RM (producerea, importul, comercializarea sau punerea ilegală la dispoziţie a mijloacelor tehnice sau a produselor program). Respectiva faptă infracţională se consideră consumată din momentul săvârşirii cel puţin a unei singure acţiuni din cele enumerate de legiuitor în dispoziţia normei, neavând importanţă la încadrare faptul survenirii unor urmări prejudiciabile.

*Tertio* – este de neînţeles de ce legiuitorul moldav a mers pe calea instituirii unor semne circumstanţiale agravante în cazul producerii, importului, comercializării sau punerii ilegale la dispoziţie a parolelor, codurilor de acces sau a datelor similare (art.$260^4$ CP RM), dar nu a agravat răspunderea penală şi pentru operaţiunile ilegale realizate cu mijloace tehnice sau produse program (art.260 CP RM). În context, notăm că la alin.(2) art.$260^4$ CP RM sunt prevăzute următoarele circumstanţe agravante: a) din interes material; b) de două sau mai multe persoane; c) de un grup criminal organizat sau de o organizaţie criminală; d) care au cauzat daune în proporţii deosebit de mari.

Nu înţelegem această tratare diferenţiată a operaţiunilor realizate cu dispozitivele sus-enunţate. O atare diferenţiere lipseşte în legislaţia României, Albaniei, Croaţiei, Cehiei, Franţei şi Lituaniei. La fel, aceasta nu se regăseşte nici în textul art.6 din Convenţia de la Budapesta. Mai mult, Convenţia de la Budapesta, în general, sugerează statelor să considere drept fapte infracţionale în formă consumată abuzurile cu asemenea dispozitive, indiferent de faptul cauzării unor urmări prejudiciabile. De remarcat că acest lucru a fost urmărit de legiuitorul român, albanez, ceh, francez, lituanian şi cel croat, care au mers pe calea construirii unor componenţe de infracţiune fără rezultat.

Dar cel mai paradoxal e faptul că deşi cele două infracţiuni au o construcţie diferită din perspectiva laturii obiective, acestea au un regim sancţionator practic identic. În partea ce vizează sancţiunea pasibilă de aplicat persoanei juridice însă,

aceasta este mai aspră chiar în cazul infracţiunii formale (formată doar din fapta prejudiciabilă) şi mai blândă în cazul infracţiunii materiale (formată din faptă, urmare prejudiciabilă, precum şi legătură cauzală dintre faptă şi urmare prejudiciabilă). Aşadar, se observă că infracţiunea prevăzută la art.260 CP RM, deşi fiind una formală, beneficiază de un regim sancţionator mai aspru comparativ cu infracţiunea prevăzută la art.260[4] CP RM, care este una materială (*Notă: Norma de la art.260 CP RM conţine următoarele pedepse: „amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 4000 la 7000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate sau cu lichidarea întreprinderii". Pentru comparaţie semnalăm că norma de la art.260[4] CP RM cuprinde următoarele pedepse: „amendă în mărime de la 850 la 1350 unităţi convenţionale sau cu închisoare de la 2 la 5 ani, cu amendă, aplicată persoanei juridice, în mărime de la 2000 la 4000 unităţi convenţionale cu privarea de dreptul de a exercita o anumită activitate*").

Nu susţinem o asemenea abordare diferenţiată a regimului sancţionator al celor două fapte manifestat de legiuitorul moldav, fiind una absolut nejustificată şi, contrară Convenţiei-cadru în această materie.

În vederea lichidării carenţelor legislative reliefate *supra*, dar şi întru asigurarea unei coerenţe dintre reglementările interne şi cele înscrise la 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 entităţile sus-indicate; b) să excludă urmarea prejudiciabilă din structura laturii obiective a infracţiunii (avem în vedere actuala infracţiune prevăzută la art.260[4] CP RM).

Subliniem că în nici una din legislaţiile penale ale statelor străine studiate de noi normele de incriminare corespondente celei înscrise la art.260[4] CP RM nu cuprind componenţe de infracţiuni materiale. Doar în cazul unor legislaţii învederăm construcţia unor componenţe de rezultat, dar care apar pe post de componenţe calificative. Cu alte cuvinte, în legislaţia unor asemenea state, componenţa de infracţiune în varianta-tip este formală, şi doar în cadrul componenţei cu circumstanţe agravante urmarea prejudiciabilă evoluează în postura de semn constitutiv al componenţei de infracţiune. Este cazul alin.(2) art.361-1 din Codul penal al Ucrainei, lit.г) alin.(2) art.285 din Codul penal al Georgiei.

Prin urmare, considerăm că legiuitorul moldav ar putea include urmarea prejudiciabilă, însă doar pe post de semn circumstanţial agravant în cadrul componenţei de infracţiune, ci nu în cadrul componenţei de bază.

În fine, în contextul infracţiunilor prevăzute la art.260 şi 260[4] CP RM precizăm că legiuitorul moldav stabileşte răspunderea penală doar pentru următoarele acţiuni prejudiciabile: a) producerea, b) importul, c) comercializarea, d) punerea la dispoziţie, sub orice altă formă.

Remarcăm însă, că simpla posesie (deţinere) a acestor entităţi materiale/imateriale nu cade sub incidenţa art.260 sau art.260[4] CP RM. În condiţii neclare, legiuitorul moldav a decis să nu preia această modalitate normativă de exprimare a ilicitului penal din textul art.6 al Convenţiei de la Budapesta. Legiuitorii altor state însă, nu au admis această omisiune. De exemplu, o asemenea acţiune prejudiciabilă regăsim la alin.(2) art.365 din Codul penal al României, art.272 din Codul penal al Croaţiei, art.293/ç din Codul penal al Albaniei, secţiunea 9(b) din Capitolul XXXIV din Codul penal al Finlandei [23], secţiunea 231 din Codul penal al Cehiei, art.285 din Codul penal al Georgiei, secţiunea 139d din Codul penal al Olandei etc. Cu titlu *de lege ferenda* recomandăm şi legiuitorului nostru să insereze o asemenea acţiune prejudiciabilă în textul celor două norme.

**Referinţe bibliografice:**


1. Raport privind activitatea Procuraturii pentru anul 2018. Chişinău, 2019. În: http://procuratura.md/file/2019-03-05_Raportul%20Public%20activitatea%20Procuraturii%20Generale%20anul%202018.pdf (accesat: 20.09.2019)
2. Codul penal, adoptat de Parlamentul Republicii Moldova la 18.04.2002. În: Monitorul Oficial al Republicii Moldova, 2002, nr.128-129, republicat în Monitorul Oficial al Republicii Moldova, 2009, nr.72-74.
3. Legea Republicii Moldova pentru modificarea şi completarea Codului penal al Republicii Moldova, nr.278 din 18.12.2008. În: Monitorul Oficial al Republicii Moldova, 2009, nr.37-40.
4. Convenţia Consiliului Europei privind criminalitatea informatică, semnată la 23.11.2001, la Budapesta. În: https://legeaz.net/text-integral/conventia-de-la-budapesta-privind-criminaltiatea-informatica (accesat: 19.09.2019)
5. Legea Republicii Moldova pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică, nr.6 din 02.02.2009. În: Monitorul Oficial al Republicii Moldova, 2009, nr.37-40.
6. Codul penal al RSSM, nr.41 din 24.03.1961. În: http://www.legis.md/cautare/getResults?doc_id=95784&lang=ro (accesat: 19.09.2019)
7. Criminal Code of the Republic of Albania. În: https://www.legislationline.org/download/action/download/id/8235/file/Albania_CC_1995_am2017_en.pdf (accesat: 20.09.2019)
8. Уголовный кодекс Российской Федерации. În: Собрание Законодательства Российской Федерации, 1996, №25.
9. Уголовный кодекс Украины. În: https://meget.kiev.ua/kodeks/ugolovniy-kodeks/razdel-1-16/ (accesat: 19.09.2019)

10. Уголовный кодекс Республики Армения. În: http://www.parliament.am/legislation.php?sel=show&ID=1349&lang=rus&3#24 (accesat: 19.09.2019)
11. Уголовный кодекс Республики Беларусь. În: http://xn----ctbcgfviccvibf9bq8k.xn--90ais/statya-349 (accesat: 19.09.2019)
12. Codul penal al României în redacţia din 2009. În: Monitorul Oficial al României, 2009, nr.510.
13. Criminal Code of the Republic of Bulgaria. În: https://www.legislationline.org/download/action/download/id/7578/file/Bulgaria_Criminal_Code_1968_am2017_ENG.pdf (accesat: 20.09.2019)
14. Уголовный кодекс Грузии. În: https://matsne.gov.ge/ka/document/download/16426/143/ru/pdf (accesat: 19.09.2019)
15. Criminal Code of Croatia. În: https://www.legislationline.org/download/action/download/id/7896/file/Croatia_Criminal_Code_2011_en.pdf (accesat: 19.09.2019)
16. Criminal Code of the Czech Republic. În: https://www.legislationline.org/download/action/download/id/6370/file/Czech%20Republic_CC_2009_am2011_en.pdf (accesat: 20.09.2019)
17. Criminal Code of Denmark. În: https://www.legislationline.org/download/action/download/id/6372/file/Denmark_Criminal_Code_am2005_en.pdf (accesat: 20.09.2019)
18. Criminal Code of the Republic of Hungary. În: https://www.legislationline.org/download/action/download/id/5619/file/HUngary_Criminal_Code_of_2012_en.pdf (accesat: 20.09.2019)
19. Criminal Code of the Kingdom of Netherlands. În: https://www.legislationline.org/download/action/download/id/6415/file/Netherlands_CC_am2012_en.pdf (accesat: 20.09.2019)
20. Proiect de Lege pentru modificarea şi completarea unor acte legislative. În:file:///C:/Users/Alina/Downloads/161.2016.ro.pdf (accesat: 19.09.2019)
21. Criminal Code of the French Republic. În: https://www.legislationline.org/download/action/download/id/3316/file/France_Criminal%20Code%20updated%20on%2012-10-2005.pdf (accesat: 20.09.2019)
22. Criminal Code of Lithuania. În: https://www.legislationline.org/download/action/download/id/8272/file/Lithuania_CC_2000_am2017_en.pdf (accesat: 20.09.2019)
23. Criminal Code of the Republic of Finland. În: https://www.legislationline.org/download/action/download/id/6375/file/Finland_CC_1889_am2015_en.pdf (accesat: 20.09.2019)