UNIVERSITATEA DE STAT DIN MOLDOVA
FACULTATEA DE DREPT
ȘCOALA DOCTORALĂ DE ȘTIINȚE JURIDICE

Cu titlu de manuscris
C.Z.U.: 343.222:343.346.8(478)(043)

STRÎMBEANU ALEXANDRU

RĂSPUNDEREA PENALĂ PENTRU ACCESUL ILEGAL LA INFORMAŢIA COMPUTERIZATĂ

SPECIALITATEA 554.01 – DREPT PENAL ȘI EXECUȚIONAL PENAL

Teză de doctor în drept

Conducător științific: _____ BRÎNZA Serghei, doctor habilitat în drept, profesor universitar

Autor: _____

CHIȘINĂU, 2023

© STRÎMBEANU ALEXANDRU, 2023

CUPRINSUL

ADNOTARE **5**

LISTA ABREVIERILOR **8**

INTRODUCERE **11**

1. ABORDĂRI DOCTRINARE ȘI NORMATIVE PRIVIND RĂSPUNDEREA PENALĂ PENTRU ACCESUL ILEGAL LA INFORMAȚIA COMPUTERIZATĂ **21**

1.1. Analiza materialelor științifice privind răspunderea penală pentru accesul ilegal la informația computerizată, publicate în Republica Moldova 21

1.2. Analiza materialelor științifice privind răspunderea penală pentru accesul ilegal la informația computerizată, publicate peste hotare 38

1.3. Condiționarea socială și juridică a incriminării accesului ilegal la informația computerizată 63

1.4. Coerența sistemică dintre art. 259 CP RM și prevederile complementare din legislația națională 72

1.5. Analiza de drept comparat a reglementărilor cu privire la accesul ilegal la informația computerizată 76

1.6. Sinteza problematicii tratate și a rezultatelor obținute în Capitolul 1 90

2. ANALIZA DE DREPT PENAL A INFRACȚIUNILOR PREVĂZUTE LA ART. 259 CP RM **94**

2.1. Obiectul infracțiunilor prevăzute la art. 259 CP RM 94

2.1.1. Obiectul juridic al infracțiunilor prevăzute la art. 259 CP RM 94

2.1.2. Obiectul material (imaterial) al infracțiunilor prevăzute la art. 259 CP RM 117

2.1.3. Victima infracțiunilor prevăzute la art. 259 CP RM 155

2.2. Latura obiectivă a infracțiunilor prevăzute la art. 259 CP RM 169

2.2.1. Fapta prejudiciabilă în cazul infracțiunilor prevăzute la art. 259 CP RM 169

2.2.2. Momentul de consumare și urmările prejudiciabile în cazul infracțiunilor prevăzute la art. 259 CP RM 205

2.2.3. Tentativa și pregătirea în cazul infracțiunilor prevăzute la art. 259 CP RM 215

2.2.4. Legătura cauzală în cazul infracțiunilor prevăzute la art. 259 CP RM 224

2.3. Latura subiectivă a infracțiunilor prevăzute la art. 259 CP RM 226

2.3.1. Vinovăția manifestată în cazul infracțiunilor prevăzute la art. 259 CP RM 226

2.3.2. Motivul, scopul și emoțiile în cazul infracțiunilor prevăzute la art. 259 CP RM 230

2.4. Subiectul infracțiunilor prevăzute la art. 259 CP RM 233

2.4.1. Persoana fizică – subiect al infracțiunilor prevăzute la art. 259 CP RM 234
2.4.2. Persoana juridică – subiect al infracțiunilor prevăzute la art. 259 CP RM 236
2.4.3. Calitatea specială a subiectului infracțiunilor prevăzute la art. 259 CP RM 240
2.5. Circumstanțele agravante ale infracțiunilor prevăzute la art. 259 CP RM.....242
2.5.1. Săvârșirea infracțiunii de două sau mai multe persoane 243
2.5.2. Săvârșirea infracțiunii cu violarea sistemelor de protecţie 250
2.5.3. Săvârșirea infracțiunii cu conectarea la canalele de telecomunicaţii 256
2.5.4. Săvârșirea infracțiunii cu folosirea unor mijloace tehnice speciale 257
2.5.5. Săvârșirea infracțiunii cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice, în scopul săvârşirii uneia dintre infracţiunile prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6 CP RM.....259
2.5.6. Săvârșirea infracțiunii în privinţa informaţiei protejate de lege.....261
2.5.7. Săvârșirea infracțiunii din motive de prejudecată 265
2.5.8. Oportunitatea agravării răspunderii în cazul săvârșirii infracțiunii fie asupra unui sistem informatic care este parte integrantă a infrastructurii critice, fie în privința informației sensibile privind protecția infrastructurilor critice 267
2.6. Sinteza problematicii tratate și a rezultatelor obținute în Capitolul 2 273

3. REZULTATELE OBȚINUTE ÎN URMA ANALIZEI DE DREPT PENAL A INFRACȚIUNILOR PREVĂZUTE LA ART. 259 CP RM.....277
3.1. Rezultatele obținute în urma analizei de drept penal a obiectului infracțiunilor prevăzute la art. 259 CP RM.....277
3.2. Rezultatele obținute în urma analizei de drept penal a laturii obiective a infracțiunilor prevăzute la art. 259 CP RM 292
3.3. Rezultatele obținute în urma analizei de drept penal a laturii subiective a infracțiunilor prevăzute la art. 259 CP RM 314
3.4. Rezultatele obținute în urma analizei de drept penal a subiectului infracțiunilor prevăzute la art. 259 CP RM.....317
3.5. Rezultatele obținute în urma analizei de drept penal a circumstanțelor agravante ale infracțiunilor prevăzute la art. 259 CP RM 321
3.6. Sinteza problematicii tratate și a rezultatelor obținute în Capitolul 3 330
CONCLUZII ŞI RECOMANDĂRI 335
BIBLIOGRAFIE 345
DECLARAȚIA PRIVIND ASUMAREA RĂSPUNDERII 369
CV-UL AUTORULUI 370

ADNOTARE

Strîmbeanu Alexandru, „Răspunderea penală pentru accesul ilegal la informația computerizată”. Teză de doctorat în drept. Școala Doctorală de Științe Juridice a Universității de Stat din Moldova. Chișinău, 2023

Structura tezei: introducere, trei capitole, concluzii și recomandări, bibliografie din 406 de titluri. Rezultatele obținute sunt publicate în 21 lucrări științifice.

Cuvintele-cheie: acces ilegal; informație computerizată; date informatice; sistem informatic; rețea informatică; calculator; sisteme de protecție.

Scopul lucrării este de a investiga temeinic elementele constitutive și circumstanțele agravante ale infracțiunilor prevăzute la art. 259 CP RM, de a evidenția vulnerabilitățile ce caracterizează interpretarea și aplicarea acestui articol, precum și de a propune soluții menite să contribuie la perfecționarea mecanismului de contracarare prin mijloace penale a accesului ilegal la informaţia computerizată.

Obiectivele cercetării: investigarea viziunilor doctrinare cu privire la răspunderea pentru infracțiunile prevăzute la art. 259 CP RM; utilizarea potențialului, de care dispun reglementările naționale cu privire la accesul la informaţia computerizată, în procesul de interpretare a acestui articol; identificarea gradului de compatibilitate dintre art. 259 CP RM și reglementările de sorginte internațională privind interzicerea accesului ilegal la informaţia computerizată, etc.

Noutatea şi originalitatea științifică a tezei rezidă în aceea că a fost realizată o analiză temeinică, sub aspect juridico-penal, a faptelor incriminate în art. 259 CP RM. Noutatea ştiinţifică a rezultatelor cercetării constă, de asemenea, în învederarea unor concepţii controversate atestate în doctrina de specialitate, în examinarea acestora şi în expunerea propriei viziuni argumentate. Pe acest fundament au fost punctate concluzii şi recomandări necesare pentru îmbunătățirea calității art. 259 CP RM și a cadrului normativ adiacent.

Rezultatele obținute care contribuie la soluționarea unei probleme ştiinţifice importante: fundamentarea concepției de interpretare a art. 259 CP RM și de calificare a infracțiunilor în baza acestui articol fără a fi încălcat principiul legalității, această fundamentare având ca efect identificarea erorilor de aplicare a art. 259 CP RM și a defectelor ce caracterizează dispoziția acestui articol, astfel fiind creată baza teoretică necesară pentru a perfecționa practica de aplicare a art. 259 CP RM și pentru a îmbunătăți calitatea acestui articol.

Semnificaţia teoretică a tezei: a) redimensionarea apărării penale a relaţiilor sociale cu privire la accesul autorizat sau permis la informaţia computerizată; b) acumularea unui amplu material teoretic şi practic indispensabil pentru dezvoltarea unor direcţii actuale şi complexe ale investigării infracţiunilor prevăzute la art. 259 CP RM; c) caracterizarea detaliată a elementelor constitutive și a circumstanțelor agravante ale infracțiunilor prevăzute la art. 259 CP RM; d) identificarea neajunsurilor de care suferă dispoziția art. 259 CP RM și practica de aplicare a acestei dispoziții.

Valoarea aplicativă a tezei: a) interpretarea din perspective noi a prevederilor art. 259 CP RM contribuie la dezvoltarea discuţiei ştiinţifice privind stabilirea temeiului juridic al răspunderii penale pentru faptele incriminate în acest articol; b) analiza de drept comparat și analiza istorică a reglementărilor privind răspunderea pentru accesul ilegal la informația computerizată comportă o semnificaţie cognitivă în vederea perceperii esenței juridice şi sociale a infracţiunilor prevăzute la art. 259 CP RM, etc.

Implementarea rezultatelor științifice: în procesul de creaţie legislativă (în scopul înlăturării neajunsurilor ce caracterizează dispoziția art. 259 CP RM), în procesul educaţional (în scopul de sporire a nivelului de cunoștințe și deprinderi ale studenţilor de la facultăţile de drept din instituţiile de învăţământ superior, a audienţilor și beneficiarilor de instruire continuă din cadrul INJ) şi în activitatea ştiinţifică de perspectivă.

АННОТАЦИЯ

Стрымбяну Александру, «Уголовная ответственность за несанкционированный доступ к компьютерной информации». Диссертация на соискание научной степени доктора права. Докторальная школа юридических наук Государственного университета Молдовы. Кишинэу, 2023

Структура диссертации: введение, три главы, выводы и рекомендации, библиография из 406 названий. Достигнутые результаты опубликованы в 21 научных работах.

Ключевые слова: несанкционированный доступ; компьютерная информация; компьютерные данные; информационная система; компьютерная сеть; компьютер; системы защиты.

Цель работы: углубленное исследование состава и отягчающих обстоятельств преступлений, предусмотренных ст. 259 УК РМ, выделение уязвимостей, характеризующих толкование и применение данной статьи, а также предложение решений, необходимых в плане совершенствования механизма противодействия уголовно-правовыми средствами несанкционированному доступу к компьютерной информации.

Задачи исследования: изыскание доктринальных взглядов на ответственность за преступления, предусмотренные ст. 259 УК РМ; использование в процессе толкования данной статьи потенциала внутриправовых норм, регламентирующих доступ к компьютерной информации и др.

Научная новизна и оригинальность результатов исследования выражаются в проведении тщательного уголовно-правового анализа преступлений, предусмотренных ст. 259 УК РМ. Научная новизна результатов исследования заключается также в изложении некоторых спорных доктринальных воззрений, в их рассмотрении и в предложении собственного аргументированного мнения. На этом основании делаются выводы и рекомендации, необходимые для улучшения качества ст. 259 УК РМ и смежной нормативной базы.

Полученные результаты, способствующие решению особо значимой научной проблемы, разрешенной в рамках проведенного диссертационного исследования состоят в обосновании концепции толкования ст. 259 УК РМ и квалификации преступлений по этой статье с соблюдением принципа законности, с целью выявления ошибок в применении ст. 259 УК РМ и недостатков, характеризующих диспозицию данной статьи, тем самым способствуя созданию теоретической базы, необходимой для совершенствования практики применения ст. 259 УК РМ и для улучшения качества данной статьи.

Теоретическая значимость: а) переосмысление концепции уголовно-правовой охраны общественных отношений по поводу санкционированного или разрешенного доступа к компьютерной информации; б) накопление обширного теоретического и практического материала, необходимого для разработки актуальных и комплексных направлений исследования преступлений, предусмотренных ст. 259 УК РМ; в) подробная характеристика состава и отягчающих обстоятельств преступлений, предусмотренных ст. 259 УК РМ и т.д.

Практическая применяемость исследования: а) толкование с новых позиций положений ст. 259 УК РМ способствует развитию научной дискуссии относительно установления правовых основ уголовной ответственности за деяния, предусмотренные данной статьей; б) сравнительно-правовой и исторический анализ норм об ответственности за несанкционированный доступ к компьютерной информации имеют познавательное значение для постижения правовой и социальной сущности преступлений, предусмотренных ст. 259 УК РМ и т.д.

Апробация результатов диссертационного исследования: в процессе законотворчества (в целях устранения недостатков ст. 259 УК РМ), в образовательном процессе (в целях повышения уровня знаний и навыков студентов юридических факультетов высших учебных заведений, слушателей и бенефициаров непрерывного образования в рамках НИЮ) и в перспективной научной деятельности.

ANNOTATION

Strimbeanu Alexandru, "Criminal liability for illegal access to computerized information". PhD in Law thesis. Doctoral School of Legal Sciences of the State University of Moldova. Chișinău, 2023

The structure of the thesis: introduction, three chapters, conclusions and recommendations, bibliography of 406 titles. The results achieved are published in 21 scientific papers.

Key-words: illegal access; computerized information; computer data; information system; computer network; computer; protection systems.

The purpose of the Ph.D. thesis is to thoroughly investigate the constituent elements and aggravating circumstances of the crimes provided by the art. 259 CrC RM, to highlight the vulnerabilities that characterize the interpretation and application of this article, as well as to propose solutions intended to contribute to the improvement of the mechanism of counteracting by criminal means illegal access to computerized information.

The objectives of investigation: investigating the doctrinal views regarding the liability for the crimes provided by the art. 259 CrC RM; the use of the potential, available in national regulations regarding access to computerized information, in the process of interpreting this article; identifying the degree of compatibility between art. 259 CrC RM and regulations of international origin regarding the prohibition of illegal access to computerized information, etc.

The scientific novelty and originality of the obtained results are expressed in a thorough criminal law analysis of crimes provided by the art. 259 CrC RM. The scientific novelty of the research results also consists in the examination of some controversial concepts attested in the specialized doctrine, in their examination and in the exposition of one's own reasoned vision. On this basis, conclusions and recommendations that are made are necessary to improve the quality of the art. 259 CrC RM and the related regulatory framework.

The obtained results which contribute solving of the foremost scientific problem: substantiation of the concept of interpretation of art. 259 CrC RM and the qualification of crimes in accordance with this article without violating the principle of legality, this substantiation having the effect of identifying errors in the application of art. 259 CrC RM and the defects that characterize the provision of this article, thus creating the theoretical basis necessary to perfect the practice of applying art. 259 CrC RM and to improve the quality of this article.

Theoretical importance: a) the resizing of the criminal defense of social relations regarding authorized or permitted access to computerized information; b) the accumulation of ample theoretical and practical material indispensable for the development of current and complex directions of the investigation of crimes provided by the art. 259 CrC RM; c) detailed characterization of the constitutive elements and aggravating circumstances of the crimes provided by the art. 259 CrC RM; d) identifying the shortcomings that characterize the provision of art. 259 CrC RM and the practice of applying this provision.

Practical value of the research paper: a) the interpretation from new perspectives of the provisions of art. 259 CrC RM contributes to the development of the scientific discussion regarding the establishment of the legal basis of criminal liability for the acts incriminated in this article; b) the analysis of comparative law and the historical analysis of the regulations regarding liability for illegal access to computerized information have a cognitive significance in order to perceive the legal and social essence of the crimes provided for in art. 259 CrC RM, etc.

Implementation of the scientific results: in the process of legislative creation (in order to remove the shortcomings that characterize the provision of art. 259 of the Criminal Code of the Republic of Moldova), in the educational process (in order to increase the level of knowledge and skills of students from law faculties in higher education institutions, of the audients and beneficiaries of continuous training from the NIJ) and in perspective scientific activity.

LISTA ABREVIERILOR

alin. – alineat

ANRCETI – Agenţia Naţională pentru Reglementare în Comunicaţii Electronice şi Tehnologia Informaţiei

art. – articol

BNM – Banca Națională a Moldovei

CCCECI – Comitetul Convenției Consiliului Europei privind criminalitatea informatică

CC RM – Codul contravențional al Republicii Moldova

CrC RM – Criminal Code of the Republic of Moldova

CEDO – Curtea Europeană a Drepturilor Omului

CNPF – Comisia Națională a Pieței Financiare

Convenția de la Budapesta – Convenţia Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23.11.2001

CP FR – Codul penal al Federației Ruse

CPG – Codul penal al Georgiei

CPGr – Codul penal al Greciei

CP MDL – Codul penal al Marelui Ducat de Luxemburg

CP RA – Codul penal al Republicii Austria

CP RBe – Codul penal al Republicii Belarus

CP RBl – Codul penal al Regatului Belgiei

CP RBu – Codul penal al Republicii Bulgaria

CP RCe – Codul penal al Republicii Cehe

CP RCi – Codul penal al Republicii Cipriote

CP RCr – Codul penal al Republicii Croaţia

CP RD – Codul penal al Regatului Danemarcei

CP RE – Codul penal al Republicii Estonia

CP RFG – Codul penal al Republicii Federale Germania

CP RFi – Codul penal al Republicii Finlanda

CP RFr – Codul penal al Republicii Franceze

CP RI – Codul penal al Republicii Italia

CP RLe – Codul penal al Republicii Letonia

CP RLi – Codul penal al Republicii Lituania

CP RM – Codul penal al Republicii Moldova din 18.04.2002

CP RM din 1961 – Codul penal al Republicii Moldova din 24.04.2002

CP RMa – Codul penal al Republicii Malta

CP RP – Codul penal al Republicii Polone

CP RSl – Codul penal al Republicii Slovace

CP RSlo – Codul penal al Republicii Slovenia

CP RSp – Codul penal al Regatului Spaniei

CP RSu – Codul penal al Regatului Suediei

CP RȚJ(O) – Codul penal al Regatului Ţărilor de Jos (Olanda)

CPR – Codul penal al României din 17.07.2009

CPU – Codul penal al Ucrainei

CPUn – Codul penal al Ungariei

CSJ – Curtea Supremă de Justiție

Directiva 2013/40/UE – Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului

evid. ns. – evidențierea noastră

INJ – Institutul Național al Justiției

Legea nr. 20/2009 – Legea nr. 20 din 03.02.2009 privind prevenirea şi combaterea criminalităţii informatice

Legea nr. 467/2003 – Legea nr. 467 din 21.11.2003 cu privire la informatizare şi la resursele informaţionale de stat

Legea nr. 1069/2000 – Legea nr. 1069 din 22.06.2000 cu privire la informatică

Legea României nr. 161/2003 – Legea României nr. 161 din 19.04.2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităților publice, a funcţiilor publice și în mediul de afaceri, prevenirea şi sancţionarea corupţiei

lit. – literă

n.a. – nota autorului

NIJ – National Institute of Justice

ONU – Organizația Națiunilor Unite

p. – pagină

parag. – paragraf

pct. – punct

secț. – secțiune

SIS – Serviciul de Informații și Securitate

subpct. – subpunct

subsecț. – subsecțiune

UE – Uniunea Europeană

vol. – volum

НИЮ – Национальный Институт Юстиции

УК РМ – Уголовный кодекс Республики Молдова

INTRODUCERE

Actualitatea și importanța temei abordate.

Incriminarea accesului ilegal la informația computerizată în legea penală a Republicii Moldova a fost determinată de apariția în anii 80' ai secolului trecut în societatea autohtonă a relațiilor privind accesul la informaţia computerizată. Apariția acestor relații a marcat tranziția în țara noastră de la o societate postindustrială spre o societate informaţională. După dezvoltarea acestor relații, s-a constatat că existența unor reglementări extrapenale cu privire la accesul la informaţia computerizată nu este suficientă pentru dezvoltarea și desfășurarea în condiții de siguranță a relațiilor sociale referitoare la accesul permis sau autorizat la informaţia computerizată. Informația computerizată a dobândit în scurt timp statutul de resursă cu o semnificație tot mai mare. În aceste condiții, a apărut necesitatea de a asigura accesul autorizat sau permis la informaţia computerizată prin măsuri adecvate de protecție împotriva ilegalităților caracterizate printr-un pericol social sporit. În consecință, abia în anul 2002, în Codul penal al Republicii Moldova din 1961 (în continuare – CP RM din 1961) a apărut art. 176[1] „Accesul ilegal (nesancţionat) la informaţia computerizată”.[1] Mai târziu, în Codul penal în vigoare al Republicii Moldova (în continuare – CP RM), fapta de acces ilegal la informația computerizată a fost incriminată în articolul 259.[2]

Interpretarea și aplicarea pe parcursul a două decenii a art. 259 CP RM a demonstrat că acesta nu este adaptat în mare parte la provocările sociale curente și, de aceea, nu permite apărarea eficientă a relațiilor sociale referitoare la accesul permis sau autorizat la informaţia computerizată. Constatăm că în Republica Moldova nu există o politică penală în domeniul prevenirii și combaterii accesului ilegal la informația computerizată. Neajunsurile, de care suferă art. 259 CP RM, au un impact negativ atât asupra interpretării și aplicării în practică a art. 259 CP RM, cât și asupra aportului adus de Republica Moldova în prevenirea și combaterea de către comunitatea internațională a infracțiunilor informatice. Art. 259 CP RM și-a epuizat potențialul preventiv și cel punitiv. Prin urmare, devine stringentă analiza profundă a problemelor legate de interpretarea și aplicarea acestui articol, precum și propunerea de soluții menite să contribuie la funcționarea eficientă a mecanismului de combatere și prevenire a accesului ilegal la informația computerizată.

---

[1] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.

[2] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

Încadrarea temei în preocupările internaţionale. Odată cu apariția primului calculator, mediul informatic a devenit o parte vulnerabilă a sistemului internațional de securitate. Tranziția de la o societate postindustrială spre o societate informațională a avut ca efect globalizarea și transnaționalizarea informației computerizate. O astfel de informație poate să prezinte semnificație atât pentru un singur individ, cât și pentru stat și societate în ansamblu. Ca urmare, infracțiunile informatice, în general, și accesul ilegal la informația computerizată, în particular, afectează securitatea nu doar la nivel național, ci și la nivel internațional. Datorită acestui fapt, cooperarea internațională în domeniul prevenirii și combaterii acestor infracțiuni capătă o importantă deosebită.

Conform alin. (2) art. 6 al Legii nr. 1069 din 22.06.2000 cu privire la informatică (în continuare – Legii nr. 1069/2000), „pentru Republica Moldova, relaţiile internaţionale în domeniul informaticii se reglementează prin convenţii şi acorduri internaţionale la care aceasta este parte. [...].”[3] În acest context se înscrie Convenţia Consiliului Europei privind criminalitatea informatică, care a fost adoptată la Budapesta la 23.11.2001[4] (în continuare – Convenția de la Budapesta), care a fost ratificată prin Legea nr. 6 din 02.02.2009 pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică.[5] Potrivit art. 2 din acest act, „fiecare parte va adopta [...] măsuri [...] pentru a incrimina ca infracțiune, potrivit dreptului său intern, accesarea intenționată și fără drept a [...] unui sistem informatic.”[6] Conform aceluiași articol, este posibil ca incriminarea unei asemenea fapte poate fi determinată „de comiterea încălcării respective prin violarea măsurilor de securitate, [...] cu [...] intenție delictuală [...].”[7]

În același context, vorbim despre Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului (în continuare – Directiva 2013/40/UE). În preambulul acestei directive se menționează, între altele: „Se impune adoptarea unei abordări comune față de elementele constitutive ale infracțiunilor, incriminând ca infracțiuni de drept comun accesarea ilegală a unui sistem informatic [...].”[8]; „Statele membre ar trebui să prevadă sancțiuni pentru atacurile împotriva sistemelor informatice [, care] să fie eficace, proporționale și

---

[3] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[4] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[5] Legea pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică: nr. 6 din 02.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 37-40, 104.
[6] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[7] *Ibidem*.
[8] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en

disuasive [...]”[9]. În conformitate cu art. 3 al Directivei 2013/40/UE, „[...] accesarea cu intenție și fără drept a unui sistem informatic [...] este incriminată atunci când este săvârșită prin încălcarea unei măsuri de securitate [...].”[10] Bineînțeles, astfel de prevederi trebuie privite prin prisma Hotărârii Guvernului nr. 1171 din 28.11.2018 pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația UE. Conform pct. 2 al acestei hotărâri, „armonizarea legislației Republicii Moldova cu legislația UE [...] are drept scop integrarea în ordinea juridică internă a legislației UE [...].”[11]

Conform alin. (2) art. 6 al Legii nr. 1069/2000), „[...] în cazul în care convenţiile [...] internaţionale conţin alte norme decât cele prevăzute de legislaţia Republicii Moldova cu privire la informatică, se aplică prevederile [...] internaţionale.”[12] Totuși, niciuna dintre normele de drept internațional, care conține recomandarea de incriminare a accesului ilegal la informația computerizată, nu este de aplicare directă. Legiuitorul moldovean a adaptat aceste norme într-o manieră nu tocmai reușită, fapt demonstrat de calitatea mediocră a art. 259 CP RM. În consecință, în procesul de perfecționare a art. 259 CP RM, unul dintre reperele principale ar trebui să-l constituie litera și spiritul reglementărilor internaționale privind interzicerea accesului ilegal la informaţia computerizată.

Încadrarea temei în preocupările naţionale și zonale. Am inițiat demersul științific având ca suport materialele la tema tezei, dedicate aspectelor de drept penal ale infracțiunilor prevăzute la art. 259 CP RM, care au fost publicate de către: S. Bacinschi; A. Barbăneagră; A. Borodac; M. Botnarenco; S. Brînza; S. Copețchi; S. Crijanovschi; L. Dumneanu; M. Gheorghiță; A. Ghimpu; L. Gîrla; R. Gojan; S. Grișciuc-Bucica; D. Gurev; N. Lazareva; A. Pareniuc; A. Smochină; V. Soltan; Iu. Stan; V. Stati, etc. (Republica Moldova); Gh. Alecu; V. Coman; S. Corlățeanu; A. Crăciunescu; V. Dobrin; M. Dobrinoiu; A.T. Drăgan; M. Dunea; C. Duvac; G. Florescu, V. Florescu; M. Gorunescu; A.V. Iugan; L.C. Kövesi; C. Manea; C. Marin; T. Medeanu; A.C. Moise; C. Moțoc; N. Niță; R.A. Nestor; F.-V. Onofrei; Z. Sadâc; P. Tamas-Erno; O. Vară; G. Zlati, etc. (România); P.P. Andrușko; D.S. Azarov; S.Ia. Burda; M.V. Karcevski; N.S. Kozak; Iu.V. Oriol; D.O. Ricika; N.A. Rozenfeld; A.Ia. Skiba; T.I. Sozanski; A.V. Zaghika, etc. (Ucraina); T.A. Abramean; O.Ia. Baev; I.R. Beghișev; A.M. Doronin; M.Iu. Dvorețki; M.A. Efremova; R.R. Gaifutdinov; A.A. Grebenkov; O.S. Guzeeva; Z.I. Hisamova; L.V. Ivanova;

[9] Ibidem.
[10] Ibidem.
[11] Hotărârea Guvernului pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene: nr. 1171 din 28.11.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 499-503, 1314.
[12] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

D.G. Malâșenko; V.A. Meșcereakov; G.P. Novosiolov; O.S. Ozerova; A.N. Popov; E.A. Russkevici; O.M. Safonov; M.V. Staricikov; V.G. Stepanov-Eghianț; A.V. Susloparov; A.E. Șarkov; A.V. Șulga; T.L. Tropina; M.A. Zubova, etc. (Federația Rusă); N.F. Ahramenka; O.I. Bahur; L.I. Gasan; A.I. Lukașov; O.G. Nikitenko; N.A. Sivițkaia; N.A. Șved; Iu.N. Tanana, etc. (Republica Belarus); A.B. Bekmagambetov; I.Ș. Borceașvili; A.M. Galiaskarova; A.T. Ismagulova; V.P. Revin; V.V. Revina, etc. (Republica Kazahstan); I.B.O. Agaev; G.S.O. Kurbanov, etc. (Republica Azerbaidjan), etc.

Încadrarea temei în preocupările colectivului de cercetare. În cadrul Departamentului Drept penal din cadrul Facultății de Drept a Universității de Stat din Moldova se remarcă un grup relativ numeros de cercetători care au elaborat lucrări ce vizează răspunderea penală pentru accesul ilegal la informația computerizată: M. Botnarenco; S. Brînza; S. Copețchi; L. Dumneanu; L. Gîrla; D. Gurev și V. Stati.

Încadrarea temei în în context inter- și transdisciplinar. Am inițiat demersul științific având ca suport, de asemenea, materialele la tema tezei, publicate de către autorii unor lucrări din domeniul dreptului constituțional, dreptului procesual penal, dreptului informațional, dreptului informatic, dreptului securității naționale, dreptului civil, dreptului proprietății intelectuale, criminologiei, criminalisticii, informaticii etc.: R. Abrihan; T. Anghel; L. Băjenaru; N. Chirpat; O. Cerbu; N.-G. Drăgulănescu; I.-T. Gigi; C. Hlopeatnicov; Gh.Iu. Ioniță; G.-I. Luncan; R.-L. Lupșa; A. Munteanu; R.N. Popescu; Iu. Rusu; D. Savu; V. Sîli; I. Soroceanu; C.O. Șofran; A.-M. Tîrziu; M. Tomescu; V. Țurcanu; I.R. Urs; I. Vasiu; L. Vasiu; M.A. Dubko; V.O. Kaleatin; A.D. Kos; Iu.V. Logvinov; V.N. Loktiuhin; V. Krâlov; S.G. Spirina; V.V. Strigunov, etc.

Prezentarea rezultatelor cercetărilor anterioare referitoare la tema aleasă. În Republica Moldova, printre oamenii de ştiinţă, preocupați de elaborarea concepţiei teoretice de soluţionare a problemei privind răspunderea penală pentru accesul ilegal la informaţia computerizată (art. 259 CP RM), trebuie evidențiați: A. Barbăneagră; A. Borodac; S. Brînza; S. Copețchi; L. Dumneanu; M. Gheorghiță; L. Gîrla; D. Gurev; V. Stati. Lucrările acestor autori au ca obiect fie întreaga gamă a elementelor constitutive și a circumstanțelor agravante ale infracțiunilor ce sunt specificate în art. 259 CP RM, fie anumite aspecte legate de calificarea infracțiunilor în baza art. 259 CP RM. În același timp, în astfel de lucrări se atestă, în unele cazuri, opinii divergente privitoare la: conținutul obiectului juridic generic, al obiectului juridic special și al obiectului material ori imaterial al infracţiunilor prevăzute în art. 259 CP RM; conținutul și structura laturii obiective a acestor infracțiuni; momentul de consumare a infracţiunilor prevăzute în art. 259 CP RM; tipul de intenție manifestată la comiterea infracțiunilor respective; calitatea specială a subiectului – persoană fizică și a subiectului – persoană juridică. Aceste diferențe de poziții

impulsionează discuția științifică, constituind un motiv determinant pentru a dezvolta investigarea științifică a întregului spectru de aspecte legate de răspunderea pentru infracţiunile prevăzute la art. 259 CP RM.

În cadrul studiului de față sunt analizate, de asemenea, materialele științifice publicate peste hotare ale savanților care și-au adus aportul la elaborarea concepţiei teoretice de soluţionare a problemei privind răspunderea penală pentru accesul ilegal la informaţia computerizată. Printre acești savanți se remarcă: D.S. Azarov; I.R. Beghișev; S.Ia. Burda; A. Crăciunescu; M. Dobrinoiu; A.M. Doronin; A.T. Drăgan; C. Duvac; G. Florescu; V. Florescu; L.C. Kövesi; C. Manea; T. Medeanu; A.N. Popov; D.O. Ricika; N.A. Rozenfeld; A.Ia. Skiba; T.I. Sozanski; V.G. Stepanov-Eghianț; G. Zlati etc. Investigațiile acestor autori sunt valoroase din perspectiva analizei comparative a infracțiunilor, prevăzute la art. 259 din Codul penal al Republicii Moldova, în raport cu infracțiunile prevăzute la: art. 360 din Codul penal al României[13] (în continuare – CPR); art. 361 din Codul penal al Ucrainei[14] (în continuare – CPU); art. 272 din Codul penal al Federației Ruse[15] (în continuare – CP FR), etc. În lucrările autorilor de peste hotare, menționați mai sus, se acordă atenție prioritară examinării elementelor constitutive (obiectul; latura obiectivă; latura subiectivă; subiectul) ale infracțiunilor de acces ilegal la informația computerizată. Desigur, ideile și concepțiile analizate pot fi luate în calcul în procesul de elaborare a concepţiei teoretice de soluţionare a problemei privind răspunderea pentru infracțiunile prevăzute la art. 259 din Codul penal al Republicii Moldova. În același timp, este important de reținut că o asemenea analiză trebuie să pornească de la premisa, conform căreia art. 360 CPR, art. 361 CPU, art. 272 CP FR etc. au un conținut diferit de cel al art. 259 CP RM. Neluarea în calcul a acestui factor ar putea avea ca efect obținerea unor rezultate științifice distorsionate cu privire la răspunderea pentru infracțiunile care sunt prevăzute de art. 259 CP RM.

Scopul lucrării este de a investiga temeinic elementele constitutive și circumstanțele agravante ale infracțiunilor prevăzute la art. 259 CP RM, de a evidenția vulnerabilitățile ce caracterizează aplicarea și interpretarea articolului respectiv, de a propune soluții menite să contribuie la perfecționarea mecanismului de contracarare prin mijloace penale a accesului ilegal la informaţia computerizată.

Obiectivele cercetării: investigarea viziunilor doctrinare cu privire la răspunderea pentru infracțiunile care sunt specificate în art. 259 CP RM; utilizarea potențialului, de care dispun

---

[13] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510

[14] *Кримінальний кодекс України*. [citat 18.12.2020] Disponibil: https://zakon.rada.gov.ua/laws/show/2341-14#Text

[15] Уголовный кодекс Российской Федерации. În: *Собрание законодательства Российской Федерации*, 1996, № 25.

reglementările naționale cu privire la accesul la informaţia computerizată, în procesul de interpretare a acestui articol; identificarea gradului de compatibilitate dintre art. 259 CP RM și reglementările de sorginte internațională privind interzicerea accesului ilegal la informaţia computerizată; studierea experienţei pozitive a altor state în planul prevenirii și combaterii prin mijloace penale a accesului ilegal la informaţia computerizată; stabilirea valorilor sociale apărate împotriva infracţiunilor ce sunt specificate în art. 259 CP RM; relevarea caracteristicilor obiectului material sau imaterial al infracţiunilor ce sunt specificate în acest articol; examinarea trăsăturilor particularizante ce caracterizează victima infracţiunilor de la art. 259 CP RM; stabilirea structurii și a conţinutului faptei prejudiciabile prevăzute de acest articol; relevarea urmărilor prejudiciabile şi a legăturii cauzale în cazul infracţiunilor de la art. 259 CP RM; pertractarea laturii subiective și a subiectului infracţiunilor prevăzute de acest articol; analiza circumstanțelor care agravează răspunderea pentru infracţiunile care sunt specificate în art. 259 CP RM; delimitarea infracțiunilor, care sunt specificate în art. 259 CP RM, de alte infracțiuni; investigarea vulnerabilităților ce caracterizează practica de aplicare a art. 259 CP RM, care este urmată de formularea de soluții; analiza neajunsurilor de natură tehnico-legislativă de care suferă dispoziţia art. 259 CP RM, ce este urmată de formularea de recomandări *de lege ferenda*.

Ipoteza de cercetare se bazează pe supoziția, conform căreia:

– incriminând faptele reunite sub denumirea marginală de acces ilegal la informaţia computerizată, legiuitorul urmărește să stabilească un echilibru rezonabil între dreptul unor persoane de a accesa în mod liber informația computerizată și dreptul altor persoane de a nu permite accesul ilegal la o asemenea informație;

– infracțiunile, ce sunt prevăzute în art. 259 CP RM, sunt infracțiuni biobiectuale, însă nu sunt infracțiuni complexe;

– în cazul infracțiunilor care sunt specificate în art. 259 CP RM, obiectul imaterial principal îl reprezintă informația computerizată. În cazul aceloraşi infracțiuni, informația computerizată distrusă, deteriorată, modificată, blocată sau copiată constituie obiectul imaterial secundar; calculatoarele, sistemul informatic sau reţeaua informatică, a căror funcționare a fost dereglată, formează obiectul material secundar;

– poziția față de structura laturii obiective a infracțiunilor, prevăzute în art. 259 CP RM, trebuie diferențiată în funcție de modalitățile normative ale acțiunii adiacente din cadrul faptei prejudiciabile;

– datorită structurii nereușite a laturii obiective a infracțiunilor care sunt prevăzute în art. 259 CP RM, lipsește posibilitatea de apărare penală eficientă a relaţiilor sociale cu privire la accesul autorizat sau permis la informaţia computerizată;

– este oportună agravarea răspunderii în cazul săvârșirii infracțiunilor, ce sunt prevăzute în art. 259 CP RM, fie asupra unui sistem informatic care este parte integrantă a infrastructurii critice, fie în privința informației sensibile privind protecția infrastructurilor critice.

Sinteza metodologiei de cercetare și justificarea metodelor de cercetare alese. Cercetările efectuate se întemeiază pe studierea doctrinei de specialitate, a legislației naționale penale și a celei extrapenale, a normelor de drept internațional, a reglementărilor UE, a jurisprudenței Curții Constituționale a Republicii Moldova și a Curții Constituționale a României, a practicii instanțelor judecătorești din Republica Moldova și din România.

În vederea realizării scopului și a obiectivelor relevate *supra*, au fost aplicate metoda logică (rațională), metoda istorică, metoda analizei sistemice și metoda comparativă.

Astfel, toate cele trei ipostaze – exegetic, dogmatic, critic – în care se înfățișează studiul art. 259 CP RM, implică utilizarea următoarelor categorii și legi ale logicii: definiția; specificarea și generalizarea; diviziunea și clasificarea; diferențierea și integrarea; analiza și sinteza; demonstrația; argumentarea; raționamentul, etc.

Din perspectivă istorică, a fost cercetat art. 176^1 CP RM din 1961. Din aceeași perspectivă, au fost investigate modificările și completările pe care art. 259 CP RM le-a suportat de-a lungul timpului.

Metoda analizei sistemice a fost aplicată întrucât art. 259 CP RM constituie o parte a unui sistem normativ integral al cărui elemente structurale sunt strâns legate între ele. Având în vedere aceste premise, putem afirma că, în sistemul normativ al Republicii Moldova, reglementările privind accesul la informația computerizată formează un sistem. Caracterul de referință (de blanchetă) al prevederilor art. 259 CP RM denotă că acesta poate fi interpretat și aplicat doar dacă este privit prin prisma reglementărilor extrapenale privind accesul la informația computerizată. Or, anumite noțiuni din art. 259 CP RM sunt definite în astfel de reglementări.

Ca punct de reper pentru analiza de drept comparat a servit cadrul penal în materie din Georgia, Grecia, Marele Ducat de Luxemburg, Regatul Belgiei, Regatul Danemarcei, Regatul Spaniei, Regatul Suediei, Regatul Ţărilor de Jos (Olanda), Republica Armenia, Republica Austria, Republica Belarus, Republica Bulgaria, Republica Cehă, Republica Cipriotă, Republica Croaţia, Republica Estonia, Republica Federală Germania, Republica Finlanda, Republica Franceză, Republica Italia, Republica Letonia, Republica Lituania, Republica Malta, Republica Polonă, Republica Portugheză, Republica Slovacă, Republica Slovenia, Regatul Spaniei, România, Ucraina, Ungaria etc.

Sumarul capitolelor tezei

Lucrarea de față este alcătuită din trei capitole. Fiecare dintre aceste capitole se încheie cu o secțiune de sinteză a rezultatelor, ce au fost obținute, precum și a problematicii tratate.

În Capitolul 1 – *Abordări doctrinare şi normative privind răspunderea penală pentru accesul ilegal la informaţia computerizată* – investigațiile efectuate s-au axat pe: materialele științifice privind răspunderea penală pentru accesul ilegal la informația computerizată, publicate în Republica Moldova și peste hotare; condiționarea socială și juridică a incriminării accesului ilegal la informația computerizată; coerența sistemică dintre art. 259 CP RM și reglementările complementare din cadrul legislației naționale; analiza de drept comparat a reglementărilor cu privire la accesul ilegal la informația computerizată.

Aceste investigații sunt necesare pentru stabilirea fundamentului doctrinar și normativ al concepţiei teoretice de soluţionare a problemei privind răspunderea pentru infracțiunile prevăzute în art. 259 CP RM. Printre obiectivele cercetării de față se numără: investigarea viziunilor doctrinare cu privire la răspunderea aplicată pentru infracțiunile ce sunt specificate în art. 259 CP RM; utilizarea potențialului, de care dispun reglementările naționale cu privire la accesul la informaţia computerizată, în procesul de interpretare a acestui articol; identificarea gradului de compatibilitate dintre art. 259 CP RM și reglementările de sorginte internațională privind interzicerea accesului ilegal la informaţia computerizată; studierea experienţei pozitive a altor state în planul prevenirii și combaterii prin mijloace penale a accesului ilegal la informaţia computerizată. Înfăptuirea acestor obiective este condiția pentru realizarea scopului prezentei teze în partea care se referă la investigarea temeinică a elementelor constitutive și a circumstanțelor agravante ale infracțiunilor ce sunt prevăzute în art. 259 CP RM, precum și la evidențierea precarităților ce vizează aplicarea și interpretarea acestui articol.

În Capitolul 2 – *Analiza de drept penal a infracțiunilor prevăzute la art. 259 CP RM* – cercetările efectuate s-au axat pe: obiectul infracțiunilor specificate în art. 259 CP RM (obiectul juridic, obiectul material (imaterial) și victima acestora); latura obiectivă a infracțiunilor prevăzute la art. 259 CP RM (fapta prejudiciabilă, momentul de consumare și urmările prejudiciabile în cazul acestora; tentativa și pregătirea în cazul infracțiunilor prevăzute la art. 259 CP RM; legătura cauzală în cazul acestora); latura subiectivă a infracțiunilor care sunt prevăzute de art. 259 CP RM (vinovăția manifestată în cazul acestora; motivul, scopul și emoțiile în cazul infracțiunilor care sunt specificate în art. 259 CP RM); subiectul infracțiunilor care sunt prevăzute de art. 259 CP RM (condițiile generale pe care le îndeplinește acest subiect; calitatea specială a subiectului infracțiunilor ce sunt prevăzute de art. 259 CP RM); circumstanțele agravante ale infracțiunilor ce sunt specificate în art. 259 CP RM (sub aspect *de lege lata*

(săvârșirea acestor infracțiuni: de două ori mai multe persoane; cu violarea sistemelor de protecţie; cu conectarea la canalele de telecomunicaţii; cu folosirea unor mijloace tehnice speciale; cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice, în scopul săvârşirii uneia dintre infracţiunile prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6 CP RM; în privinţa informaţiei protejate de lege); sub aspect *de lege ferenda* (oportunitatea agravării răspunderii în cazul săvârșirii infracțiunii fie asupra unui sistem informatic care este parte integrantă a infrastructurii critice, fie în privința informației sensibile privind protecția infrastructurilor critice)).

Aceste investigații se concretizează în aplicarea materialelor și a metodelor care sunt necesare în contextul analizei de drept penal a infracțiunilor ce sunt prevăzute de art. 259 CP RM. Printre obiectivele cercetării de față se numără: stabilirea valorilor sociale apărate împotriva infracţiunilor ce sunt prevăzute de art. 259 CP RM; relevarea caracteristicilor obiectului material sau imaterial al infracţiunilor prevăzute de acest articol; examinarea trăsăturilor particularizante ce caracterizează victima infracţiunilor care sunt prevăzute de art. 259 CP RM; stabilirea structurii și a conţinutului faptei prejudiciabile prevăzute de acest articol; relevarea urmărilor prejudiciabile şi a legăturii cauzale în cazul infracţiunilor care sunt prevăzute de art. 259 CP RM; pertractarea laturii subiective și a subiectului infracţiunilor prevăzute de acest articol; analiza circumstanțelor care agravează răspunderea pentru infracţiunile ce sunt prevăzute de art. 259 CP RM; delimitarea infracțiunilor, care sunt prevăzute de art. 259 CP RM, de alte infracțiuni; investigarea vulnerabilităților ce caracterizează practica de aplicare a art. 259 CP RM, ce este urmată de formularea de soluții; analiza neajunsurilor de natură tehnico-legislativă de care suferă dispoziţia art. 259 CP RM, ce este urmată de formularea de recomandări *de lege ferenda*. Înfăptuirea acestor obiective este condiția pentru realizarea *per ansamblu* a scopului prezentei teze.

Capitolul 3 – *Rezultatele obținute în urma analizei de drept penal a infracțiunilor prevăzute la art. 259 CP RM* – este axat pe contribuțiile personale ale autorului, inclusiv pe rezultatele originale obţinute de către autor.

Rezultatele, ce au fost obținute în urma analizei de drept penal a infracțiunilor prevăzute la art. 259 CP RM, sunt grupate astfel: rezultatele obținute în urma analizei de drept penal a obiectului acestor infracțiuni; rezultatele care au fost obținute în urma analizei de drept penal a laturii obiective a infracțiunilor prevăzute la art. 259 CP RM; rezultatele care au fost obținute în urma analizei de drept penal a laturii subiective a acestor infracțiuni; rezultatele obținute în urma analizei de drept penal a subiectului infracțiunilor ce sunt prevăzute de art. 259 CP RM;

rezultatele ce au fost obținute în urma analizei de drept penal a circumstanțelor agravante ale acestor infracțiuni.

Investigațiile, efectuate în Capitolul 3, reprezintă efectul și bilanțul aplicării în Capitolul 2 al tezei a materialelor și a metodelor care sunt necesare în contextul analizei de drept penal a infracțiunilor prevăzute la art. 259 CP RM. În mod firesc, aceste investigații urmăresc aceleași obiective ale cercetării, care sunt preconizate a fi realizate în cadrul Capitolului 2 al tezei. Înfăptuirea unor asemenea obiective reprezintă condiția pentru realizarea *per ansamblu* a scopului prezentei teze.

1. ABORDĂRI DOCTRINARE ȘI NORMATIVE PRIVIND RĂSPUNDEREA PENALĂ PENTRU ACCESUL ILEGAL LA INFORMAȚIA COMPUTERIZATĂ

1.1. Analiza materialelor științifice privind răspunderea penală pentru accesul ilegal la informația computerizată, publicate în Republica Moldova

În opinia lui C.R. Butculescu, „doctrina are rolul de a clarifica mesajul juridic transmis în cadrul comunicării materiale a dreptului, identificând [...] problemele sociale care necesită reglementare”.[16] Același autor continuă: „[...] Doctrina are și rolul de a clarifica mesajele transmise prin comunicarea formală a dreptului, contribuind [...] la îmbunătățirea [...] înțelegerii normelor juridice [...]”.[17] La rândul său, I. Flămânzeanu afirmă că „doctrina juridică exercită o influenţă [...] asupra judecătorilor care [...] îşi fundamentează motivarea soluţiilor [...] [, precum și] prin formarea de juriști chemaţi să aplice sau să interpreteze legea”.[18]

Suntem de acord cu acești autori. Fiind conștienți de rolul incontestabil al doctrinei juridice în contribuirea la interpretarea și aplicarea legii penale în corespundere cu principiul legalității, în cadrul acestui studiu vom analiza materialele științifice referitoare la accesul ilegal la informaţia computerizată (art. 259 CP RM), publicate în Republica Moldova.

Urmărind succesiunea în timp a acestor materiale, începem analiza noastră cu o lucrare publicată în 2003.[19] Autorul comentariului la art. 259 CP RM este unul dintre coautorii acestei lucrări – *M. Gheorghiță*.

În opinia autorului în cauză, obiectul juridic generic al infracțiunilor ce sunt prevăzute de art. 259 CP RM îl constituie relațiile sociale referitoare la „securitatea publică privind producerea, utilizarea, difuzarea protecția informației și a resurselor informaționale, sistemelor de prelucrare a informației cu aplicarea MEC (mașinilor electronice de calcul).”[20] Examinând obiectul juridic special, M. Gheorghiță consideră că acesta este format din „relațiile sociale care apar în procesul colectării, prelucrării, păstrării și prezentării informației computerizate și a resurselor

[16] BUTCULESCU, Claudiu Ramon. Rolul clarificator al doctrinei pentru comunicarea juridică. În: *Impactul transformărilor socio-economice și tehnologice la nivel național, european și mondial*, 2015, nr. 6, pp. 23-28. ISSN 2393-3240.
[17] Ibidem.
[18] FLĂMÂNZEANU, Ion. Doctrina ca izvor de drept. În: *Revista Studii de Drept Românesc*, 2010, nr. 1, pp. 23-30. ISSN 2284 -9394.
[19] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chișinău: Arc, 2003. 836 p. ISBN 9975-61-291-1.
[20] Ibidem, p. 568.

informaționale."[21] Deși folosește sintagma „obiect nemijlocit al infracțiuni", autorul în cauză are în vedere obiectul material al infracțiunii, menționând „tehnica computerizată [...], precum și diferite mijloace de telecomunicații, cu ajutorul cărora tehnica de calcul se conectează la rețelele informaționale [...]."[22]

În contextul analizei laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, M. Gheorghiță susține că „în cazul în care accesul ilegal la informația computerizată este un procedeu de săvârșire a altei infracțiuni, fapta săvârșită trebuie calificată drept concurs de infracțiuni."[23] De asemenea, autorul dat consemnează: „Componența infracțiunii este materială. Infracțiunea se consideră consumată începând cu prezența cel puțin a uneia din consecințele enumerate în lege [...]."[24]

Caracterizând latura subiectivă a infracțiunilor de acces ilegal la informaţia computerizată, M. Gheorghiță stabilește că aceasta „se manifestă prin intenție directă sau indirectă. [...] Cauzele și scopurile infracțiunii pot fi diverse: aviditate; răzbunare; invidie; huliganism [...] etc.".[25]

În fine, în ceea ce privește subiectul infracțiunilor care sunt prevăzute de art. 259 CP RM, M. Gheorghiță este de opinia că acesta „este persoana fizică responsabilă [...] care a atins vârsta de 16 ani".[26] Același autor continuă: „În cazul în care accesul ilegal la informația computerizată a fost săvârșit de reprezentantul persoanei juridice [...], răspunderea o poartă executantul nemijlocit și persoana juridică."[27]

Următoarea lucrare îl are ca autor pe *A. Borodac* și datează din 2004.[28]

În rezultatul pertractării obiectului juridic al infracțiunilor de acces ilegal la informaţia computerizată, autorul dat conchide că „obiectul generic de grup al infracțiunilor în domeniul informaticii îl constituie relațiile sociale care ocrotesc securitatea informațională computerizată"[29]; „Obiectul nemijlocit de bază [...] îl constituie relațiile sociale care ocrotesc dreptul posesorului de informație computerizată privind inviolabilitatea acesteia și exploatarea corectă a sistemului informatic".[30]

Analiza laturii obiective a infracțiunilor în cauză îi permite lui A. Borodac să vorbească despre trei semne ale acesteia. Cu toate acestea, autorul dat evidențiază doar două asemenea

---

[21] Ibidem, p. 568.
[22] Ibidem, p. 568.
[23] Ibidem, p. 569.
[24] Ibidem, p. 569.
[25] Ibidem, p. 570.
[26] Ibidem, p. 569.
[27] Ibidem, p. 569.
[28] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chișinău: Tipografia Centrală, 2004. 622 p. ISBN 9975-9788-7-8.
[29] Ibidem, p. 362.
[30] Ibidem, p. 362.

semne: „1) accesul ilegal la informația computerizată; 2) distrugerea, deteriorarea, blocarea sau copierea informației, sau dereglarea funcționării calculatoarelor, a sistemului sau a rețelelor informatice.”[31] Nu este clar ce rol atribuie A. Borodac semnelor enumerate mai sus: părți componente ale faptei prejudiciabile; fapta prejudiciabilă și urmările prejudiciabile?

În continuare respectivul autor definește mai multe noțiuni utilizate în art. 259 CP RM, care se referă la variate semne constitutive.

În planul examinării elementelor constitutive subiective ale infracțiunilor de acces ilegal la informaţia computerizată, A. Borodac arată că „latura subiectivă a infracțiunii se caracterizează atât prin intenție directă, cât și prin intenție indirectă”[32]; „Subiect al infracțiunii poate fi orice persoană fizică responsabilă, care a atins vârsta de 16 ani, precum și o persoană juridică.”[33]

Următoarea lucrare datează din 2005, avându-l drept coautor pe *A. Barbăneagră*[34], care realizează comentariul la art. 259 CP RM.

În demersul de identificare a valorii sociale fundamentale vătămate prin săvârșirea infracțiunilor prevăzute de acest articol, A. Barbăneagră punctează că „obiectul generic al infracțiunii se constituie din relațiile sociale ce vizează securitatea informațiilor.”[35] În scopul accesibilizării interpretării prevederilor art. 259 CP RM, autorul respectiv definește noțiunile „informație computerizată”, „acces ilegal la informația computerizată”, „sistem informatic” etc.

Din perspectiva alin. (1) art. 25 CP RM, coroborat cu art. 259 CP RM, A. Barbăneagră susține că „infracțiunea se consideră consumată din momentul în care s-a produs una dintre acțiunile enumerate în dispozițiile legii.”[36] Având o opinie diferită față de cea exprimată de M. Gheorghiță și A. Borodac, A, Barbăneagră consideră că, în cazul infracțiunilor prevăzute la art. 259 CP RM, latura subiectivă „se realizează prin intenție directă.”[37] Această opinie decurge din raportarea de către A. Barbăneagră a infracțiunilor analizate la categoria de infracțiuni formale.

Autorul dat relevă astfel caracteristicile subiectului infracțiunilor de acces ilegal la informaţia computerizată: „Subiect al infracțiunii poate fi orice persoană fizică, responsabilă, care a împlinit vârsta de 16 ani [...] și persoana juridică”.[38]

Din anul 2005 datează o lucrare care îl are în calitate de coautor pe *V. Stati*.[39]

---

[31] Ibidem, p. 364.
[32] Ibidem, p. 366.
[33] Ibidem, p. 366.
[34] BARBĂNEAGRĂ, Alexei et al. *Codul penal comentat şi adnotat*. Chișinău: Cartier, 2005. 656 p. ISBN 9975-29-338-X.
[35] Ibidem, p. 434.
[36] Ibidem, p. 435.
[37] Ibidem, p. 435.
[38] Ibidem, p. 435.
[39] BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005. 804 p. ISBN 9975-79-324-X.

Între altele, autorul dat susține că „obiectul juridic generic al infracţiunilor din Capitolul XI [...] îl reprezintă relaţiile sociale din domeniul informaticii și telecomunicaţiilor.”[40] Această opinie este în concordanță cu Legea nr. 254 din 09.07.2004 pentru modificarea şi completarea Legii telecomunicaţiilor nr. 520-XIII din 7 iulie 1995 şi a Codului penal al Republicii Moldova.[41] Conform legii date, titlul Capitolului XI al părții speciale a Codului penal a fost modificat din „Infracţiuni în domeniul informaticii” în „Infracţiuni în domeniul informaticii şi telecomunicaţiilor”. Dezvoltând ideea, V. Stati clasifică astfel infracțiunile specificate în respectivul capitol: „a) infracţiuni în domeniul informaticii (prevăzute la art. 259, 260, 261 CP RM); b) infracţiuni în domeniul telecomunicaţiilor (prevăzute la art. 261^1 CP RM).”[42]

Privitor la obiectul juridic special al infracţiunilor ce sunt prevăzute de art. 259 CP RM, autorul respectiv menționează că acesta are un caracter complex: „obiectul juridic principal [...] [–] relaţiile sociale privitoare la accesul legal la informaţia computerizată. Obiectul juridic secundar [...] [–] relaţiile sociale referitoare la intervenţia legală în sistemul informaţional”[43]; „Obiectul material sau [...] imaterial [...]: informaţia computerizată; calculatoare; sistemul informatic; reţeaua informatică.”[44]

În contextul examinării obiectului infracțiunilor de acces ilegal la informaţia computerizată, V. Stati învederează calitatea specială a participantului la relațiile sociale protejate de art. 259 CP RM: „Victimă a infracţiunii [...] [–] proprietarul sau posesorul de resurse și sisteme informaţionale, de tehnologii și mijloace de asigurare a acestora [...] [, precum și] utilizatorul de informaţie computerizată.”[45]

De asemenea, reține atenția punctul de vedere cu privire la conținutul și structura laturii obiective a faptelor infracționale analizate: „a) fapta prejudiciabilă care constă în acţiunea principală de acces ilegal la informaţia computerizată, însoţită de acţiunea adiacentă [...]”[46]; b) urmările prejudiciabile care se exprimă sub formă de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei [etc.]”[47]; c) legătura cauzală [...].”[48] Din această opinie rezultă clar că infracțiunile de acces ilegal la informaţia computerizată sunt infracțiuni cu componență

[40] Ibidem, p. 493.
[41] Legea pentru modificarea şi completarea Legii telecomunicaţiilor nr. 520-XIII din 7 iulie 1995 şi a Codului penal al Republicii Moldova: nr. 254 din 09.07.2004. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 189-192, 848.
[42] BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005, p. 494. 804 p. ISBN 9975-79-324-X.
[43] Ibidem, p. 495.
[44] Ibidem, p. 495.
[45] Ibidem, p. 496.
[46] Ibidem, p. 496.
[47] Ibidem, p. 496.
[48] Ibidem, p. 496.

materială, iar urmările prejudiciabile constituie semnul secundar obligatoriu al laturii obiective a acestor infracțiuni.

În exegeza dedicată noțiunii cheie ce caracterizează fapta prejudiciabilă prevăzută la art. 259 CP RM, V. Stati enunță: „„Acces" înseamnă [...] darea de instrucţiuni unui sistem informatic, comunicarea cu/printr-un sistem informatic, stocarea informaţiei sau regăsirea acesteia într-un sistem informatic"[49]; „Accesul trebuie să fie ilegal, adică să se realizeze prin încălcarea măsurilor de securitate reglementare, cu intenţia de a obţine [...] informaţie confidenţială."[50] Se are în vedere informația „a cărei colectare sau răspândire poate prejudicia interesele publice sau drepturile și interesele ocrotite de lege ale persoanelor fizice ori juridice."[51] În aceeași ordine de idei, autorul precitat deosebește „accesul ilegal" în accepția art. 259 CP RM de alte fapte: „Nu se consideră acces ilegal: 1) accesul autorizat de către [proprietar sau posesor] pentru testarea sau protecţia sistemului informatic"[52]; „2) accesul autorităţilor publice în contextul urmăririi penale sau al efectuării măsurilor operative de investigaţii, în conformitate cu legea"[53]; „3) accesul în activităţile obișnuite și legitime de proiectare a sistemelor informatice, practicile de operare curentă a sistemelor informatice sau practicile comerciale legale"[54]; 4) „accesul la informaţia despre sine."[55]

Încheind examinarea laturii obiective a infracțiunilor analizate, V. Stati evocă: „Infracţiunea prevăzută la art. 259 CP RM este una materială"[56]; „Ea se consideră consumată din momentul survenirii urmărilor prejudiciabile sub forma distrugerii, deteriorării, modificării [...] [etc. a] informaţiei computerizate [...] [etc.]."[57]

Caracteristicile laturii subiective ale infracţiunilor prevăzute la art. 259 CP RM, stabilite de V. Stati, nu diferă esențial de cele menționate mai sus de către M. Gheorghiță, A. Borodac și A. Barbăneagră: „Latura subiectivă [...] se caracterizează prin intenţie directă sau indirectă. Motivele infracţiunii pot consta în: interesul „sportiv", intenţii huliganice, răzbunare, interes material etc."[58] În ce privește ultimul element constitutiv al infracțiunilor examinate – subiectul, punctul de vedere al lui V. Stati prezintă anumite diferențe în comparație cu pozițiile altor autori: „1) persoana fizică responsabilă, care la momentul săvârșirii infracţiunii a atins vârsta de 16 ani;

[49] Ibidem, p. 496.
[50] Ibidem, p. 496.
[51] Ibidem, p. 496.
[52] Ibidem, p. 497.
[53] Ibidem, p. 497.
[54] Ibidem, p. 497.
[55] Ibidem, p. 497.
[56] Ibidem, p. 497.
[57] Ibidem, p. 497.
[58] Ibidem, p. 497.

2) persoana juridică care desfășoară activitate de întreprinzător."[59] Această calitate specială a persoanei juridice – subiect al infracțiunii este determinată de dispoziția de la alin. (4) art. 21 CP RM: „Persoana juridică care desfăşoară activitate de întreprinzător poartă răspundere penală pentru infracţiunile săvârşite, prevăzute la art. [...] 259 [...]."[60] Această dispoziție a avut un asemenea conținut până la intrarea în vigoare a Legii nr. 277 din 18.12.2008 pentru modificarea şi completarea Codului penal al Republicii Moldova.[61] Odată cu intrarea în vigoare a acestei legi, dispoziția de la alin. (4) art. 21 CP RM a dobândit un alt conținut: „Persoanele juridice, cu excepţia autorităţilor publice, răspund penal pentru infracţiunile pentru săvârşirea cărora este prevăzută sancţiune pentru persoanele juridice în partea specială din prezentul cod."[62] Abia din acest moment se poate vorbi despre persoana juridică (cu excepţia autorităţii publice) ca subiect al infracțiunilor de acces ilegal la informaţia computerizată.

V. Stati încheie analiza infracţiunilor prevăzute la art. 259 CP RM cu examinarea variantei agravate prevăzute la alin. (2) al acestui articol, care presupune comiterea acestor infracţiuni: a) repetat; b) de două ori mai multe persoane; c) cu violarea sistemului de protecţie; d) cu conectarea la canalele de telecomunicaţii; e) cu folosirea unor mijloace tehnice speciale.

Următoarea publicație științifică, ce nu poate fi trecută cu vederea, este a lui *N. Lazareva* și datează din 2007.[63]

Acest autor caracterizează în felul următor valoarea socială din cadrul obiectului juridic special al infracțiunilor de acces ilegal la informaţia computerizată: „drepturile proprietarului informației computerizate asupra inviolabilității acesteia".[64] Aceeași autoare include în această valoare „interesele privind funcționarea corectă (în siguranță) a calculatoarelor, a sistemului informatic sau a reţelei informatice."[65]

În contextul pertractării faptei prejudiciabile prevăzute la art. 259 CP RM, N. Lazareva menționează: „Nu poate fi considerat „acces la informația computerizată" simpla luare fizică [...] a unui suport de informații [...], în scopul vânzării acestuia[...]"[66]; „O astfel de faptă este

---

[59] Ibidem, p. 497.
[60] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[61] Legea pentru modificarea şi completarea Codului penal al Republicii Moldova: nr. 277 din 18.12.2008. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 41-44, 120.
[62] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[63] ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista științifică a USM „Studia Universitatis". Seria „Ştiinţe sociale"*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.
[64] Ibidem.
[65] Ibidem.
[66] Ibidem.

calificată ca atentare asupra patrimoniului (de exemplu, ca furt (art. 186 CP RM))".[67] În același context, prezintă valoare următoarele reflecții ale autorului precitat: „Accesul la informația computerizată poate fi considerat neautorizat dacă făptuitorul: nu are temeiuri legale pentru a accesa această informație"[68]; „are temeiuri legale pentru a accesa această informație, însă o accesează cu încălcarea ordinii stabilite, fără a respecta măsurile de protecție a informației computerizate."[69]

Ca și A. Barbăneagră, N. Lazareva consideră că infracţiunile prevăzute la art. 259 CP RM „au o componență formală și se consideră consumate din momentul săvârșirii faptei prejudiciabile."[70] Această părere diferă de cea expusă de M. Gheorghiță, A. Borodac și V. Stati.

În continuare, N. Lazareva definește noțiunile care desemnează modalitățile normative ale faptei prejudiciabile analizate.

La fel ca M. Gheorghiță, A. Borodac și V. Stati, N. Lazareva este de părerea că infracțiunile de acces ilegal la informaţia computerizată sunt comise cu „intenție directă sau indirectă".[71] Ca motive ale infracțiunilor date, autoarea respectivă numește: „interesul material; răzbunare; invidie; motivul huliganic; năzuința de a strica reputația unui concurent de afaceri [...] etc."[72] În fine, subiectul infracțiunilor examinate este descris de către N. Lazareva în următorul mod: „persoana fizică responsabilă, care, în momentul comiterii infracțiunii, a atins vârsta de 16 ani, sau persoana juridică."[73]

Din 2009 datează o lucrare care îi are în calitate de coautori pe *A. Barbăneagră* și *Gh. Alecu.*[74] Aceștia realizează comentariul la art. 259 CP RM.

În legătură cu valoarea socială din cadrul obiectului juridic special al infracţiunilor prevăzute de articolul dat, autorii în cauză susțin că aceasta constă în „securitatea informaţiilor şi protecţia sistemelor informaţionale şi a datelor stocate pe ele."[75]; „Confidenţialitatea, intimitatea, dreptul persoanei de a-şi lansa opiniile, libertatea de expresie, dreptul la proprietate etc. apar în calitate de obiecte suplimentare de atentare."[76] Este de reținut caracterizarea obiectului imaterial și a victimei infracțiunilor de acces ilegal la informaţia computerizată, făcută de A. Barbăneagră și Gh. Alecu: „Sintagma „informaţie computerizată" presupune stocarea pe un suport informaţional

---

[67] Ibidem.
[68] Ibidem.
[69] Ibidem.
[70] Ibidem.
[71] Ibidem.
[72] Ibidem.
[73] Ibidem.
[74] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009. 860 p. ISBN 978-9975-105-20-0.
[75] Ibidem, p. 567.
[76] Ibidem, p. 567.

a unor date despre persoane, subiecte, fapte [...], care permit identificarea lor”[77]; „Proprietarul resurselor şi sistemelor informaţionale [...] exercită integral dreptul de posesiune, folosinţă şi dispoziţie asupra resurselor şi sistemelor informaţionale [...].”[78]

Având ca premisă ideea promovată de A. Barbăneagră în 2003 în lucrarea consemnată mai sus, concepția lui A. Barbăneagră și Gh. Alecu, referitoare la latura obiectivă a infracțiunilor analizate, presupune: „Latura obiectivă a infracţiunii se realizează printr-o activitate de acces nesancţionat, fără drept, la un sistem informatic”[79]; „Sintagma „accesul ilegal la informaţia computerizată” desemnează accesul neautorizat la informaţii, efectuat cu încălcarea regimului de lucru [...].”[80] Mai multă claritate acestei concepții imprimă următorul punct de vedere, exprimat de către cei doi coautori: „Modalităţile de realizare a accesului ilegal la informaţiile computerizate sunt: distrugerea, deteriorarea, modificarea, blocarea, copierea informaţiei; [etc.]”[81]; „Prin distrugere se înţelege fapta persoanei orientată spre nimicirea informaţiei, care nu mai poate fi restabilită”[82]; „Blocarea se realizează prin împiedicarea recepţionării sau transmiterii informaţiei computerizate”[83]; „Modificarea desemnează schimbarea aspectului, formei şi a conţinutului informaţiei [...]”[84]; „Acţiunea de copiere presupune transferul ilegal al informaţiei computerizate de pe un suport material pe altul”[85]; „Prin dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice se înţeleg acţiunile de defectare a tehnicii menţionate.”[86] Așadar, distrugerea, deteriorarea, modificarea, blocarea, copierea informaţiei, precum și dereglarea funcţionării calculatoarelor, a sistemului informatic sau a reţelei informatice, sunt privite de către A. Barbăneagră și Gh. Alecu nu ca urmări prejudiciabile ale infracțiunilor prevăzute la art. 259 CP RM, ci ca modalități ale faptei prejudiciabile de acces ilegal la informaţia computerizată.[87]

Având ca premisă ideea promovată de A. Barbăneagră în 2003 în lucrarea specificată mai sus, concepția lui A. Barbăneagră și Gh. Alecu, referitoare la momentul consumativ al infracțiunilor analizate, presupune: „Infracţiunea se consideră consumată din momentul în care s-a produs una

[77] Ibidem, p. 567.
[78] Ibidem, p. 567.
[79] Ibidem, p. 567.
[80] Ibidem, p. 567.
[81] Ibidem, p. 568.
[82] Ibidem, p. 568.
[83] Ibidem, p. 568.
[84] Ibidem, p. 568.
[85] Ibidem, p. 568.
[86] Ibidem, p. 568.
[87] STRÎMBEANU, Alexandru. Materiale științifice referitoare la accesul ilegal la informaţia computerizată publicate în Republica Moldova. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 3, pp. 133-142. ISSN 1814-3199.

din acţiunile enumerate în dispoziţia legii."[88] În context, este necesar să concretizăm că, la momentul publicării lucrării pe care o analizăm, intrase în vigoare Legea nr. 278 din 18.12.2008 pentru modificarea şi completarea Codului penal al Republicii Moldova[89] (în continuare – Legea nr. 278/2008). În conformitate cu această lege, dispoziția de la alin. (1) art. 259 CP RM a fost modificată din „Accesul ilegal la informaţia computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică, dacă acest acces este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice"[90] în „Accesul ilegal la informaţia computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică"[91], „al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic"[92] „ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic"[93], „dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice şi dacă a cauzat daune în proporţii mari".[94]

Totodată, este interesant că A. Barbăneagră și Gh. Alecu deviază de la ideea promovată de A. Barbăneagră în 2003 în lucrarea consemnată mai sus, referitoare la tipul intenției ce caracterizează infracțiunile de acces ilegal la informaţia computerizată: „Latura subiectivă a infracţiunii se realizează prin [...] intenţie directă sau indirectă"[95]; „Făptuitorul conştientizează caracterul prejudiciabil al faptei, prevede urmările şi le doreşte sau le admite [...] pentru a distruge, deteriora, modifica, bloca sau a copia informaţia computerizată [...] [etc.]."[96] Cu privire la ultimul dintre elementele constitutive ale infracțiunilor examinate, opinia celor doi coautori este: „Subiect al infracţiunii poate fi orice persoană fizică, responsabilă, care a împlinit vârsta de

[88] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0.
[89] Legea pentru modificarea și completarea Codului penal al Republicii Moldova: nr. 278 din 18.12.2008. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 37-40, 98.
[90] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[91] Ibidem.
[92] Ibidem.
[93] Ibidem.
[94] Ibidem.
[95] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0.
[96] Ibidem, p. 568.

16 ani [...] şi persoana juridică."[97] Analiza infracțiunilor prevăzute la art. 259 CP RM se încheie cu pertractarea agravantelor specificate în alin. (2) al acestui articol.

În anul 2010 a fost editată lucrarea ai cărei coautori sunt *L. Gîrla* și *Iu. Tabarcea.*[98]

Obiectul juridic generic al infracțiunilor de acces ilegal la informaţia computerizată este descris astfel de către coautorii în cauză: „relațiile sociale care asigură securitatea producerii, păstrării, folosirii, distribuirii sau protecției informației computerizate, a sistemelor informatice, a resurselor informaționale și a serviciilor de telecomunicații".[99] Caracterizând valoarea socială din cadrul obiectului juridic special al faptelor infracționale respective, L. Gîrla și Iu. Tabarcea punctează că aceasta o formează: „ordinea legală de acces la informația computerizată"[100]; „Obiectul juridic secundar este format din relațiile publice care asigură legalitatea accesului la sistemele informatice."[101] Originalitatea acestui punct de vedere îl confirmă învederarea obiectului juridic secundar al infracţiunilor care sunt prevăzute de art. 259 CP RM.

În legătură cu examinarea obiectului infracțiunilor în cauză, cei doi coautori mai afirmă: „Obiectul material [...] îl reprezintă: informația computerizată; calculatorul; sistemul informatic, rețeaua informatică. [...]"[102]; „Victimă [...] poate fi proprietarul sau posesorul resurselor informaționale sau al sistemelor informatice, al tehnologiilor sau al mijloacelor de asigurare a acestora [...]"[103]; „De asemenea, victimă [...] poate fi utilizatorul informației computerizate."[104]

Conținutul și structura laturii obiective a infracțiunilor de acces ilegal la informaţia computerizată sunt descrise de către L. Gîrla și Iu. Tabarcea în maniera care nu diferă de cea prezentată de către V. Stati în lucrarea menționată mai sus, al cărei coautor acesta este. În aceeași ordine de idei, prezintă interes reflecțiile lui L. Gîrla și Iu. Tabarcea cu privire la ilegalitatea accesului în accepția art. 259 CP RM. Aceiași coautori definesc noțiunile utilizate în art. 259 CP RM, care desemnează modalitățile normative ale faptei prejudiciabile. L. Gîrla și Iu. Tabarcea consideră materiale infracțiunile prevăzute de acest articol, descriind astfel momentul de consumare a acestora: „momentul distrugerii, deteriorării, modificării, blocării sau copierii informaţiei computerizate, al dereglării funcţionării calculatoarelor, a sistemului sau a reţelei informatice."[105]

---

[97] Ibidem, p. 568.
[98] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010. 592 с. ISBN 978-9975-4158-2-8.
[99] Ibidem, c. 8.
[100] Ibidem, c. 13.
[101] Ibidem, c. 13.
[102] Ibidem, c. 14.
[103] Ibidem, c. 15.
[104] Ibidem, c. 15.
[105] Ibidem, p. 19.

În privința laturii subiective a infracțiunilor analizate, cei doi coautori exprimă punctul de vedere care este majoritar în doctrina penală autohtonă: intenția directă sau indirectă; motivul concretizat în: interesul material; interesul personal; concurența neloială, etc. Caracterizând subiectul infracțiunilor prevăzute la art. 259 CP RM, L. Gîrla și Iu. Tabarcea descrie nu doar condițiile generale pe care acesta trebuie să le îndeplinească, ci și calitatea lui specială: „persoana care nu are dreptul de acces la informaţia computerizată, la sistemul informatic sau la reţeaua informatică, stabilit prin lege sau prin contract”[106]; „persoana care depășește limitele permisiunii de acces la acestea”[107]; „persoana care nu a obținut permisiunea [...] să efectueze [...] operațiuni în sistemul informatic”.[108] Analiza, pe care au întreprins-o L. Gîrla și Iu. Tabarcea, finalizează cu investigarea detaliată a circumstanțelor agravante consemnate în alin. (2) art. 259 CP RM.

Din același an 2010 datează publicația științifică elaborată de către *S. Grișciuc-Bucica.*[109]

În opinia acesteia, valoarea socială din cadrul obiectului juridic generic al infracţiunilor ce sunt specificate în art. 259 CP RM se exprimă în „drepturile și interesele legitime [...] în domeniul creării și circulației informației computerizate.”[110]

În continuare, S. Grișciuc-Bucica analizează conținutul unor noțiuni care apar, printre altele, în art. 259 CP RM, și care vizează semnele constitutive ale infracțiunilor corespunzătoare. Autoarea menționează: „Informația computerizată, ca obiect imaterial al infracțiunii, este un semn obligatoriu al componențelor de infracțiuni analizate”[111]; „În consecință, aceasta demonstrează că respectiva categorie de infracțiuni ar trebui denumită „infracțiuni contra securității informaționale” [...]”[112]; „În legea penală în vigoare se admite o confuzie de noțiuni, deoarece conceptul „securitatea informațională” este privită prea îngust, doar din punctul de vedere al securității informațiilor conținute în computere și în sistemele informatice”[113]; „Este recomandabil [să se opereze amendamente] pentru a exclude posibilitatea interpretării greșite a noțiunii „infracțiuni informatice””[114]; „În caz contrar, s-ar putea ajunge la o coliziune juridică, precum și la interpretarea și aplicarea incorectă a normelor penale”.[115]

---

[106] Ibidem, c 19.
[107] Ibidem, c. 19.
[108] Ibidem, c. 20.
[109] ГРИЩУК-БУЧКА, Светлана. Уголовно-правовая характеристика преступлений против компьютерной безопасности (по законодательству Республики Молдова). În: *Securitatea informaţională 2010. Conferință internațională (Chişinău, 15-16 aprilie 2010)*. Chișinău: ASEM, 2010, pp. 97-101. ISBN 978-9975-75-509-2.
[110] Ibidem.
[111] Ibidem.
[112] Ibidem.
[113] Ibidem.
[114] Ibidem.
[115] Ibidem.

În anul 2011 a fost editată lucrarea lui *S. Brînza* și *V. Stati.*[116]

Ținând cont faptul completării Codului penal cu art. 260^1-260^6, operate prin Legea nr. 278/2008 și condiționată de angajamentele pe plan internațional ale Republicii Moldova, acești autori propun următoarea clasificare: „1) infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice (prevăzute la art. 259, 260, 260^1-260^4, 261 CP RM)”[117]; „2) infracţiuni informatice în accepţiune strictă (prevăzute la art. 260^5 şi 260^6 CP RM)”[118]; „3) infracţiuni în domeniul telecomunicaţiilor (prevăzută la art. 261^1 CP RM).”[119]

Prezintă interes și relaţia dintre infracţiunile prevăzute la art. 259 CP RM, pe de o parte, şi infracţiunile specificate la art. 178, 260^1-260^3 CP RM, pe de altă parte, examinată de către S. Brînza și V. Stati. Autorii în cauză conchid că infracţiunile prevăzute la art. 259 CP RM sunt infracţiuni materiale, întrucât se consideră consumate „din momentul producerii daunelor în proporţii mari.”[120]

În contextul analizei subiectului infracțiunilor de acces ilegal la informaţia computerizată, S. Brînza și V. Stati afirmă că subiect al acesteia poate fi „numai persoana care nu este autorizată [...], care depăşeşte limitele autorizării ori nu are permisiunea [...] să efectueze [...] operaţiuni într-un sistem informatic”.[121] În legătură cu agravanta specificată la lit. g) alin. (2) art. 259 CP RM, aceiași autori susțin: „Se are în vedere că accesată este nu oricare informaţie computerizată, dar o informaţie computerizată protejată de lege”[122]; „Se are în vedere: informaţia [...] despre starea sănătăţii psihice a persoanei; informaţia despre [...] starea sănătăţii sale reproductive [...] etc.”[123]; „Dacă este săvârşit accesul ilegal la informaţia computerizată protejată de lege, despre viaţa personală care constituie secretul personal ori familial al unei alte persoane, nu este exclus concursul”[124] „[, și anume] dintre infracţiunea prevăzută de lit. g) alin. (2) art. 259 CP RM şi una din infracţiunile specificate la alin. (1) sau (1^1) art. 177 CP RM.”[125]

În 2013 este publicată lucrarea lui *S. Bacinschi.*[126]

---

[116] BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011. 1324 p. ISBN 978-9975-53-028-7.
[117] Ibidem, p. 258.
[118] Ibidem, p. 258.
[119] Ibidem, p. 258.
[120] Ibidem, p. 269.
[121] Ibidem, p. 269.
[122] Ibidem, p. 270.
[123] Ibidem, p. 270.
[124] Ibidem, p. 271.
[125] Ibidem, p. 271.
[126] BACINSCHI, Serghei. Răspunderea penală pentru accesul ilegal la informaţia computerizată protejată de lege. În: *Probleme actuale privind protecţia şi securitatea persoanelor implicate în procesul penal (Materialele conferinţei ştiinţifico-practice internaţionale, 21 martie 2013)*. Chişinău: Academia „Ştefan cel Mare” a MAI, 2013, pp. 229-236. ISBN 978-9975-4407-2-1.

În cadrul acesteia, autorul întreprinde o analiză juridico-penală nu a infracţiunilor prevăzute la art. 259 CP RM în ansamblul lor, ci doar a agravantei prevăzute la lit. g) alin. (2) din acest articol – „în privinţa informaţiei protejate de lege”.

În acest scop sunt definite și examinate noțiunile utilizate în art. 259 CP RM. Analiza art. 212 din Codul de procedură penală al Republicii Moldova și a art. 315 şi 316 CP RM îl determină pe S. Bacinschi să ajungă la concluzia că dacă „informaţia ţine de confidenţialitatea urmăririi penale şi divulgarea datelor din cadrul acesteia, sunt pasibile de răspundere penală doar acele persoane care instrumentează cauza penală”[127] „sau care, contrar interdicţiei persoanelor care efectuează urmărirea penală, au divulgat aceste informaţii”[128]; „În ambele cazuri, persoana responsabilă de efectuarea urmăririi penale fie a prezumat că aceste date vor fi divulgate, din momentul ce a pus o interdicţie, fie ea însăşi le-a divulgat prejudiciind astfel urmărirea penală.”[129] În opinia autorului respectiv, în cazul accesării ilegale a unor astfel de informații nu poate fi aplicat art. 259 CP RM, „deoarece o condiţie obligatorie a componenţei este cauzarea de daune în proporţii mari.”[130]

În 2015 apare o lucrare elaborată de către *S. Brînza* și *V. Stati.*[131]

Analiza infracțiunilor prevăzute la art. 259 CP RM, efectuată în cadrul acesteia, nu diferă, în mare parte, de exegeza aceloraşi infracțiuni care datează din 2011, despre care am scris anterior.

Ca element de noutate, S. Brînza și V. Stati evidențiază că în art. 259 CP RM este prevăzută răspunderea pentru două infracțiuni, nu pentru una singură: „Sub denumirea marginală de acces ilegal la informaţia computerizată, în art. 259 CP RM, sunt reunite două variante-tip de infracțiuni şi o singură variantă agravată de infracțiune”[132]; „La lit. h) alin. (2) art. 259 CP RM este specificată nu o circumstanță agravantă a infracțiunii prevăzute la alin. (1) art. 259 CP RM”[133]; „De fapt, la alin. (1) și lit. h) alin. (2) art. 259 CP RM, sunt prevăzute două infracțiuni de sine stătătoare. Aceste două infracțiuni se pot afla între ele în concurs.”[134] În continuare se argumentează: „Nu există o componență „de bază” de acces ilegal la informaţia computerizată, componență care: 1) nu ar presupune producerea unor daune având o mărime concretă”[135] și „2) pe care s-ar grefa în calitate de circumstanțe agravante: a) producerea unor daune în proporţii

[127] Ibidem.
[128] Ibidem.
[129] Ibidem.
[130] Ibidem.
[131] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015. 1300 p. ISBN 978-9975-53-470-3.
[132] Ibidem, p. 346.
[133] Ibidem, p. 346.
[134] Ibidem, p. 346.
[135] Ibidem, p. 346.

mari; b) producerea unor daune în proporţii deosebit de mari”[136] „Cauzarea de daune în proporții deosebit de mari nu poate fi privită ca apendice [...] la componența [...] specificată la alin. (1) art. 259 CP RM [...]”.[137]

Lui *S. Crijanovschi* îi aparține o lucrare publicată în 2016.[138]

Scopul acestei lucrări este de a identifica tendințele din practica judiciară a Republicii Moldova și din cea a României, privind aplicarea răspunderii pentru accesul ilegal la informaţia computerizată.

Autorul în cauză menționează: „În general, proprietarii, deţinătorii sau utilizatorii de drept aleg să-şi protejeze sistemele informatice prin măsuri standard de securitate”[139]; „Protecţia poate fi fizică [...] sau logică [...]”[140]; „La nivel fizic, forţarea presupune dezafectarea dispozitivelor mecanice de securitate prin diferite mijloace mecano-chimico-electrice. La nivel logic, avem atacuri asupra parolelor.”[141]

În alt context, S. Crijanovschi afirmă: „În marea majoritate a cazurilor, făptuitorul acţionează pentru obţinerea de date informatice. Prin „obţinerea de date informatice” se înţelege inclusiv copierea acestora pe suporţi externi de stocare”[142]; „Dacă scopul accesului neautorizat a fost obţinerea de date informatice, starea de nesiguranţă a sistemului de calcul este dublată de starea de nesiguranţă a datelor informatice stocate în acesta sau prelucrate de către acesta”[143]; „Încălcarea măsurilor de securitate va determina însă o transformare efectivă adusă obiectului material al infracţiunii, măsura de securitate fiind, în acest caz, parte integrantă a sistemului informatic”[144]; „Astfel, clarificând unele aspecte discutabile ale faptei infracționale de acces ilegal la informaţia computerizată putem mai ușor să obținem răspunsuri la anumite probleme juridice complexe.”[145]

În 2019 își face apariția lucrarea lui *S. Copețchi.*[146]

---

[136] Ibidem, p. 346.
[137] Ibidem, p. 346.
[138] CRIJANOVSCHI, Sergiu. Accesul ilegal la informaţia computerizată în practica judiciară a Republicii Moldova și a României. În: *Conferința „Integrare prin cercetare și inovare” (Chișinău, Moldova, 28-29 septembrie). Vol. 1*. Chișinău: CEP USM, 2016, pp. 250-253. ISBN 978-9975-71-815-8.
[139] Ibidem.
[140] Ibidem.
[141] Ibidem.
[142] Ibidem.
[143] Ibidem.
[144] Ibidem.
[145] Ibidem.
[146] COPEȚCHI, Stanislav. Infracţiunile informatice potrivit legii penale moldave: studiu de drept comparat și propuneri *de lege ferenda*. În: *Realități și perspective ale învățământului juridic național. Culegerea materialelor științifice elaborate în baza comunicărilor de la Conferinţa ştiinţifică naţională cu participare internaţională, organizată cu ocazia a 60 de ani de la înființarea Facultății de Drept (USM, 01-02 octombrie 2019, Chișinău). Vol. II*. Chișinău: CEP USM, 2020, pp. 29-40. ISBN 978-9975-149-88-4.

În primul rând, atrage atenția opinia acestui autor cu privire la tangențele altor infracțiuni cu infracțiunile de acces ilegal la informaţia computerizată: „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”[147]; „Realizarea unor acţiuni suplimentare [...] nu ar trebui să conteze la încadrare potrivit art. 259 CP RM”[148], „ci la individualizarea pedepsei sau, eventual, pentru încadrarea celor săvârşite în tiparul unei alte norme de incriminare”[149]; „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”[150]; „În acest sens, par a fi elocvente modelele legislative din legislaţiile penale [...] aflate în consonanţă perfectă cu cel desprins din textul Convenţiei de la Budapesta.”[151]

S. Copețchi are o poziție tranșantă referitoare la structura laturii obiective a infracțiunilor examinate: „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”[152]; „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”[153]; „Potrivit unui Proiect [...][154], 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”[155] „urmând ca aceasta să apară pe post de circumstanţă agravantă la lit. h) alin. (2) art. 259 CP RM”[156]; „Susţinem

---

[147] Ibidem.
[148] Ibidem.
[149] Ibidem.
[150] Ibidem.
[151] Ibidem.
[152] COPEȚCHI, Stanislav. Infracţiunile informatice potrivit legii penale moldave: studiu de drept comparat și propuneri *de lege ferenda*. În: *Realități și perspective ale învățământului juridic național. Culegerea materialelor științifice elaborate în baza comunicărilor de la Conferinţa ştiinţifică naţională cu participare internaţională, organizată cu ocazia a 60 de ani de la înființarea Facultății de Drept (USM, 01-02 octombrie 2019, Chișinău). Vol. II*. Chișinău: CEP USM, 2020, pp. 29-40. ISBN 978-9975-149-88-4.
[153] Ibidem.
[154] *Proiectul legii pentru modificarea și completarea unor acte legislative (Legea privind Serviciul de Informații și Securitate al RM – art. 7; Codul penal – art. 178, 208[1], 259 ș.a.)*. [citat 30.08.2020] Disponibil: www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/3183/language/ro-RO/Default.aspx+&cd=3&hl=ro&ct=clnk&gl=at
[155] COPEȚCHI, Stanislav. Infracţiunile informatice potrivit legii penale moldave: studiu de drept comparat și propuneri *de lege ferenda*. În: *Realități și perspective ale învățământului juridic național. Culegerea materialelor științifice elaborate în baza comunicărilor de la Conferinţa ştiinţifică naţională cu participare internaţională, organizată cu ocazia a 60 de ani de la înființarea Facultății de Drept (USM, 01-02 octombrie 2019, Chișinău). Vol. II*. Chișinău: CEP USM, 2020, pp. 29-40. ISBN 978-9975-149-88-4.
[156] Ibidem.

propunerea legislativă avansată. Este neclară însă, cauza tergiversării transpunerii în realitate a respectivei iniţiative legislative."[157]

Continuă succesiunea lucrărilor analizate de noi publicația care aparține lui *C. Moțoc* și *L. Gîrla.*[158]

Din publicația dată aflăm că „scopul acestui articol rezidă în efectuarea unei analize juridice cuprinzătoare a semnelor obiective ale infracțiunilor prevăzute la articolele 178, 259, 260^1, 260^2 CP RM"[159] „cu scopul de a cerceta plenitudinea și relevanța protecției juridico-penale a secretului profesional în legea penală a Republicii Moldova"[160]; „În cadrul cercetării științifice s-a studiat literatura de specialitate, s-a analizat legislația extrapenală din Republica Moldova, s-au examinat actele internaționale în materia asigurării și protecției datelor personale confidențiale; s-au analizat semnele obiective ale faptelor infracționale prevăzute la articolele 178, 259, 260^1, 260^2 CP RM"[161]; „s-a examinat practica judiciară; s-a cercetat plenitudinea și relevanța protecției juridico-penale a secretului profesional în legea penală a Republicii Moldova"[162]; „s-a argumentat necesitatea revizuirii normelor care urmează a fi revizuite; s-au propus modificări *de lege ferenda* în scopul îmbunătățirii viitoare a legii penale."[163]

Una dintre concluziile celor doi autori, care se remarcă prin implicațiile sale, este: „Accesul ilegal la informația computerizată care constituie secretul profesional va constitui infracțiune în sensul lit. d) alin. (2) art. 259 CP RM doar în cazul în care sunt respectate câteva condiții obligatorii: 1) informația este computerizată"[164]; „2) subiectul faptei infracționale este o persoană neautorizată"[165]; „3) accesul este însoțit de alte acțiuni"[166]; „4) accesul a cauzat daune în proporţii mari"[167]; „5) obiectul imaterial al faptei de acces ilegal la informația computerizată îl constituie informația protejată de lege"[168]; „Sintagma „informație protejată de lege" va include și o categorie specială de informații protejate de lege, cum ar fi secretul profesional"[169]; „Informația confidențială cu privire la viața privată a persoanei, protejată atât în regim de secret

---

[157] Ibidem.
[158] MOȚOC, Costică, GÎRLA, Lilia. Protecția juridico-penală a secretului profesional prin prisma incriminărilor prevăzute la art. 178, 259, 260^1, 260^2 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale"*, 2020, nr. 3, pp. 139-151. ISSN 1814-3199.
[159] Ibidem.
[160] Ibidem.
[161] Ibidem.
[162] Ibidem.
[163] Ibidem.
[164] Ibidem.
[165] Ibidem.
[166] Ibidem.
[167] Ibidem.
[168] Ibidem.
[169] Ibidem.

primar, cât și în regim de secret secundar [...], constituie obiectul imaterial al infracțiunii prevăzute la lit. g) alin. (2) art. 259 CP RM."[170]

Aceste opinii comportă valoare științifică în contextul stabilirii conținutului circumstanțelor agravante prevăzute la lit. d) și g) alin. (2) art. 259 CP RM.

Încheiem examinarea materialelor științifice privitoare la răspunderea penală pentru accesul ilegal la informația computerizată, publicate în Republica Moldova, cu lucrarea elaborată de către *L. Dumneanu* și *D. Gurev*".[171]

Această lucrare are ca obiect analiza tuturor infracțiunilor în domeniul informatic, inclusiv a infracțiunilor ce sunt specificate în art. 259 CP RM. În afară de elementele constitutive și circumstanțele agravante ale acestor infracțiuni, autoarele se axează pe aspecte de interes pentru analiza de drept penal a infracțiunilor în domeniul informatic: concepte definitorii privind tehnologiile informaționale; calculatorul și sistemul de calcul; rețele de calculatoare și Internetul; securitatea informațională; evoluția normelor internaționale și transnaționale privitoare la infracțiunile săvârșite în domeniul informatic; evoluția reglementărilor naționale privind infracțiunile săvârșite în domeniul informatic, etc.

În contextul analizei obiectului infracțiunilor prevăzute la art. 259 CP RM, atrage atenția următorul punct de vedere care vizează obiectul material (imaterial) al infracţiunii care este specificată în alin. (1) art. 259 CP RM. În opinia celor două autoare, acest obiect „se poate exprima în mai multe variante, având un caracter alternativ: informaţia computerizată; calculatoarele; sistemul informatic; reţeaua informatică."[172] Această opinie este utilă în vederea stabilirii mai detaliate a conținutului obiectului material sau imaterial al infracțiunilor prevăzute la art. 259 CP RM. La fel de utilă este viziunea lui L. Dumneanu și D. Gurev referitoare loa înțelesul noțiunii „acces" utilizate în art. 259 CP RM: „Prin acces se înţelege [...] accesarea elementelor unui sistem informatic, comunicarea cu/printr-un sistem informatic, depozitarea informaţiei sau regăsirea acesteia într-un sistem informatic"[173]; „Accesul presupune penetrarea unui alt sistem informatic, conectat prin reţele de telecomunicaţii publice sau într-un alt sistem informatic din aceeaşi reţea, indiferent prin ce metoda de comunicare."[174] Nu în ultimul rând, în contextul examinării problemei legate de pluralitatea de victime ale infracțiunilor prevăzute la

[170] Ibidem.
[171] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM. 261 p. ISBN 978-9975-158-29-9.
[172] Ibidem, p. 89.
[173] Ibidem, p. 93.
[174] Ibidem, p. 93.

art. 259 CP RM, L. Dumneanu și D. Gurev afirmă: „Nu se exclude identificarea unei sau mai multor victime (cu calități diferite) într-o singură infracțiune.”[175]

Vom dezvolta această idee *infra*, pentru a ajunge la concluzia că „infracțiunea are o singură victimă în cazul în care aceeași persoană este atât proprietarul, alt posesor sau utilizatorul informaţiilor computerizate accesate ilegal, cât și proprietarul sau alt posesor al informației distruse, deteriorate, modificate, blocate sau copiate, ori al calculatorului, al sistemului informatic sau al reţelei informatice, ale căror funcționare a fost dereglată”[176]; „În alte cazuri, proprietarul, alt posesor sau utilizatorul informaţiilor computerizate accesate ilegal poate fi altcineva decât proprietarul sau alt posesor al calculatorului, al sistemului informatic sau al reţelei informatice, ale căror funcționare a fost dereglată.”[177]; „Doar în aceste din urmă cazuri, putem vorbi despre prezența victimei principale și a victimei secundare.”[178]

1.2. Analiza materialelor științifice privind răspunderea penală pentru accesul ilegal la informația computerizată, publicate peste hotare

Una dintre sarcinile de bază ale cercetărilor cu caracter juridico-penal constă în contribuirea la dezvoltarea dreptului penal ca ramură de știință. Știința dreptului penal reprezintă un sistem în continuă evoluție de concepții cu privire la legitățile de dezvoltare a societății și a gândirii, obținute în rezultatul studierii fenomenelor juridico-penale. Accesul ilegal la informaţia computerizată este unul dintre aceste fenomene. În literatura de specialitate străină se acordă o atenţie deosebită problematicii privind răspunderea penală pentru accesul ilegal la informaţia computerizată. Materialele ştiinţifice publicate la această temă sunt elocvente și numeroase. În cadrul studiului de față se va face o analiză temeinică a acestor materiale ştiinţifice. O atenţie deosebită va fi acordată publicaţiilor din ultimii ani.

În 2003 a fost publicat autoreferatul tezei de doctor susținute de *A.M. Doronin.*[179]

Autorul dat relevă că „norma, care prevede răspunderea penală pentru accesul ilegal la informaţia computerizată, este o verigă necesară în sistemul juridic de protecție a securității în

---

[175] Ibidem, p. 92-93.
[176] STRÎMBEANU, Alexandru. Victima secundară a infracțiunilor prevăzute la art. 259 din Codul penal. În: *Conferința științifică națională cu participare internațională dedicată aniversării a 75-a a Universității de Stat din Moldova „Integrare prin cercetare și inovare” (10-11 noiembrie 2021)*. Chișinău: CEP USM, 2021, pp. 6-8. ISBN 978-9975-152-48-8.
[177] Ibidem.
[178] Ibidem.
[179] ДОРОНИН, А.М. *Уголовная ответственность за неправомерный доступ к компьютерной информации*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Москва, 2003. 24 с.

sfera informațiilor computerizate”[180]; „Adoptarea și aplicarea acesteia sunt condiționate social, inclusiv sub aspectul prevenirii comiterii unei astfel de fapte.”[181] A.M. Doronin definește noțiunea de acces ilegal la informaţia computerizată ca „acces la informaţia computerizată al persoanei care nu are dreptul să obțină și să utilizeze fie această informație, fie sistemul informatic în care se află informația computerizată.”[182] Același autor arată că „norma penală, care stabilește răspunderea pentru accesul ilegal la informația computerizată, este o normă de referire”[183]; „Ea necesită examinarea completă a prevederilor actelor normative în domeniul informațional, al comunicațiilor, al programării computerelor, al protecției informațiilor bancare, comerciale și a altor informații confidențiale etc.”.[184]

În rezultatul analizei efectuate, A.M. Doronin ajunge la concluzia că legea penală a Federației Ruse ar trebui completată cu o dispoziție în care ar fi incriminată circulația ilegală a informației computerizate, adică „acțiunile intenționate îndreptate spre distrugerea, modificarea, blocarea, perturbarea funcționării computerelor, sistemelor informatice sau a rețelelor acestora, al căror obiect este informația computerizată destinată accesului liber al unui număr nelimitat de persoane [...]”.[185] În aceeași ordine de idei, respectivul autor propune adoptarea unei variante perfecționate a art. 272 CP FR (care este similar cu art. 259 CP RM).

În același an este publicată teza de doctor care s fost susținută de *N.A. Rozenfeld.*[186]

Autorul în cauză consideră că obiectul juridic generic al infracțiunilor, prevăzute de art. 361-363 CPU, îl formează „relațiile sociale în domeniul asigurării atât a funcționării neîntrerupte și stabile a computerelor, a sistemelor și rețelelor de computere, cât și al siguranței și integrității informațiilor computerizate, precum și a suporturilor pentru asemenea informații.”[187] În ce privește obiectul juridic special al infracțiunilor ce sunt specificate în art. 361 CPU (care este similar cu art. 259 CP RM), N.A. Rozenfeld enunță că acesta îl constituie „dreptul de a deține și a dispune de informația computerizată”.[188] În opinia aceluiași autor, obiectul material sau imaterial al infracțiunilor prevăzute la art. 361 CPU este reprezentat de: „computere; sisteme sau rețele de computere; informații computerizate și suporturi de informații computerizate”.[189] Doar

---

[180] Ibidem, c. 5.
[181] Ibidem, c. 5.
[182] Ibidem, c. 6.
[183] Ibidem, c. 6.
[184] Ibidem, c. 6.
[185] Ibidem, c. 6.
[186] РОЗЕНФЕЛЬД, Н.А. *Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж*: дис. на здоб. наук. ступ. канд. юрид. наук. Київ, 2003. 222 с.
[187] Ibidem, c. 51.
[188] Ibidem, c. 54.
[189] Ibidem, c. 59.

posesorii și utilizatorii informației computerizate sunt considerați de către N.A. Rozenfeld victime ale infracțiunilor prevăzute la art. 361 CPU. În viziunea autorului în cauză, „accesul ilegal la informaţia computerizată trebuie privit ca un astfel de acces la informaţia computerizată sau la suporturile pentru o asemenea informație”[190], „care are loc fie fără acordul sau în pofida dezacordului proprietarului informaţiei computerizate sau al unei persoane autorizate de acesta”[191], „fie cu încălcarea regulilor de acces stabilite de aceștia, care se comite prin utilizarea de software și (sau) a unor mijloace tehnice speciale.”[192] Analiza infracțiunilor, prevăzute la art. 361 CPU, se încheie cu examinarea elementelor constitutive subiective.

În 2006 iese de sub tipar monografia elaborată de către *M. Dobrinoiu.*[193]

În cadrul acesteia este efectuată, printre altele, analiza infracţiunilor prevăzute la art. 42[194] al Legii României nr. 161 din 19.04.2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităților publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei[195] (în continuare – Legea României nr. 161/2003). În opinia lui M. Dobrinoiu, infracțiunile respective aparțin de categoria de infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice. Examinând obiectul juridic generic (de grup) al infracţiunilor prevăzute la art. 42 al Legii României nr. 161/2003, autorul în cauză concluzionează că acesta îl constituie „valoarea socială numită sistem informatic şi de relaţiile sociale care iau naştere în legătură cu utilizarea sistemelor automate de prelucrare a datelor.”[196] După M. Dobrinoiu, obiectul juridic special al infracțiunilor supuse analizei îl formează „interesul juridic protejat [...] al proprietarului, deţinătorului sau utilizatorului de drept (legal) al

---

[190] Ibidem, c. 80.
[191] Ibidem, c. 80.
[192] Ibidem, c. 80.
[193] DOBRINOIU, Maxim. *Infracţiuni în domeniul informatic*. Bucureşti: C.H. Beck, 2006. 401 p. ISBN 978-973-655-941-9.
[194] Acest articol conținea următoarele prevederi: „(1) Accesul, fără drept, la un sistem informatic constituie infracţiune şi se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă”*; „(2) Fapta prevăzută la alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoare de la 6 luni la 5 ani”*; (3) Dacă fapta prevăzută la alin. (1) sau (2) este săvârşită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani”.*

* Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităților publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.

Art. 42 din Legea României nr. 161/2003 a fost abrogat prin Legea României nr. 187 din 24.10.2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal** (în continuare – Legea României nr. 187/2012).

** *Monitorul Oficial al României*, 2012, nr. 757.

[195] Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităților publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.
[196] DOBRINOIU, Maxim. *Infracţiuni în domeniul informatic*. Bucureşti: C.H. Beck, 2006, p. 147. 401 p. ISBN 978-973-655-941-9.

sistemului informatic”[197], „dar şi al proprietarului, deţinătorului ori utilizatorului de drept al datelor informatice stocate sau vehiculate în respectivul sistem informatic.”[198]

Același teoretician opinează că obiectul material al infracţiunilor, prevăzute la art. 42 al Legii României nr. 161/2003, îl reprezintă „entităţile materiale care compun sistemele informatice (calculatoare, reţele de calculatoare, elemente hardware – echipamente periferice, cabluri, plăci, servere etc.”[199] „şi software – programe, aplicaţii, baze de date etc.) şi [...] datele informatice spre care se îndreaptă atenţia făptuitorului.”[200] Privitor la subiectul activ al infracțiunilor sus-menționate, M. Dobrinoiu afirmă că acesta „poate fi orice persoană responsabilă penal, textul neprevăzând o calitate specială pentru aceasta”[201]; „În marea majoritate a cazurilor, asemenea persoane posedă cunoştinţe în domeniul tehnologiei informaţiei”[202]; „Dintre aceştia, un procent însemnat îl reprezintă experţii [...] familiarizaţi cu „spargerea” măsurilor de securitate ale calculatoarelor sau reţelelor de calculatoare”.[203]

Subiectul pasiv al infracţiunilor, prevăzute la art. 42 al Legii României nr. 161/2003, este caracterizată astfel de către respectivul doctrinar: „Este persoana fizică sau juridică proprietară sau deţinătoare de drept a sistemului informatic accesat ilegal sau a datelor informatice vizate”[204]; „Prin extensie, poate exista subiect pasiv colectiv [...], atunci când accesul în sistemul informatic generează în mod automat accesul ilegal în alte sisteme similare interconectate cu primul”[205]; „Poate exista subiect pasiv secundar în cazul în care datele informatice vizate de accesul ilegal se referă la o persoană fizică sau juridică, alta decât proprietarul sau deţinătorul de drept al respectivului sistem informatic”[206]; „Spre exemplu, făptuitorul accesează ilegal sistemul integrat de evidenţă informatizată a persoanei şi intră în posesia datelor personale referitoare la un anumit individ (evident, cu scopul de a le folosi ulterior).”[207]

Cu referire la elementul material (fapta prejudiciabilă) din cadrul infracțiunilor pertractate, M. Dobrinoiu relevă: „Se realizează prin accesul fără drept într-un sistem informatic (staţie de lucru, server ori reţea informatică)”[208]; „Accesul, în înţelesul dat de lege, desemnează intrarea în tot sau

[197] Ibidem, p. 147.
[198] Ibidem, p. 147.
[199] Ibidem, p. 148.
[200] Ibidem, p. 148.
[201] Ibidem, p. 148.
[202] Ibidem, p. 148.
[203] Ibidem, p. 148.
[204] Ibidem, p. 148.
[205] Ibidem, p. 148.
[206] Ibidem, p. 149.
[207] Ibidem, p. 149.
[208] Ibidem, p. 149.

numai într-o parte a sistemului informatic”[209]; „Metoda de comunicare – la distanţă, inclusiv graţie legăturii prin satelit sau nu, ori de aproape – nu prezintă importanţă”[210]; „În forma sa cea mai simplă, accesul fără drept la un sistem informatic presupune o interacţiune a făptuitorului cu tehnica de calcul vizată prin intermediul echipamentelor sau diverselor componente ale sistemului vizat [...]”[211]; „Pentru obţinerea accesului, făptuitorul va încerca o gamă variată de procedee tehnice, cum ar fi: atacul prin parolă, atacul de acces [...] etc.”[212]

În fine, autorul precitat caracterizează latura subiectivă a infracţiunilor prevăzute la art. 42 al Legii României nr. 161/2003: intenţie directă sau indirectă; scopul special de obţinere de date informatice – în cazul infracțiunii prevăzute la alin. (2) din articolul în cauză.

Din 2007 datează monografia elaborată de către *D.S. Azarov.*[213]

Din punctul de vedere al acestui autor, valoarea socială din cadrul obiectului juridic generic al infracțiunilor prevăzute la art. 361 CPU este „utilizarea computerelor, sistemelor și rețelelor informatice.”[214] D.A. Azarov distinge două obiecte juridice speciale al acestor infracțiuni: obiectul juridic principal – „relațiile sociale [...] care apar și există în legătură cu desfășurarea activităților de ordin informațional asupra informațiilor computerizate”[215]; obiectul juridic secundar – „relațiile sociale de proprietate.”[216]

În viziunea autorului în cauză, în cazul infracțiunilor prevăzute la 361 CPU, obiectele supuse influențării nemijlocite infracționale pot fi împărțite în două grupuri: „mijloace tehnice dăunătoare destinate accesului ilegal la informaţia computerizată, sisteme informatice [...] și alte entități (de exemplu, informație)”.[217]

Prezintă interes reflecțiile lui D.A. Azarov cu privire la urmările prejudiciabile în contextul infracțiunilor examinate: „Inițial, în art. 361 CPU erau menționate urmările prejudiciabile sub forma distorsionării sau distrugerii informației computerizate sau a suporturilor pentru astfel de informații”[218]; „O asemenea dispoziție legală a fost supusă unor critici meritate: termenul „distorsiune” este utilizat incorect în raport cu suporturile pentru informațiile computerizate [...]”[219]; „pentru cauzarea unor asemenea urmări, răspunderea poate fi aplicată în conformitate cu

---

[209] Ibidem, p. 149.
[210] Ibidem, p. 149.
[211] Ibidem, p. 149.
[212] Ibidem, p. 149.
[213] АЗАРОВ, Д.С. *Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)*. Київ: Атіка, 2007. 304 с. ISBN 966-326-230-3.
[214] Ibidem, c. 45.
[215] Ibidem, c. 62.
[216] Ibidem, c. 62.
[217] Ibidem, c. 72.
[218] Ibidem, c. 174.
[219] Ibidem, c. 174.

articolele din Titlul VI „Infracțiuni contra proprietății” al părții speciale a Codului penal al Ucrainei.”[220]

Analiza infracțiunilor prevăzute la art. 361 CPU o încheie examinarea caracteristicilor subiectului și ale laturii subiective.

În 2009 a fost publicat articolul științific al cărui autor este *C. Manea.*[221]

Această publicație este dedicată pertractării infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003. Astfel, C. Manea relevă că valoarea socială din cadrul obiectului juridic special al acestor infracțiuni constă în „securitatea şi confidenţialitatea sistemului informatic ori [...] încrederea în datele şi sistemele informatice sau în desfăşurarea corectă a operaţiunilor legate de acestea”.[222]

Privitor la obiectul material sau imaterial al infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003, autorul respectiv susține că acesta este reprezentat de „entităţile materiale care reprezintă sistemele sau reţelele informatice [...] asupra cărora se îndreaptă acţiunea ilicită”.[223]

C. Manea nu uită să caracterizeze subiectul activ al infracțiunilor în cauză – „orice persoană fizică ce întruneşte condiţiile generale pentru a răspunde penal”[224]; „De regulă, aceste persoane sunt experţi în calculatoare şi reţelele de calculatoare, persoane familiarizate cu „spargerea” măsurilor de securitate [...]”[225]; „Subiectul activ poate fi şi o persoană juridică cu limitările şi în condiţiile prevăzute în art. 19^1 C. pen.[226]”.[227]

În privința subiectului pasiv al infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003, doctrinarul în cauză evocă: „Este persoana fizică sau juridică deţinătoare de drept a sistemului informatic”[228]; „Poate fi subiect pasiv secundar şi altă persoană [...] în cazul în care

---

[220] Ibidem, c. 174.
[221] MANEA, Cornelia. Accesul ilegal la un sistem informatic. În: *Revista Pro Lege*, 2009, nr. 1, pp. 40-48. ISSN 1224-2411.
[222] Ibidem.
[223] Ibidem.
[224] Ibidem.
[225] Ibidem.
[226] Se are în vedere art. 19^1 din Codul penal al României din 21.07.1968*: „Persoanele juridice, cu excepția statului, a autorităților publice și a instituțiilor publice care desfășoară o activitate ce nu poate face obiectul domeniului privat”*, „răspund penal pentru infracțiunile săvârșite în realizarea obiectului de activitate sau în interesul ori în numele persoanei juridice, dacă fapta a fost săvârșită cu forma de vinovăție prevăzută de legea penală”*; „Răspunderea penală a persoanei juridice nu exclude răspunderea penală a persoanei fizice care a contribuit, în orice mod, la săvârșirea aceleiași infracțiuni.”*
* *Buletinul Oficial*, 1968, nr. 79-79 bis.
[227] MANEA, Cornelia. Accesul ilegal la un sistem informatic. În: *Revista Pro Lege*, 2009, nr. 1, pp. 40-48. ISSN 1224-2411.
[228] Ibidem.

datele informatice [...] se referă la o persoană [...], alta decât deţinătoarea sistemului informatic”.[229]

Este nelipsit de interes punctul de vedere exprimat de C. Manea cu privire la conținutul elementului material al infracțiunilor analizate: „Practic, făptuitorul acţionează asupra sistemului informatic prin forţarea acestor protecţii”[230]; „Forţarea unei protecţii logice variază de la încercarea de aflare a combinaţiei corecte [...] până la rularea unor programe specializate care identifică secvenţa de acces [...]”[231]; „Pentru existenţa elementului material [...] este necesar ca accesul la un sistem informatic să se realizeze „fără drept”, sintagmă care are înţelesul arătat în art. 35 alin. (2) din Legea nr. 161/2003[232]”.[233]

Caracterizând latura subiectivă a infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003, autorul respectiv afirmă: „În variantele prevăzute de alin. 1 şi 3 teza I, accesul ilegal la un sistem informatic se comite cu intenţie directă sau indirectă”[234]; „În majoritatea cazurilor, autorul caută să dăuneze. Intenţia de a scoate dintr-un asemenea act un profit ilicit nu este necesară şi ea nu este tipică acestei forme de comportament delictual”[235]; „Este, totuşi, posibil să existe o motivaţie indirect lucrativă, de exemplu, dorinţa de a face rău unui concurent”[236]; „În cazul variantelor prevăzute în alin. 2 şi 3 teza II, forma de vinovăţie specifică este intenţia directă, calificată prin scop, cerinţa esenţială a laturii subiective referindu-se la obţinerea de date informatice.”[237]

În 2011 a fost susținută teza de doctorat al cărei autor este *L.C. Kövesi.*[238]

În compartimentul VI.3.3.1 al acestei teze este efectuată examinarea infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003. În ceea ce privește valoarea socială din cadrul obiectului juridic special al respectivelor infracțiuni, L.C. Kövesi susține că aceasta constă în „securitatea sistemului informatic, inviolabilitatea acestuia şi care sunt de naturii a garanta

---

[229] Ibidem.
[230] Ibidem.
[231] Ibidem.
[232] Potrivit acestei norme, „acționează fără drept persoana care se află în una dintre următoarele situații: a) nu este autorizată, în temeiul legii sau al unui contract”*; „b) depășește limitele autorizării”*; „c) nu are permisiunea [...] de a efectua orice altă operațiune într-un sistem informatic.”*
* Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.
[233] MANEA, Cornelia. Accesul ilegal la un sistem informatic. În: *Revista Pro Lege*, 2009, nr. 1, pp. 40-48. ISSN 1224-2411.
[234] Ibidem.
[235] Ibidem.
[236] Ibidem.
[237] Ibidem.
[238] KÖVESI, Laura Codruța. *Combaterea crimei organizate prin dispoziţii de drept penal* / tz. de doct. în drept. Timișoara, 2011. 479 p.

confidenţialitatea şi integritatea atât a datelor, cât şi a sistemelor informatice."[239] După aceasta, respectivul autor punctează că infracțiunile analizate vatămă „patrimoniul organizaţiei, instituţiei, persoanei [...], încrederea publică în măsurile de siguranţă ale integrităţii datelor şi programelor informatice"[240]; „Reglementarea legală urmăreşte să protejeze sistemele informatice şi datele stocate pe acestea, de accesul neautorizat"[241]; „În raport cu dispoziţia legală aceste infracţiuni lezează mai multe relaţii sociale şi ca atare au două ori mai multe obiecte juridice, dintre care unul principal şi altul secundar"[242]; „De exemplu, accesul neautorizat la un sistem informatic în domeniul apărării loveşte atât în siguranţa naţională şi capacitatea de apărare a statului [...]."[243]

Referitor la obiectul material sau imaterial al infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003, L.C. Kövesi enunță că acesta constă în „anumite entităţi, cum ar fi sistemele sau reţelele informatice [...] asupra cărora se îndreaptă fapta de a accesa, fără drept, un sistem informatic."[244]

În continuare, același autor formulează concluzii privitoare la subiectul activ al infracțiunilor examinate – „orice persoană fizică sau juridică care îndeplineşte condiţiile legale pentru a răspunde din punct de vedere penal, legea neprevăzând o calitate specială pentru aceasta"[245]; „Persoana fizică răspunde penal dacă a împlinit vârsta de 14 ani şi a săvârşit fapta cu vinovăţie şi are discernământ"[246], „iar persoana juridică dacă a comis fapta în realizarea obiectului de activitate sau în interesul ori în numele persoanei juridice."[247]

Din punctul de vedere al lui L.C. Kövesi, în ipoteza infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003, „subiectul pasiv poate fi persoana fizică sau juridică al cărei sistem informatic a fost accesat fără drept"[248]; „De regulă, este [...] proprietara sau deţinătoarea de drept a sistemului informatic accesat ilegal sau a datelor informatice vizate"[249]; „Acest subiect pasiv poate fi şi unul colectiv [...] atunci când accesul [...] generează în mod automat accesul ilegal în alte sisteme similare interconectate cu primul."[250]

---

[239] Ibidem, p. 388-389.
[240] Ibidem, p. 389.
[241] Ibidem, p. 389.
[242] Ibidem, p. 389.
[243] Ibidem, p. 389.
[244] Ibidem, p. 389.
[245] Ibidem, p. 389.
[246] Ibidem, p. 389.
[247] Ibidem, p. 389.
[248] Ibidem, p. 391.
[249] Ibidem, p. 391.
[250] Ibidem, p. 391.

De asemenea, este analizat elementul material al acestor infracțiuni. În viziunea lui L.C. Kövesi, acesta „se realizează printr-o acţiune şi anume „accesul interzis”, adică fără drept, într-un sistem informatic”[251]; „Accesul fără drept la un sistem informatic presupune, potrivit art. 35 alin. (2) din Legea nr. 161/2003, că persoana respectivă se află în una din următoarele situaţii: nu este autorizată, în temeiul legii sau a unui contract”[252]; „depăşeşte limitele autorizării”[253]; „nu are permisiunea [...] de a desfăşura [...] operaţiuni într-un sistem informatic.”[254]

Nu în ultimul rând, este stabilit conținutul laturii subiective a infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003: intenţie directă sau indirectă; scopul special de obţinere de date informatice – în ipoteza infracțiunii care este prevăzută de alin. (2) din articolul în cauză.[255]

În 2012 este publicat articolul științific care a fost elaborat de către *V. Florescu* și *G. Florescu.*[256]

Obiectul de investigare al acestora îl reprezintă, printre altele, infracțiunile prevăzute de art. 42 din Legea României nr. 161/2003. În acest registru, V. Florescu și G. Florescu identifică valorile sociale specifice și relațiile sociale alăturate, care sunt protejate împotriva infracțiunilor respective: „Sunt apărate juridic relaţiile sociale dezvoltate în baza integrităţii datelor şi a securităţii sistemului informatic, dar în secundar şi relaţiile sociale dintre persoanele titulare de drepturi [...] asupra sistemului [...]”[257]; „De exemplu: accesul neautorizat la un sistem informatic din domeniul transportului aerian de pasageri [...] loveşte atât în siguranţa pasagerilor, cât şi în instituţia sau persoana titulară a sistemului penetrat ori a informaţiilor accesate [...].”[258]

Comportă originalitate părerea autorilor în cauză cu privire la obiectul material sau imaterial al infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003: „Din punct de vedere fizic, material sunt apărate echipamentele electronice şi electromecanice care compun sistemele informatice [...], dar şi programele şi aplicaţiile care rulează în sistemul informatic [...].”[259]

În continuare V. Florescu și G. Florescu răspund la întrebarea „Cine poate fi infractorul sau subiectul activ al infracţiunii?”: „Textul incriminării nu prevede o anumită calitate persoanei”[260];

---

[251] Ibidem, p. 391.
[252] Ibidem, p. 391.
[253] Ibidem, p. 391.
[254] Ibidem, p. 391.
[255] STRÎMBEANU, Alexandru. Materialele științifice referitoare la accesul ilegal la informaţia computerizată publicate peste hotare. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 8, pp. 114-127. ISSN 1814-3199.
[256] FLORESCU, Valentin, FLORESCU, Gabriela. Analiza infracţiunilor informatice incriminate în legislaţia în vigoare şi din perspectiva noului Cod penal. În: *Revista Română de Informatică şi Automatică*, 2012, vol. 22, nr. 2, pp. 21-38. ISSN 1841-4303.
[257] Ibidem.
[258] Ibidem.
[259] Ibidem.
[260] Ibidem.

„Orice persoană [...] poate avea rolul de subiect activ, inclusiv persoana juridică cu limitările şi în condiţiile prevăzute în art. 19^1 Cod penal.”[261]

Caracterizând subiectul pasiv al infracțiunilor prevăzute de art. 42 din Legea României nr. 161/2003, aceiași autori susțin: „Poate fi persoana [...] deţinătoare de drept a sistemului informatic”[262]; „În secundar, poate fi şi altă persoană [...] în cazul în care datele informatice vizate de accesul ilegal se referă la o persoană [...] alta decât deţinătoarea sistemului informatic [...].”[263]

În fine, prezintă valoare explicativă netăgăduită opinia lui V. Florescu și G. Florescu cu privire la elementul material al infracțiunilor examinate: „Accesul fără drept [...] înseamnă interacţiunea făptuitorului cu sistemul de calcul vizat prin intermediul echipamentelor periferice de control [...]”[264]; „Esenţial [...] este ca accesul la sistemul informatic să se realizeze de către persoana care se află într-una din următoarele situaţii: nu este autorizată [...]”[265], „depăşeşte limitele autorizării”[266], „nu are permisiunea [...] de a efectua orice altă operaţiune într-un sistem informatic [...].”[267]

Din același an datează articolul științific al lui *G. Zlati.*[268]

Autorul dat ia în vizor anumite probleme legate de calificarea faptelor în conformitate cu art. 42 din Legea României nr. 161/2003. Astfel, atrage atenția analiza raportului dintre infracțiunile prevăzute la acest articol și infracțiunea prevăzută la alin. (4) art. 24[269] al Legii României nr. 365 din 07.06.2002 privind comerțul electronic[270] (în continuare – Legii României nr. 365/2002).

În acest plan, G. Zlati afirmă: „În această secțiune vom aborda problematica operațiunii de skimming, prin trimitere la posibilitatea aplicării art. 42 din Legea nr. 161/2003”[271]; „Discuția nu este una iluzorie, deoarece însăși Înalta Curte de Casație și Justiție a statuat într-o decizie de speță că „fapta de a monta un dispozitiv de citire a benzii magnetice a cardurilor bancare în fanta unui bancomat constituie infracțiunea de acces, fără drept, la un sistem informatic săvârșită prin

---

[261] Ibidem.
[262] Ibidem.
[263] Ibidem.
[264] Ibidem.
[265] Ibidem.
[266] Ibidem.
[267] Ibidem.
[268] ZLATI, George. Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare, precum și a noului Cod penal. În: *Dreptul*, 2012, nr. 10, pp. 204-229. ISSN 1018-0435.
[269] Această normă (abrogată prin Legea României nr. 187/2012) prevedea răspunderea pentru tentativa la falsificarea instrumentelor de plată electronică.
[270] Legea României privind comerțul electronic: nr. 365 din 07.06.2002. În: *Monitorul Oficial al României*, 2002, nr. 483.
[271] ZLATI, George. Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare, precum și a noului Cod penal. În: *Dreptul*, 2012, nr. 10, pp. 204-229. ISSN 1018-0435.

încălcarea măsurilor de securitate, prevăzută în art. 42 alin. (1) și (3) din Legea nr. 161/2003”[272]; „Chiar dacă agentul introduce skimmer-ul fără drept în fanta bancomatului, reușind astfel să obțină datele cardului bancar, nu se realizează vreo interacțiune la nivel logic cu bancomatul”[273]; „Accesul nu trebuie privit ca fiind o simplă interacțiune cu sistemul informatic vizat”[274]; „Acest mod simplist de interpretare a noțiunii de acces [...] nu face decât să extindă aplicabilitatea textului de lege dincolo de intenția legiuitorului european [...].”[275]

Abordând raportul dintre infracțiunile prevăzute la art. 42 din Legea României nr. 161/2003 și infracțiunea prevăzută la alin. (1) art. 27[276] al Legii României nr. 365/2002, autorul respectiv opinează: „Prin art. 27 alin. (1) din Legea nr. 365/2002 coroborat cu art. 1 pct. 11 lit. b)[277] din același act normativ, legiuitorul român a incriminat efectuarea unei retrageri de numerar prin utilizarea unui instrument de plată electronicã fără consimțământul titularului instrumentului respectiv”[278]; „Soluția corectă este de a califica acest raport drept un concurs de calificări”[279]; „Mai exact, discutăm despre un concurs de calificări (redundante) unde accesul la sistemul informatic constituie element al infracțiunii prevăzute în art. 27 alin. (1) raportat la art. 1 pct. 11 lit. b) din Legea nr. 365/2002”.[280]

În continuare se argumentează: „Susținem acest lucru deoarece retragerea de numerar nu poate fi realizată decât prin accesarea bancomatului [...]”[281]; „Discutăm, așadar, despre o legătură intrinsecă între accesul fără drept la un sistem informatic și retragerea de numerar din bancomat”[282]; „Cu alte cuvinte, accesul se confundă cu retragerea de numerar ori o tentativă de retragere de numerar”[283]; „De exemplu, să presupunem că accesul la sistemul informatic [...] se

---

[272] *Decizia Secției Penale a Înaltei Curți de Justiție și Casație a României nr. 371 din 02.02.2010*. [citat 12.09.2020] Disponibil: https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=54367

[273] ZLATI, George. Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare, precum și a noului Cod penal. În: *Dreptul*, 2012, nr. 10, pp. 204-229. ISSN 1018-0435.

[274] Ibidem.

[275] Ibidem.

[276] Această normă (abrogată prin Legea României nr. 187/2012) prevedea răspunderea pentru „efectuarea uneia dintre operațiunile prevăzute la art. 1 pct. 10, prin utilizarea unui instrument de plată electronică”*, „inclusiv a datelor de identificare care permit utilizarea acestuia, fără consimţământul titularului instrumentului respectiv”.*

* Legea României privind comerțul electronic: nr. 365 din 07.06.2002. În: *Monitorul Oficial al României*, 2002, nr. 483.

[277] Norma dată se referă la „retrageri de numerar, precum și încărcarea și descărcarea unui instrument de monedă electronică”.*

* Legea României privind comerțul electronic: nr. 365 din 07.06.2002. În: *Monitorul Oficial al României*, 2002, nr. 483.

[278] ZLATI, George. Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare, precum și a noului Cod penal. În: *Dreptul*, 2012, nr. 10, pp. 204-229. ISSN 1018-0435.

[279] Ibidem.

[280] Ibidem.

[281] Ibidem.

[282] Ibidem.

[283] Ibidem.

consumă în momentul introducerii corecte a codului PIN”[284]; „În acest moment, ne referim implicit și la o tentativă de retragere de numerar [art. 250 alin. (1) din noul Cod penal ori art. 27 alin. (1) raportat la art. 1 pct. 1 lit. b) din Legea nr. 365/2002]”.[285]

De asemenea, din 2012 datează articolul științific al cărui autor este *C. Duvac.*[286]

Obiectul de studiu al acestuia îl constituie infracțiunile de acces ilegal la un sistem informatic, prevăzute de art. 360 CPR.[287] Analizând obiectul juridic special al respectivelor infracțiuni, C. Duvac arată că acesta „constă în relaţiile sociale care se nasc şi se dezvoltă în legătură cu siguranţa şi integritatea unui sistem informatic şi implicit a unor date informatice.”[288]

În ceea ce privește obiectul material sau imaterial al infracțiunilor prevăzute de art. 360 CPR, doctrinarul în cauză opinează că acesta constă în „entităţile materiale care reprezintă sistemele sau reţelele informatice [...] asupra cărora se îndreaptă acţiunea ilicită.”[289]

În vederea interpretării prevederilor art. 360 CPR, C. Duvac definește două noțiuni cheie utilizate în acest articol: „Prin „sistem informatic” se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională”[290], „dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic – art. 181 alin. (1) C. pen. (interpretarea autentică contextuală)”[291]; „Programul informatic reprezintă un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat”.[292]

Același autor caracterizează condițiile pe care trebuie să le îndeplinească subiecţii infracţiunilor prevăzute la art. 360 CPR: „Subiectul activ nemijlocit (autor) poate fi orice persoană fizică ce întruneşte condiţiile generale pentru a răspunde penal”[293]; „Subiectul activ al acestei infracţiuni poate fi şi o persoană juridică cu limitările şi în condiţiile prevăzute în art. 135 C. pen.”[294]; „Subiectul pasiv [...] este persoana [...] deţinătoare legitimă a sistemului informatic”[295]; „Poate fi subiect pasiv secundar şi o altă persoană [...] în cazul în care datele

---

[284] Ibidem.
[285] Ibidem.
[286] DUVAC, Constantin. Accesul ilegal la un sistem informatic în reglementarea noului Cod penal. În: *Revista română de dreptul proprietăţii intelectuale*, 2012, nr. 1, pp. 88-109. ISSN 1584-7241.
[287] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510
[288] DUVAC, Constantin. Accesul ilegal la un sistem informatic în reglementarea noului Cod penal. În: *Revista română de dreptul proprietăţii intelectuale*, 2012, nr. 1, pp. 88-109. ISSN 1584-7241.
[289] Ibidem.
[290] Ibidem.
[291] Ibidem.
[292] Ibidem.
[293] Ibidem.
[294] Ibidem.
[295] Ibidem.

informatice vizate de accesul ilegal se referă la o persoană [...] alta decât deţinătoarea sistemului informatic [...].”[296]

Cu referire la elementul material al infracţiunilor pertractate, C. Duvac afirmă: „Nu sunt întrunite elementele constitutive ale infracţiunii examinate dacă făptuitorul interacţionează cu un sistem informatic ce permite accesul liber sau gratuit al publicului”[297] „ori dacă se accesează un sistem informatic bun comun al celor doi soţi de către unul dintre aceştia în condiţiile în care acesta este în mod uzual folosit de fiecare dintre ei”[298], „iar datele informatice stocate nu sunt personalizate şi semnalizate ca atare prin criptare sau protejare”[299]; „Aceeaşi idee se susţine dacă se accesează unele date informatice stocate sau vehiculate de altă persoană care are acces la acelaşi computer”[300], „faptă despre care se afirmă însă că reprezintă o încălcare a reglementărilor din instituţia respectivă, pe linia protejării informaţiilor”[301]; „Acces ilegal la un sistem informatic în concurs real cu violarea secretului corespondenţei [reprezintă] accesarea aplicaţiei de poştă electronică pentru a obţine mesajele anterioare, primite sau trimise de către subiectul pasiv, în scopul obţinerii de date informatice”.[302]

Sunt nelipsite de interes opiniile autorului respectiv privitoare la cerinţele esenţiale pe care trebuie să le îndeplinească acţiunile incriminate în art. 360 CPR: „Acţionează fără drept persoana care se află în una dintre următoarele situaţii: nu este autorizată [...]”[303]; „depăşeşte limitele autorizării sau nu are permisiunea [...] de a efectua [...] operaţiuni într-un sistem informatic – art. 35 alin. (2) din Legea nr. 161/2003”[304]; „Nu acţionează fără drept însă cei care accesează sistemele informatice cu autorizarea celor în drept [...]”[305], „chiar dacă cel care le foloseşte în fapt (detentorul) nu este de acord cu o astfel de operaţiune realizată, de exemplu, cu ocazia unui control sau a unei verificări a activităţii detentorului.”[306]

Nu în ultimul rând, C. Duvac formulează concluzii care se referă la latura subiectivă a infracţiunilor prevăzute la art. 360 CPR: „Accesul ilegal la un sistem informatic, în variantele prevăzute în alin. (1) şi (3), se poate comite numai cu intenţie directă sau indirectă”[307];

[296] Ibidem.
[297] Ibidem.
[298] Ibidem.
[299] Ibidem.
[300] Ibidem.
[301] Ibidem.
[302] Ibidem.
[303] Ibidem.
[304] Ibidem.
[305] Ibidem.
[306] Ibidem.
[307] Ibidem.

„Săvârşirea din culpă a faptei prevăzute în art. 360 C. pen. nu atrage incidenţa acestui text”[308]; „Scopul este o condiţie constitutivă a infracţiunii numai în cazul variantei agravate prevăzute în alin. 2 al textului”[309]; „În acest caz, forma de vinovăţie specifică acestei infracţiuni este intenţia directă calificată prin scop. Cerinţa esenţială referitoare la scop constă în obţinerea de date informatice.”[310]

În 2013 a fost publicat articolul științific elaborat de către *T. Medeanu* și *A. Crăciunescu.*[311]

În debutul acestui articol cei doi autori examinează problemele ce țin de: reglementarea infracţiunilor informatice şi necesitatea prevenirii lor; caracterul transnaţional şi complexitatea unor infracţiuni din acest domeniu. Totuși, interesul cel mai mare îl comportă analiza infracţiunilor prevăzute la art. 360 CPR.

Examinând obiectul juridic special al acestor infracţiuni, T. Medeanu și A. Crăciunescu enunță că acesta îl constituie „relaţiile sociale referitoare la ocrotirea şi apărarea sistemelor informatice şi la securitatea datelor informatice.”[312] Obiectul material al infracţiunilor prevăzute la art. 360 CPR este caracterizat astfel de către autorii în cauză: „sistemul informatic în care se realizează accesul fraudulos.”[313]

Caracteristicile subiecţilor acestor infracţiunii, evocate de cei doi autori, nu diferă mult de respectivele caracteristici prezentate mai sus, evidențiate de către alți doctrinari: „Subiectul activ [...] poate fi orice persoană fizică ce întruneşte condiţiile de vârstă şi responsabilitate prevăzute de legea penală”[314]; „În general, aceste persoane sunt experţi în calculatoare şi reţelele de calculatoare, sau persoane care dispun de un set de cunoştinţe în domeniu”[315]; „Subiect activ poate fi şi o persoană juridică cu limitările şi în condiţiile prevăzute în art. 135 C.pen.”[316]; „Subiectul pasiv al infracţiunii poate fi persoana fizică sau juridică deţinătoare de drept a sistemului informatic, chiar dacă nu i s-a cauzat în acest mod un prejudiciu”[317]; „Poate fi subiect pasiv secundar şi altă persoană [...] în cazul în care datele informatice vizate de accesul ilegal se referă la o persoană [...] alta decât deţinătoarea sistemului informatic”[318]; „În această ipostază se

---

[308] Ibidem.
[309] Ibidem.
[310] Ibidem.
[311] MEDEANU, Tiberiu, CRĂCIUNESCU, Adrian. Accesul ilegal la un sistem informatic elemente constitutive şi delimitarea de alte infracţiuni. În: *Sesiunii ştiinţifice internaţionale „Uniunea Europeană – spaţiu de libertate, securitate şi justiţie” (Academia de Poliţie, Bucureşti, 23 mai 2013)*. Bucureşti: Editura Universitară, pp. 28-37. ISBN 978-606-591-723-1.
[312] Ibidem.
[313] Ibidem.
[314] Ibidem.
[315] Ibidem.
[316] Ibidem.
[317] Ibidem.
[318] Ibidem.

găseşte persoana inclusă în sistemul informatic accesat ilegal, care poate suferi consecinţe de ordin moral, financiar, administrativ, juridic ori de altă natură."[319]

Sub aspectul laturii obiective a infracţiunilor prevăzute la art. 360 CPR, T. Medeanu și A. Crăciunescu relevă elementul material al acestora: „Accesul ilegal va exista în cazul găsirii şi utilizării unei căi de intrare într-un alt sistem de calcul, în condiţiile în care nu avea dreptul să facă acest lucru"[320]; „Accesarea unor date informatice stocate sau vehiculate de altă persoană care are acces la acelaşi computer, nu reprezintă infracţiunea de acces ilegal la un sistem informatic [...]."[321]

În același context, cei doi autori scot în evidență un aspect de maximă relevanță ce ține de latura obiectivă a infracţiunilor prevăzute la art. 360 CPR: „Cerinţa esenţială pentru existenţa infracţiunii constă în realizarea accesului „fără drept""[322]; „În sensul legii penale, acţionează fără drept persoana care se află în una dintre următoarele situaţii: nu este autorizată [...]"[323]; „depăşeşte limitele autorizării"[324]; „nu are permisiunea [...] de a efectua [...] operaţiuni într-un sistem informatic."[325]

În sfârșit, nu poate fi trecută cu vederea opinia lui T. Medeanu și A. Crăciunescu cu privire la latura subiectivă a infracțiunilor respective: „Infracţiunea de bază poate fi săvârşită cu intenţie directă sau indirectă"[326]; „În cazul formelor agravate prevăzute în alin. (2) şi (3), forma de vinovăţie specifică este intenţia directă calificată prin scop sau prin înlăturarea restricţiilor de accesare a sistemului informatic"[327]; „Cerinţa esenţială referitoare la scop constă în obţinerea de date informatice"[328].; „Pentru consumarea acesteia nu este necesar să se realizeze, prin acţiunea ilicită a făptuitorului, obţinerea de date informatice"[329]; „Pentru existenţa elementului subiectiv, în această ipoteză de incriminare, este suficient să se constate că făptuitorul, prevăzând rezultatul faptei sale a urmărit obţinerea unor date informatice."[330]

---

[319] Ibidem.
[320] Ibidem.
[321] Ibidem.
[322] Ibidem.
[323] Ibidem.
[324] Ibidem.
[325] Ibidem.
[326] Ibidem.
[327] Ibidem.
[328] Ibidem.
[329] Ibidem.
[330] Ibidem.

Teza de doctor habilitat în drept, susținută în 2016 de către *V.G. Stepanov-Eghianț*[331], este o altă publicație consacrată analizei accesului ilegal la informația computerizată.

Acest autor a întreprins, printre altele, analiza infracțiunilor prevăzute la art. 272 CP FR. În viziunea lui V.G. Stepanov-Eghianț, valoarea socială din cadrul obiectului juridic generic al acestor infracțiuni constă în „crearea, păstrarea, utilizarea sau transmiterea în siguranță a informației computerizate."[332] Același autor exprimă poziția că obiectul juridic special al infracțiunilor ce sunt prevăzute de art. 272 CP FR este format din „relațiile sociale care asigură dreptul proprietarului informației computerizate la crearea, păstrarea, utilizarea și transmiterea acesteia în condiții de siguranță."[333]

Ca obiect imaterial al infracțiunilor respective, V.G. Stepanov-Eghianț vede „nu oricare informație în formă computerizată, ci doar aceea care este protejată de lege".[334] În viziunea aceluiași autor, „accesul ilegal se poate face în două moduri: fie prin sustragerea suportului în sine al informației computerizate [...]"[335], „urmată de accesarea informației computerizate stocate pe acesta"[336], „fie prin interceptarea informației computerizate pe calea folosirii mijloacelor tehnice computerizate. Majoritatea infracțiunilor sunt comise în al doilea mod."[337] După V.G. Stepanov-Eghianț, „infracțiunile prevăzute la art. 272 CP FR trebuie să [...] implice producerea uneia dintre urmările prejudiciabile specificate în dispoziția acestui articol."[338]

Cu privire la subiectul infracțiunilor examinate, doctrinarul în cauză susține: „Subiectul general al accesului ilegal la informația computerizată este persoană fizică responsabilă care a atins vârsta de 16 ani și care nu are dreptul de a accesa informația computerizată"[339]; „În ipoteza prevăzută la alin. 2 art. 272 CP FR, ne referim la un subiect special al infracțiunii, care comite accesul ilegal la informația computerizată folosind situația sa de serviciu."[340]

Referitor la latura subiectivă a infracțiunilor pertractate, V.G. Stepanov-Eghianț menționează „intenția directă sau indirectă, cu precizarea că intenția este manifestată în raport cu producerea urmărilor prejudiciabile enumerate în art. 272 CP FR."[341]

În 2016 este publicat un articol științific al cărui autor este *V. Stati*.[342]

---

[331] СТЕПАНОВ-ЕГИЯНЦ, В.Г. *Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект)*: дис. на соис. учен. степ. докт. юрид. наук. Москва, 2016. 389 с.
[332] Ibidem, c. 141.
[333] Ibidem, c. 145.
[334] Ibidem, c. 149.
[335] Ibidem, c. 167.
[336] Ibidem, c. 167.
[337] Ibidem, c. 167.
[338] Ibidem, c. 191.
[339] Ibidem, c. 237.
[340] Ibidem, c. 215.
[341] Ibidem, c. 237.

Scopul investigației întreprinse de acest autor se exprimă în analiza comparativă a infracțiunilor informatice (inclusiv a infracțiunilor de acces ilegal la informația computerizată) prevăzute de legile penale ale Republicii Moldova, României și Ucrainei. Întru realizarea acestui scop, V. Stati remarcă prezența în fiecare dintre cele trei legi penale a normelor care constituie expresia aderării Republicii Moldova, României și Ucrainei la Convenţia de la Budapesta.[343] În codurile penale ale acestor trei state sunt prezente articole în care se stabilește răspunderea pentru accesul ilegal la informația computerizată.

După părerea lui V. Stati, „scopul normelor din Capitolul XI din partea specială a Codului penal al Republicii Moldova este de a apăra ordinea de drept atât împotriva infracțiunilor informatice, cât și împotriva infracțiunilor în domeniul telecomunicațiilor”[344]; „Reieșind din normele Titlului XVI din partea specială a Codului penal al Codului penal al Ucrainei, obiectul protecției îl constituie relațiile sociale în sfera utilizării computerelor, a sistemelor și rețelelor de computere, precum și a rețelelor de telecomunicații”[345]; „Normele Capitolului VI din Titlul VII al părții speciale a Codului penal al României sunt destinate să apere ordinea de drept numai împotriva infracțiunilor care sunt îndreptate contra siguranței și integrității sistemelor și datelor informatice”[346]; „Domeniul de utilizare a rețelelor de telecomunicații nu este reprezentat de obiectul generic al acestor infracțiuni.”[347]

O altă comparație interesantă ține de subiectul infracțiunilor de acces ilegal la informația computerizată. După V. Stati, „subiectul infracțiunilor prevăzute la art. 259 CP RM poate fi doar persoana autorizată să utilizeze, să folosească, să administreze sau să controleze un sistem informatic”[348] „ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic”[349], „însă care nu are dreptul de acces la informația computerizată, depășește

---

[342] СТАТИ, Виталий. Компьютерные преступления в уголовном законодательстве Республики Молдова, Румынии и Украины: сравнительно-правовой анализ. În: *Kieler Ostrechts-Notizen*, 2016, nr. 2 - 2017, nr. 1, pp. 54-59. ISSN 1862-1589.

[343] Conform art. 2 al acestei convenții, „fiecare parte va adopta măsurile legislative și alte măsuri considerate necesare pentru a incrimina ca infracțiune”*, „potrivit dreptului său intern, accesarea intenționată și fără drept a ansamblului ori a unei părți a unui sistem informatic”*; „O parte poate condiționa o astfel de incriminare de comiterea încălcării respective prin violarea măsurilor de securitate”*, „cu intenția de a obține date informatice ori cu altă intenție delictuală, sau de legătura dintre încălcarea respectivă și un sistem informatic conectat la alt sistem informatic”.*

* *Convention on Cybercrime*. [citat 12.09.2020] Disponibil: https://rm.coe.int/1680081561

[344] СТАТИ, Виталий. Компьютерные преступления в уголовном законодательстве Республики Молдова, Румынии и Украины: сравнительно-правовой анализ. În: *Kieler Ostrechts-Notizen*, 2016, nr. 2 - 2017, nr. 1, pp. 54-59. ISSN 1862-1589.

[345] Ibidem.

[346] Ibidem.

[347] Ibidem.

[348] Ibidem.

[349] Ibidem.

limitele autorizării ori nu are permisiunea persoanei competente”[350]; „Pentru comparație, judecând după dispozițiile art. 360 CPR și ale alin. 1 art. 361 CPU, subiectul infracțiunilor corespunzătoare nu este unul special.”[351]

Cât privește scopul infracțiunilor de acces ilegal la informația computerizată, același autor relevă: „Conform art. 360 CPR, scopul obținerii de date informatice este special și, în același timp, agravează răspunderea”[352]; „În art. 259 CP RM și în alin. 1 art. 361 CPU, nu este specificat un asemenea scop.”[353]

În fine, nu poate fi ignorată comparația privitoare la persoana juridică – subiect al infracțiunilor de acces ilegal la informația computerizată: „Săvârșirea infracțiunilor prevăzute în Titlul XVI al părții speciale a Codului penal al Ucrainei nu este prevăzută în art. 96^3 din acest cod penal ca temei pentru aplicarea persoanelor juridice a unor măsuri cu caracter juridico-penal”[354]; „Pentru comparație, este posibil ca atât persoana fizică, cât și persoana juridică să aibă calitatea de subiecți ai infracțiunilor specificate în Capitolul VI din Titlul VII al părții speciale a Codului penal al României”[355]; „Legiuitorul moldovean are o abordare selectivă privind chestiunea în cauză: nu doar persoana fizică, ci și persoana juridică pot fi subiecți ai infracțiunilor prevăzute de art. 259 [...] CP RM”[356]; „Doar persoana fizică poate fi subiectul infracțiunilor specificate la art. 260^2, 260^5 și 260^6 CP RM.”[357]

În 2017 a fost susținută teza de doctor în drept a lui *I.R. Beghișev.*[358]

Acest autor face o constatare care prezintă relevanță și în contextul dreptului penal al Republicii Moldova: „Un neajuns semnificativ al legii penale în vigoare a Federației Ruse constă în decalajul dintre terminologia art. 272 CP FR[359] și starea actuală a dezvoltării științei și tehnologiei.”[360] Dezvoltând ideea, I.R. Beghișev explică de ce consideră anacronică terminologia art. 272 CP FR: „În acest articol este stabilită răspunderea pentru accesul ilegal doar la informația computerizată protejată de lege, deși, pe lângă sistemele informatice, informații cu caracter similar se găsesc în sistemele de telecomunicații [...]”[361]; „În afară de obiectele în care

---

[350] Ibidem.
[351] Ibidem.
[352] Ibidem.
[353] Ibidem.
[354] Ibidem.
[355] Ibidem.
[356] Ibidem.
[357] Ibidem.
[358] БЕГИШЕВ, И.Р. *Понятие и виды преступлений в сфере обращения цифровой информации*: дис. на соиск. учен. степ. канд. юрид. наук. Казань, 2017. 204 с.
[359] În acest articol este incriminat accesul ilegal la informația computerizată.
[360] БЕГИШЕВ, И.Р. *Понятие и виды преступлений в сфере обращения цифровой информации*: дис. на соиск. учен. степ. канд. юрид. наук. Казань, 2017, с. 53. 204 с.
[361] Ibidem, с. 53.

se află și circulă informația deja menționate în art. 272 CP FR, în acest articol trebuie specificate alte tipuri ale acestora, și anume dispozitivele de informații și telecomunicații, sistemele și rețelele acestora."[362]

Din perspectiva perfecționării dispozițiilor referitoare la accesul ilegal la informația computerizată, comportă interes următoarea aserțiune a lui I.R. Beghișev: „În art. 272 CP FR, până în decembrie 2011, ca obiect de localizare a informației computerizate era specificat suportul material de astfel de informații"[363]; „Se pare că prin „suporturi materiale de informații computerizate" se au în vedere mașinile, mecanismele și diverse echipamente destinate memorării și înregistrării unor asemenea informații"[364]; „Atunci când legiuitorul rus a utilizat sintagma „suport material de informații computerizate", el a avut în vedere [...] elementul de stocare a informațiilor computerizate, care face parte dintr-un computer"[365]; „Însă, sistemele de telecomunicații nu sunt mașini de felul lor"[366]; „Actualmente, în afară de computere, suporturi de informații computerizate pot diverse unități flash, hard disk-uri amovibile, CD-uri etc."[367]; „În legătură cu cele menționate mai sus, susținem punctul de vedere al legiuitorului cu privire la excluderea sintagmei „suport material de informații computerizate" din dispoziția art. 272 CP FR."[368] Cu această ocazie, consemnăm că o sintagmă asemănătoare este folosită în art. 259 CP RM.

În 2018 a fost publicată lucrarea elaborată de către *A.N. Popov.*[369]

În cadrul acestei lucrări distingem analiza infracțiunilor de acces ilegal la informația computerizată. În opinia autorului respectiv, obiectul juridic generic al infracțiunilor prevăzute la art. 272 CP FR, îl formează „securitatea informațională ca parte a securității publice".[370] Referitor la valoarea socială din cadrul obiectului juridic special al infracțiunilor analizate, A.N. Popov recurge la o formulare generală care s-ar potrivi în aceeași măsură obiectelor juridice speciale ale celorlalte infracțiuni prevăzute în Capitolul 28 din partea specială a Codului penal al Federației Ruse: „starea de protecție a persoanei, societății și statului împotriva amenințărilor informaționale".[371] La fel de lipsită de concretețe este părerea autorului în cauză cu privire la

[362] Ibidem, c. 53-54.
[363] Ibidem, c. 54.
[364] Ibidem, c. 54.
[365] Ibidem, c. 54.
[366] Ibidem, c. 54.
[367] Ibidem, c. 54.
[368] Ibidem, c. 54.
[369] ПОПОВ, А.Н. *Преступления в сфере компьютерной информации*. Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. 68 с.
[370] Ibidem, c. 21.
[371] Ibidem, c. 22.

obiectul material sau imaterial al infracțiunilor prevăzute la art. 272 CP FR: „În sens larg, tot ceea ce formează infrastructura informațională poate fi considerat obiect material sau imaterial al infracțiunilor în sfera informației computerizate.”[372]

Caracterizând latura obiectivă a faptelor infracționale de acces ilegal la informația computerizată, A.N. Popov afirmă: „Latura obiectivă a infracțiunilor, prevăzute de art. 272 CP FR, include trei semne obligatorii: 1) accesul ilegal la informația computerizată protejată de lege”[373]; „2) urmările prejudiciabile sub forma distrugerii, blocării, modificării sau copierii informației în cauză”[374]; „3) legătura de cauzalitate dintre accesul ilegal la informația computerizată protejată de lege și urmările prejudiciabile prevăzute de lege”[375]; „Accesul la informația computerizată presupune aflarea conținutului acesteia și utilizarea acesteia [...].”[376]

În rezultatul examinării laturii subiective a infracțiunilor de acces ilegal la informația computerizată, același doctrinar susține: „Accesul ilegal la informația computerizată protejată de lege poate fi comisă doar intenționat”[377]; „Însă, aceasta nu înseamnă că infracțiunile prevăzute la art. 272 CP FR, pot fi săvârșite exclusiv intenționat”[378]; „Or, legea stabilește răspunderea penală nu pentru accesul ilegal în sine, ci pentru acțiunea care urmează accesului ilegal”[379]; „Prin urmare, forma vinovăției trebuie stabilită în raport cu urmările prejudiciabile sub forma distrugerii, blocării, modificării sau copierii informației computerizate”[380]; „În art. 272 CP FR nu se menționează că infracțiunile corespunzătoare pot fi săvârșite doar din imprudență”[381]; „Având în vedere dispoziția alin. 2 art. 24 CP FR[382], se poate concluziona că infracțiunile, prevăzute la art. 272 CP FR, pot fi săvârșite cu intenție sau din imprudență”[383]; „Dacă făptuitorul a săvârșit cu intenție accesul ilegal la informația computerizată protejată de lege, iar această faptă a cauzat din imprudență modificarea informației în cauză, constatăm temeiul aplicării art. 272 CP FR.”[384]

---

[372] Ibidem, c. 22.
[373] Ibidem, c. 33.
[374] Ibidem, c. 33.
[375] Ibidem, c. 33.
[376] Ibidem, c. 33.
[377] Ibidem, c. 37.
[378] Ibidem, c. 37.
[379] Ibidem, c. 37.
[380] Ibidem, c. 37.
[381] Ibidem, c. 37.
[382] Conform acestei dispoziții, „faptă, comisă doar din imprudență, se consideră infracțiune numai dacă această formă de vinovăție este menționată expres în articolul corespunzător din partea specială a prezentului cod.”*
* Уголовный кодекс Российской Федерации. În: *Собрание законодательства Российской Федерации*, 1996, № 25.
[383] ПОПОВ, А.Н. *Преступления в сфере компьютерной информации*. Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018, с. 37. 68 с.
[384] Ibidem, c. 37.

În ceea ce privește subiectul infracțiunilor de acces ilegal la informația computerizată, A.N. Popov opinează: „Se are în vedere orice persoană fizică responsabilă care a atins vârsta de 16 ani”[385], „care a săvârșit accesul ilegal la informația computerizată protejată de lege, ceea ce a cauzat urmările prejudiciabile prevăzute de lege.”[386]

Din 2019 datează lucrarea monografică elaborată de către *T.I. Sozanski, S.Ia. Burda* și *A.Ia. Skiba.*[387]

Acești autori examinează, printre altele, infracțiunile prevăzute la art. 361 CPU. În viziunea lui T.I. Sozanski, S.Ia. Burda și A.Ia. Skiba, obiectul juridic al acestor infracțiuni îl constituie „dreptul de proprietate asupra informației computerizate și relațiile sociale cu privire la prestarea și beneficierea de serviciile de telecomunicații.”[388] Nu este clar dacă teoreticienii respectivi se referă la obiectul juridic generic sau la obiectul juridic special al infracțiunilor ce sunt prevăzute de art. 361 CPU.

În contextul pertractării obiectului material sau imaterial al infracțiunilor în cauză, T.I. Sozanski, S.Ia. Burda și A.Ia. Skiba definesc noțiunile „computer”, „sistem automatizat” etc. Latura obiectivă a infracțiunilor prevăzute la art. 361 CPU este descrisă astfel de cei trei autori: „Latura obiectivă se exprimă în modificarea regimului de funcționare a computerului, a sistemului de computere sau a rețelei de computere”[389], „pe calea influențării asupra suportului de informație computerizată sau a mijlocului de prelucrare automată a acesteia.”[390] Analizând același element constitutiv al infracțiunilor în cauză, T.I. Sozanski, S.Ia. Burda și A.Ia. Skiba stabilesc conținutul faptei prejudiciabile specificate în art. 361 CPU: „modificarea regimului de funcționare a computerului, a sistemului de computere sau a rețelei de computere”[391], „pe calea influențării asupra suportului de informație computerizată sau a mijlocului de prelucrare automată a acesteia”[392], „săvârșită cu încălcarea regimului de acces la informația computerizată, stabilit de legislație, ceea ce aduce atingere relațiilor sociale de proprietate asupra informației computerizate.”[393]

---

[385] Ibidem, c. 37.
[386] Ibidem, c. 37.
[387] СОЗАНСЬКИЙ, Т.І., БУРДА, С.Я., СКИБА, А.Я. *Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку у схемах*. Львів: Львівський державний університет внутрішніх справ, 2019. 20 с.
[388] Ibidem, c. 7.
[389] Ibidem, c. 7.
[390] Ibidem, c. 7.
[391] Ibidem, c. 8.
[392] Ibidem, c. 8.
[393] Ibidem, c. 8.

În continuare, sunt definite toate acele concepte care se referă la urmările prejudiciabile ce sunt prevăzute de art. 361 CPU. Analiza finalizează cu investigarea trăsăturilor individualizante ale subiectului și ale laturii subiective a infracțiunilor prevăzute de acest articol.

La fel, din 2019 datează articolul științific care a fost elaborat de către *A.T. Drăgan.*[394]

În cadrul analizei efectuate se distinge examinarea infracțiunilor de acces ilegal la un sistem informatic conform reglementărilor Codului penal al României. În acest context, A.T. Drăgan acordă atenție: conținutului legal al infracțiunilor în cauză; comparării prevederilor relevante din Codul penal al României în vigoare cu prevederile corespondente din legea penală română anterioară; elementelor preexistente ale faptelor infracționale prevăzute de art. 360 CPR; structurii și conținutului juridic al infracțiunilor respective; pedepselor pentru infracțiunile prevăzute de art. 360 CPR; aspectelor procedurale legate de aceste infracțiuni, etc.

Comportă originalitate viziunea enunțată de doctrinarul în cauză referitor la obiectul juridic al infracțiunilor prevăzute de art. 360 CPR: „Obiectul juridic este valoarea socială numită „sistem informatic" și relațiile sociale care apar în legătură cu utilizarea sistemelor automate de prelucrare a datelor."[395] Nu este clar dacă această opinie se referă la obiectul juridic generic sau la obiectul juridic special al infracțiunilor analizate.

În legătură cu obiectul material sau imaterial al infracțiunilor prevăzute de art. 360 CPR, A.T. Drăgan susține că acesta „este reprezentat de entitățile materiale ce alcătuiesc [sistemul informatic] [...], precum și de datele computerizate [...]."[396]

În ceea ce privește subiecții infracțiunilor prevăzute la art. 360 CPR, A.T. Drăgan relevă: „Subiect activ poate fi orice persoană [...] care are discernământ penal. Nicio calitate specială nu este cerută de lege în acest scop" [397]; „Subiect pasiv al infracțiunii este persoana [...] care deține sisteme informatice și al cărui drept la integritate, confidențialitate și disponibilitate a sistemelor informatice sau a datelor computerizate a fost încălcat sau pus în pericol" [398]; „Poate exista un subiect pasiv colectiv [...] atunci când accesul la sistemul informatic generează automat acces ilegal la alte sisteme similare interconectate cu primul."[399]

Nu putem face abstracție de reflecțiile lui A.T. Drăgan cu privire la elementul material al infracțiunilor prevăzute la art. 360 CPR: „Accesul ilegal la un sistem informatic are loc adesea

[394] DRĂGAN, Alin Teodorus. Illegal access to a computer system from the standpoint of the current Criminal Code. În: *Journal of Legal Studies "Vasile Goldiş"*, 2019, nr. 23, pp. 33-43. ISSN 1582-5442.
[395] Ibidem.
[396] Ibidem.
[397] Ibidem.
[398] Ibidem.
[399] Ibidem.

prin utilizarea tehnicilor de inginerie socială”[400]; „Făptuitorul poate studia site-ul web al companiei [...] pentru a obține numele managerilor și apoi apela telefonic compania respectivă, pretinzând că este noul tehnician IT”[401]; „Făptuitorul îi poate comunica persoanei care răspunde la telefon că trebuie să-și actualizeze computerul de la distanță, dar că și-a pierdut parola, după care să ceară amabil parola de la interlocutor”[402]; „În ceea ce privește cerința esențială, legiuitorul prevede necesitatea accesului fără drept (ilegal)”[403] „În sensul articolului în cauză, persoana care se află în una dintre următoarele situații acționează fără drept: „a) nu este autorizată, în condițiile legii sau prin contract”[404]; „b) depășește limitele autorizației”[405]; „c) nu are permisiunea persoanei fizice sau juridice care are competența de a o acorda.”[406]

Studiul lui A.T. Drăgan se încheie cu examinarea laturii subiective a faptelor infracționale ce sunt prevăzute de art. 360 CPR: „Fapta poate fi comisă cu intenție directă ori indirectă”[407]; În cazul variantei agravate prevăzute la alin. (2), forma vinovăției este intenția directă, calificată de scop”[408]; „Textul incriminator prevede cerința unui scop numai în cazul alin. (2): cel de obținere a datelor informatice.”[409]

Din același an 2019 datează articolul științific al cărui autor este *V. Stati.*[410]

În acest articol, accesul ilegal la informația computerizată este analizat dintr-o perspectivă concretă, și anume din cea a legăturii acestei fapte cu fabricarea sau punerea în circulație a monedelor virtuale în Republica Moldova.

În special, V. Stati menționează: „Miningul poate atrage răspunderea penală în ipoteza despre care ne vorbesc V.A. Perov și R. Abrihan. Astfel, primul dintre acești autori menționează „utilizarea unui program-virus de computer care permite folosirea unui anumit procent din puterea de calcul a computerului infectat, pentru ca făptuitorul să poată practica mining”.[411] La rândul său, R. Abrihan opinează: „Minarea profitabilă de monede necesită o cantitate imensă de

---

[400] Ibidem.
[401] Ibidem.
[402] Ibidem.
[403] Ibidem.
[404] Ibidem.
[405] Ibidem.
[406] Ibidem.
[407] Ibidem.
[408] Ibidem.
[409] Ibidem.
[410] STATI, Vitalie. Fabricarea sau punerea în circulație a monedelor virtuale în Republica Moldova: conotații juridico-penale. În: *Актуальные научные исследования в современном мире // Журнал*. Переяслав, 2019, Вып. 11, ч. 5, с. 100-108. ISSN 2524-0986.
[411] ПЕРОВ, В.А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют. În: *Безопасность бизнеса*, 2018, № 2, с. 25-29. ISSN 2072-3644.

putere de calcul”[412], „de aceea atacatorii instalează programe malware pe computerele utilizatorilor pentru a „sustrage” puterea de calcul necesară”[413].[414]

După care V. Stati continuă: „În circumstanțele descrise de cei doi autori precitați, este aplicabil art. 260^6 CP RM”[415], „care prevede răspunderea, printre altele, pentru introducerea datelor informatice în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă aceste acţiuni au cauzat daune în proporţii mari”[416]; „În afară de aceasta, este aplicabilă prevederea de la lit. f) alin. (2) art. 259 CP RM”[417], „care stabilește răspunderea pentru accesul ilegal la informaţia computerizată, săvârşit cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice”[418], „în scopul săvârşirii, *inter alia*, a uneia dintre infracţiunile prevăzute la art. 260^6 CP RM”.[419]

În concluzie la investigația pe care a întreprins-o, V. Stati susține: „Fabricarea sau punerea în circulație a monedelor virtuale nu reprezintă o problemă de natură penală în sine”[420]; „Astfel de activități dobândesc conotații penale în prezența unor condiții suplimentare”[421], „atunci când ele apar ca modalități faptice ale unor infracțiuni (de exemplu, ale infracțiunilor prevăzute la art. 196, 243, 259, 260, 260^4, 260^6, 279 din Codul penal).”[422]

Încheiem examinarea materialelor științifice referitoare la accesul ilegal la informaţia computerizată, publicate peste hotare, cu analiza tezei de doctor în drept susținute în anul 2019 de *D.O. Ricika.*[423]

În ceea ce privește obiectul juridic generic al faptelor infracționale prevăzute în Titlul XVI din partea specială a Codului penal al Ucrainei, după părerea doctrinarului respectiv, acesta îl formează „relațiile sociale care suferă atingere datorită influențării asupra informației care circulă în sistemele informatice.”[424] Atunci când caracterizează obiectul juridic special al

---

[412] ABRIHAN, Raluca. *Tendințe în securitate IT: România, peste medie la minare ilicită de criptomonede, atacuri phishing şi ransomware*. [citat 05.09.2020] Disponibil: https://www.startupcafe.ro/smart-tech/tendinte-securitate-it-atac-minare-ilegalacriptomonede-microsoft.htm
[413] Ibidem.
[414] STATI, Vitalie. Fabricarea sau punerea în circulație a monedelor virtuale în Republica Moldova: conotații juridico-penale. În: *Актуальные научные исследования в современном мире // Журнал*. Переяслав, 2019, Вып. 11, ч. 5, с. 100-108. ISSN 2524-0986.
[415] Ibidem.
[416] Ibidem.
[417] Ibidem.
[418] Ibidem.
[419] Ibidem.
[420] Ibidem.
[421] Ibidem.
[422] Ibidem.
[423] РИЧКА, Д.О. *Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку*: дис. на здоб. наук. ступ. канд. юрид. наук. Ірпінь, 2019, 212 с.
[424] Ibidem, c. 72.

infracțiunilor ce sunt prevăzute de art. 361 CPU, D.O. Ricika remarcă pluralitatea valorilor sociale specifice și a relațiilor sociale aferente, apărate împotriva infracțiunilor în cauză: „Obiectul [...] îl formează funcționarea normală a computerelor, a sistemelor automatizate, a rețelelor de computere și a rețelelor de telecomunicații”[425]; „Sensul normei constă în aceea că ea asigură ocrotirea relațiilor sociale de două tipuri: relațiile sociale de proprietate asupra informației computerizate și relațiile sociale cu privire la prestarea serviciilor de telecomunicații”[426]; „Proprietatea asupra informației computerizate constituie ansamblul drepturilor persoanei de a: poseda suportul de informație computerizată”[427]; „a folosi informația, stocată pe acest suport, în vederea satisfacerii necesităților informaționale”[428]; „a permite altora să utilizeze informația de pe suportul în cauză, să o modifice [...].”[429]

În ceea ce privește obiectul material sau imaterial al infracțiunilor prevăzute la art. 361 CPU, același doctrinar opinează că la acesta „se raportează informația computerizată și informația transmisă prin canalele de telecomunicații”[430]; „Dacă analizăm esența prevederilor acestui articol, atunci am putea conchide că obiectul material sau imaterial îl reprezintă: 1) computerele”[431]; „2) sistemele automatizate; 3) rețelele de computere; 4) rețelele de telecomunicații”[432]; „În realitate, nu este așa. Or, rolul cheie îl joacă tocmai informația care se află în entitățile sus-menționate”.[433]

În rezultatul analizei laturii obiective a infracțiunilor prevăzute la art. 361 CPU, D.O. Ricika afirmă că „accesul ilegal la informația computerizată se comite pe calea acțiunii”[434]; „Latura obiectivă îmbracă două forme alternative: 1) accesul ilegal la computere, la sisteme automatizate sau la rețele de computere”[435]; „2) accesul ilegal la rețelele de telecomunicații.”[436]

Referitor la latura subiectivă a infracțiunilor pertractate, doctrinarul în cauză susține că acestea pot fi săvârșite doar cu intenție directă sau indirectă. Analiza infracțiunilor, prevăzute la art. 361 CPU, o încheie examinarea caracteristicilor subiectului acestor infracțiuni.

---

[425] Ibidem, c. 75.
[426] Ibidem, c. 75.
[427] Ibidem, c. 75.
[428] Ibidem, c. 76.
[429] Ibidem, c. 76.
[430] Ibidem, c. 83.
[431] Ibidem, c. 83.
[432] Ibidem, c. 83.
[433] Ibidem, c. 83.
[434] Ibidem, c. 95.
[435] Ibidem, c. 95.
[436] Ibidem, c. 95.

1.3. Condiționarea socială și juridică a incriminării accesului ilegal la informația computerizată

Potrivit alin. (1) art. 2 din Codul penal al Republicii Moldova (în continuare – CP RM), „legea penală apără, împotriva infracţiunilor, [...] întreaga ordinea de drept”.[437] Din această dispoziție rezultă că legea penală apără cele relațiile și valorile sociale pe care societatea le consideră de maximă importanță. Opinia lui E.S. Gabidullin este: „Condiționarea socială a oricărui fenomen presupune necesitatea acestui fenomen, care rezultă din circumstanțele și condițiile sociale, legate de viața oamenilor în societate [...]”[438]. La rândul său, M.A. Efremova subliniază că „norma dreptului penal va fi eficientă numai dacă este condiționată social”[439]. Incriminarea și dezincriminarea anumitor fapte constituie vectori importanți în procesul de implementare a politicii penale. În funcție de necesitățile societății, sunt incriminate sau dezincriminate fapte îndreptate împotriva acestor relații și valori. Astfel, incriminarea sau dezincriminarea unei fapte este condiționată nu doar sub aspect juridic, dar și sub aspect social.

În funcție de condițiile istorice, de evoluția sau de involuția factorilor societali, se poate schimba cercul de valori și relații sociale apărate de legea penală. Necesitățile societății sunt direct dependente de aceste schimbări. Apariția unor interese complet noi ale societății și ale statului în sfera informațională a avut ca efect apariția unor manifestări socialmente periculoase fundamental noi, care nu se aflau în vizorul normelor penale existente. Răspândirea și utilizarea în anii '90 ai secolului trecut a primelor tehnologii informaționale a dus la apariția de noi relații sociale care nu se încadrau în tiparul celor existente. Apărarea penală a acestor relații a devenit în scurt timp o necesitate stringentă.[440]

Sub influența factorilor generatori de insecuritate societală, faptele, care până nu demult erau percepute ca socialmente utile sau socialmente neutre ori a căror natură nu era cunoscută suficient de către membrii societății, au devenit periclitante sub aspect social. Datoria legiuitorului este să declare infracționale faptele care au dobândit pericol social. N.E. Krâlova argumentează că „doar infracțiunile au un astfel de grad de prejudiciabilitate, pe care legiuitorul

---

[437] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

[438] ГАБИДУЛЛИН, Э.С. Социальная обусловленность как основание уголовно-правового запрета. În: *Журнал правовых и экономических исследований*, 2017, № 4, с. 32-37. ISSN 1995-1248.

[439] ЕФРЕМОВА, М.А. *Уголовно-правовая охрана информационной безопасности*: дис. на соиск. учен. степ. докт. юрид. наук. Москва, 2018, с. 84. 427 с.

[440] STRÎMBEANU, Alexandru. Condiționarea socială și juridică a incriminării accesului ilegal la informația computerizată. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234976

îl numește „pericol social”. Alte fapte ilegale nu-l posedă”[441]. Totodată, M.M. Dolghieva consideră că „legiuitorul ar trebui să recurgă la incriminare numai atunci când nu există măsuri alternative de influențare [...]”[442]; „Într-un asemenea caz, unele interese ale societății urmează a fi sacrificate în favoarea altora”[443]; „Tocmai de aceea incriminarea trebuie să fie aprobată de societate.”[444] Așadar, incriminarea poate genera efecte sociale negative și ar trebui invocată la cazuri excepționale, cu titlu de *ultima ratio*.

În pct. 45 din Raportul explicativ la Convenţia Consiliului Europei privind criminalitatea informatică se glosează: „Cel mai eficient mijloc de prevenire a accesului neautorizat [la un sistem informatic] este, desigur, introducerea și dezvoltarea unor măsuri de securitate eficiente”[445]; „Cu toate acestea, un răspuns cuprinzător trebuie să includă, de asemenea, amenințarea aplicării și aplicarea propriu-zisă a măsurilor de drept penal”[446]; „O interdicție penală a accesului neautorizat [...] poate oferi [...] o protecție suplimentară împotriva pericolelor descrise mai sus chiar și la o etapă timpurie.”[447]

În pct. 35 al Hotărârii Guvernului nr. 857 din 31.10.2013 cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020” este stipulat: „Pe cât o societate este mai informatizată, cu atât este mai mult expusă riscurilor cibernetice”[448], „iar asigurarea securităţii spaţiului cibernetic trebuie să constituie o preocupare majoră a tuturor actorilor implicaţi, mai ales la nivel instituţional [...]”[449]; Prin securitate cibernetică se înţelege starea de normalitate rezultată în urma aplicării [...] de măsuri [...] prin care se asigură confidenţialitatea”[450], „integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic.”[451]

---

[441] КРЫЛОВА, Н.Е. Существует ли уголовное право «в широком смысле слова». În: *Научные основы уголовного права и процессы глобализации: материалы V Российского конгресса уголовного права, 27-28 мая 2010 г.* Москва: Проспект, 2010, с. 721-727. ISBN 978-5-392-01701-0.
[442] ДОЛГИЕВА, М.М. Социальная обусловленность возникновения уголовно-правовых запретов нарушений, совершаемых в сфере оборота криптовалюты. În: *Актуальные проблемы российского права*, 2018, № 10, с. 225-235. ISSN 1994-1471.
[443] Ibidem.
[444] ДОЛГИЕВА, М.М. Социальная обусловленность возникновения уголовно-правовых запретов нарушений, совершаемых в сфере оборота криптовалюты. În: *Актуальные проблемы российского права*, 2018, № 10, с. 225-235. ISSN 1994-1471.
[445] *Explanatory Report to the Convention on Cybercrime*. [citat 30.12.2022] Disponibil: https://rm.coe.int/16800cce5b
[446] Ibidem.
[447] Ibidem.
[448] Hotărârea Guvernului cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”: nr. 857 din 31.10.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 252-257, 963.
[449] Ibidem.
[450] Ibidem.
[451] Ibidem.

În acelaşi act normativ se menționează: „Globalitatea spaţiului cibernetic este de natură să amplifice riscurile la adresa acestora afectând în aceeaşi măsură atât sectorul privat, cât şi cel public”[452]; „Ameninţările din spaţiul cibernetic se materializează prin exploatarea vulnerabilităţilor de natură umană, tehnică şi procedurală”[453], „cel mai adesea în: 1) atacuri cibernetice împotriva infrastructurilor care susţin funcţii de utilitate publică [...]”[454]; „2) accesarea neautorizată a infrastructurilor cibernetice; 3) modificarea, ştergerea sau deteriorarea neautorizată de date informatice ori restricţionarea ilegală a accesului la aceste date”[455]; „4) spionajul cibernetic; 5) cauzarea unui prejudiciu patrimonial, [...].”[456]

Privită prin prisma acestor formulări, semnificația axiologică a relațiilor sociale din domeniul informatic nu poate fi tăgăduită. Ea poate fi comparată cu semnificația axiologică a relațiilor sociale cu privire la securitatea publică și cu cea a relațiilor sociale cu privire la patrimoniu. În opinia lui D.S. Azarov, „relațiile sociale din domeniul informatic sunt direct legate de: 1) toate sferele vieții în care informațiile sunt stocate, prelucrate, utilizate într-o formă computerizată”[457]; „2) relațiile de proprietate (deoarece datele informatice reprezintă un obiect al dreptului de proprietate)”[458]. Apreciind că omisiunea de incriminare a ameninţărilor din spaţiul cibernetic specificate mai sus ar fi în detrimentul societății, legiuitorului nu-i rămâne decât să le declare infracționale. În caz contrar, vulnerabilitatea relațiilor sociale din domeniul informatic ar submina continuu agregatul social. Aceasta determină necesitatea de a apăra pe cale penală respectivele relații.

L. Spînu-Dumneanu menționează just că „tehnologiile informaţionale, inclusiv orice sistem de calculatoare reţine, la momentul actual, oportunităţi şi necesităţi noi”[459], „de încălcare a prevederilor normative şi creează un potenţial sporit de săvârşire a unor [...] infracţiuni comise altfel decât în modurile cunoscute până la momentul actual”[460]; „Comunitatea în principiu, este nevoită să ofere tribut pentru toate daunele de orice natură cauzate de „criminalitatea

---

[452] Ibidem.
[453] Ibidem.
[454] Ibidem.
[455] Ibidem.
[456] Ibidem.
[457] АЗАРОВ, Д.С. *Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)*. Київ: Атіка, 2007, с. 20. 304 с. ISBN 966-326-230-3.
[458] Ibidem, с. 20.
[459] SPÎNU-DUMNEANU, L. Evoluările internaţionale şi naţionale în domeniul infracţiunilor informatice. În: *Realități și perspective ale învățământului juridic național. Culegerea materialelor științifice elaborate în baza comunicărilor de la Conferinţa ştiinţifică naţională cu participare internaţională, organizată cu ocazia a 60 de ani de la înființarea Facultății de Drept (USM, 01-02 octombrie 2019, Chișinău)*. Chișinău: CEP USM, 2020, pp. 112-120. ISBN 978-9975-149-80-8.
[460] Ibidem.

informatică""[461], „aceasta continuă să se bazeze pe sistemele computerizate în aproape toate domeniile vieţii sociale: controlul mijloacelor de transport, inclusiv traficului aerian, al trenurilor şi metrourilor, diriguirea domeniului medical sau al securităţii naţionale".[462]

De asemenea, M. Dobrinoiu accentuează că „o singură breşă realizată în operarea [sistemelor informatice] poate pune în pericol vieţi omeneşti"[463], „ceea ce denotă faptul că dependenţa societăţii de sistemele informatice a căpătat o dimensiune mult mai profundă decât cea intuită iniţial"[464]; „Expansiunea [...] reţelelor de calculatoare [...] a dus la creşterea vulnerabilităţii acestor sisteme şi la crearea de oportunităţi pentru producerea de infracţiuni."[465]

Astfel, factorii, care determină necesitatea de a atribui ilicitate infracțională accesului ilegal la informaţia computerizată, sunt de ordin social-juridic și social-economic: intensificarea schimbului de informații între persoanele fizice, persoanele juridice și state; penetrarea tehnologiilor informaționale în toate domeniile activității umane; utilizarea masivă a comunicațiilor prin satelit, a calculatoarelor și a rețelelor de calculatoare; creșterea nivelului de disponibilitate a membrilor societății de a comunica prin sistemele informatice; condiționarea tot mai frecventă a participării la diverse activități sociale de prezența abilităților legate de computer, de internet și de soft-ul de specialitate; accentuarea dependenţei competitivității economice a unei țări, a unui domeniu economic, a unei întreprinderi etc. de folosirea tehnologiilor informaţionale; globalitatea și caracterul transnațional al rețelelor prin intermediul cărora decurge comunicarea intermediată de computer; posibilitatea accesării simultane de către o singură persoană a sute și mii de computere amplasate atât în aceeași țară, cât și în diferite țări; dificultățile de probare a săvârșirii accesului ilegal la informaţia computerizată; latența sporită a acestei fapte, etc.

Apariția în legea penală a Republicii Moldova a dispozițiilor de incriminare a faptelor, îndreptate contra relațiilor sociale din domeniul informatic, a reprezentat un pas firesc și previzibil. Prin Legea nr. 830 din 07.02.2002 privind completarea Codului penal şi a Codului de procedură penală[466] (în continuare – Legea nr. 830/2002), Codul penal al Republicii Moldova din 24.03.1961 a fost completat cu Capitolul VI[1] „Infracţiuni în domeniul tehnologiilor

[461] Ibidem.
[462] Ibidem.
[463] DOBRINOIU, Maxim. *Infracţiuni în domeniul informatic*. Bucureşti: C.H. Beck, 2006, p. 79. 401 p. ISBN 978-973-655-941-9.
[464] Ibidem, p. 79.
[465] Ibidem, p. 79.
[466] Legea privind completarea Codului penal și a Codului de procedură penală: nr. 830 din 07.02.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 46-48, 304.

informaţionale”.[467] Acest articol a cuprins următoarele articole: art. 176^1 „Accesul ilegal (nesancţionat) la informaţia computerizată”[468]; art. 176^2 „Însuşirea ilegală a informaţiei computerizate”[469]; art. 176^3 „Fabricarea sau desfacerea mijloacelor specifice în scopul obţinerii accesului ilegal (nesancţionat) la sistemul computerizat”[470]; art. 176^4 „Modificarea informaţiei computerizate”[471]; art. 176^5 „Sabotajul computerizat”[472]; art. 176^6 „Crearea, utilizarea sau răspândirea programelor dăunătoare”[473]; art. 176^7 „Încălcarea regulilor de exploatare a sistemului computerizat”.[474]

În ceea ce privește art. 176^1 CP RM din 1961, acesta avea două alineate și o notă: „Accesul ilegal (nesancţionat) la informaţia ce se păstrează în sistemul computerizat, cu încălcarea sistemului de protecţie, se pedepseşte cu amendă în mărime de la două sute până la cinci sute de salarii minime”[475]; „Aceeaşi acţiune săvârşită din imprudenţă, care a cauzat nimicirea sau blocarea informaţiei, precum şi scoaterea din funcţiune a utilajului computerizat ori alte urmări grave, se pedepseşte cu privaţiune de libertate pe un termen de până la doi ani sau cu amendă în mărime de la o sută până la şase sute de salarii minime”[476]; „Notă. În prezentul capitol, prin sistem computerizat se subînţeleg computerul, reţelele computerizate locale şi globale, precum şi suporţii electronici ai informaţiei.”[477]

Probabil, ca modele proxime pentru elaborarea art. 176^1 CP RM din 1961 au servit alin. 1 art. 349 din Codul penal al Republicii Belarus (în continuare – CP RBe) și art. 286 din Codul penal model al CSI. Astfel, alin. 1 art. 349 CP RBe stabilește răspunderea pentru „accesul neautorizat la informația ce se păstrează în sistemul computerizat, în rețea sau în suporturile de date”[478], „însoțit de violarea sistemului de protecție (accesul neautorizat la informația computerizată)”[479], „care a cauzat din imprudență modificarea, nimicirea sau blocarea informației ori scoaterea din funcţiune a utilajului computerizat ori alte daune considerabile.”[480] La rândul său, art. 286 din Codul penal model al CSI prevede răspunderea pentru: „(1) „accesul neautorizat la informația ce

[467] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
[468] Ibidem.
[469] Ibidem.
[470] Ibidem.
[471] Ibidem.
[472] Ibidem.
[473] Ibidem.
[474] Ibidem.
[475] Ibidem.
[476] Ibidem.
[477] Ibidem.
[478] *Уголовный Кодекс Республики Беларусь: № 275-З от 9 июля 1999 г.* [citat 06.03.2022] Disponibil: https://kodeksy-by.com/ugolovnyj_kodeks_rb.htm
[479] Ibidem.
[480] Ibidem.

se păstrează în sistemul computerizat, în rețea sau în suporturile de date”[481], „însoțit de violarea sistemului de protecție”[482], „care a cauzat din imprudență modificarea, nimicirea sau blocarea informației ori scoaterea din funcţiune a utilajului computerizat ori alte daune considerabile [...]”[483]; (2) „Acțiunile, prevăzute la alineatul 1 al acestui articol, care au cauzat din imprudență urmări grave [...]”[484]. Spre deosebire de infracțiunile ce sunt prevăzute de alin. 1 art. 349 CP RBe și alin. 1 art. 286 din Codul penal model al CSI, infracțiunea prevăzută la alin. 1 art. 176^1 CP RM din 1961 a fost concepută să aibă componență formală. Urmările prejudiciabile, inclusiv urmările grave, au fost specificate în alin. 2 art. 176^1 CP RM din 1961.

În momentul intrării în vigoare a art. 176^1 CP RM din 1961 nu a existat o normă penală în care să fie incriminată, ca modalitate normativă sau ca modalitate faptică, acțiunea de acces ilegal (nesancţionat) la informaţia computerizată. În acest mod, legiuitorul a respectat principiul neredundanței noii incriminări, care presupune, printre altele, imposibilitatea aplicării normelor de drept penal deja existente în raport cu fapta nou incriminată. În acel moment, în CP RM din 1961 existau doar două articole (art. 61 „Trădarea de Patrie” și art. 62 „Spionajul”) care prevedeau răspunderea pentru accesul ilegal la anumite categorii de informaţii (secret de stat sau un secret militar) care puteau îmbrăca o formă computerizată. În cazul în care obiectul imaterial al infracțiunilor prevăzute la art. 61 sau 62 CP RM din 1961 avea o formă computerizată, aceste articole reprezentau o normă specială în raport cu art. 176^1 CP RM din 1961. Respectiv, informațiile, care reprezentau obiectul imaterial al infracțiunii care este prevăzută la art. 176^1 CP RM din 1961, nu puteau să constituie un secret de stat sau un secret militar.

Relațiile, sociale care apăreau și se dezvoltau în legătură cu informațiile, ce reprezentau obiectul imaterial al infracțiunii care a fost prevăzută la art. 176^1 CP RM din 1961, au necesitat apărare penală datorită nerespectării de către făptuitor a regulilor referitoare la accesarea acestora. Nevoia de a incrimina accesul ilegal la informaţia computerizată a fost condiționată de interzicerea sau restricționarea accesului la o astfel de informație pentru anumite persoane. Această interdicție sau restricționare, sfidată de către făptuitor, determina intrarea acestuia în sistemul computerizat, cu încălcarea sistemului de protecţie, pentru a apela informații pe care făptuitorul nu era autorizat să le acceseze. Caracterizând o ipoteză asemănătoare cu cea descrisă în art. 259 CP RM, M.A. Dubko menționează just că „regimul juridic al informațiilor este o caracteristică a informației ca obiect al raporturilor juridice, care rezultă din caracterul imaterial

[481] *Модельный Уголовный кодекс. Рекомендательный законодательный акт для Содружества Независимых Государств*. [citat 06.03.2022] Disponibil: docs.cntd.ru/document/901781490
[482] Ibidem.
[483] Ibidem.
[484] Ibidem.

al acesteia”[485], „pe când cerințele privind protecția informațiilor sunt determinate de conținutul acestora, și nu de forma în care sunt prezentate.”[486] De asemenea, I.Iu. Bogdanovskaia confirmă că „diversele restricții privind informațiile sunt legate, în primul rând, de conținutul acesteia.”[487] Așadar, nu forma computerizată a informației, dar caracterul prohibit sau restricționat al accesării acesteia condiționează necesitatea incriminării faptei prevăzute la art. 259 CP RM.

La momentul intrării în vigoare a Legii nr. 830/2002 exista un sistem nu tocmai evoluat de relații sociale din domeniul informatic, care necesita apărare penală. Aceste relații constituiau obiectul de reglementare al Legii nr. nr. 1069/2000. Conform art. 1 al legii date, ea „stabileşte principalele reguli şi condiţii de activitate în domeniul informaticii în Republica Moldova”[488], „drepturile şi obligaţiile statului, ale persoanelor juridice şi fizice în procesul creării, administrării, utilizării şi întreţinerii sistemelor informatice”[489], „principiile şi măsurile de asigurare a libertăţii şi protecţiei datelor în sistemele informatice, dreptului de acces la serviciile informatice.”[490]

Art. 2 al Legii nr. 1069/2000 conține definițiile a două noțiuni utilizate în art. 176^1 CP RM din 1961: „acces neautorizat – acces la informaţii efectuat cu încălcarea regimului de lucru”[491]; „sistem informatic – ansamblu de programe şi echipamente care asigură prelucrarea automată a datelor.”[492] În afară de aceasta, unele norme din Legea nr. 1069/2000 stabilesc condițiile a căror încălcare constituie temeiul aplicării art. 176^1 CP RM din 1961: „Accesul [...] la informaţiile ce se conţin în sistemele informatice este asigurat în conformitate cu prevederile respective ale Constituţiei, prezentei legi şi altor acte legislative”[493] (alin. (1) art. 3); „Se interzice accesul şi conectarea neautorizate la sistemele şi reţelele informatice”[494] (alin. (3) art. 4); „Persoanele [...] au dreptul să obţină de la titularii bazelor de date, direct sau pe alte căi de acces, confirmarea că aceştia deţin sau nu date care se referă la persoana respectivă”[495] (alin. (1) art. 20); „Dreptul prevăzut la alin. (1) nu se extinde asupra activităţilor de informatică legale ce constituie informaţie oficială cu accesibilitate limitată, precum şi asupra datelor rezultate din asemenea

---

[485] ДУБКО, М.А. Основание и причины криминализации неправомерного завладения компьютерной информацией. În: Вестник Академии МВД Республики Беларусь, 2017, № 1, с. 87-91. ISSN 2079-9837.
[486] Ibidem.
[487] *Право на доступ к информации. Доступ к открытой информации* / Отв. ред. БОГДАНОВСКАЯ, И.Ю. Москва: Юстицинформ, 2009, с. 59. 344 с. ISBN 978-5-7205-1003-9.
[488] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova,* 2001, nr. 73-74, 547.
[489] Ibidem.
[490] Ibidem.
[491] Ibidem.
[492] Ibidem.
[493] Ibidem.
[494] Ibidem.
[495] Ibidem.

activităţi”[496] (alin. (2) art. 20); „Persoanele juridice şi fizice care încalcă prevederile prezentei legi poartă răspundere administrativă, materială sau penală, după caz, conform legislaţiei”[497] (art. 37). Putem vedea că aceste norme reglementează interzicerea sau restricționarea accesului la informațiile computerizate pentru anumite persoane.

La 12.06.2003 a intrat în vigoare actualul Cod penal. În scurt timp a fost adoptată Legea nr. 467/2003, care a dezvoltat și a consolidat sistemul de relații sociale din domeniul informatic. Conform alin. (1) art. 1 al acestei legi, ea „stabileşte regulile de bază şi condiţiile de activitate în domeniul creării şi dezvoltării infrastructurii informaţionale naţionale ca mediu de funcţionare al societăţii informaţionale din Republica Moldova”[498], „reglementează raporturile juridice care apar în procesul de creare, formare şi utilizare a resurselor informaţionale automatizate de stat, a tehnologiilor, sistemelor şi reţelelor informaţionale.”[499] Legea nr. 467/2003 conține anumite reglementări care stabilesc condițiile a căror încălcare constituie temeiul aplicării art. 259 CP RM (care a succedat art. 176[1] CP RM din 1961): „Resursele informaţionale de stat sunt publice şi accesibile tuturor”[500]; „Excepţie face informaţia documentată atribuită, conform legii, categoriei de informaţie cu acces limitat”[501] (art. 27); „Încălcarea prezentei legi se pedepseşte pe cale civilă, administrativă sau penală, în condiţiile legii”[502] (art. 32).

Dezvoltarea și consolidarea sistemului de relații sociale din domeniul informatic a continuat cu adoptarea Decretului Președintelui Republicii Moldova nr. 1743 din 19.03.2004 privind edificarea societăţii informaţionale în Republica Moldova. Conform acestuia, edificarea societăţii informaţionale în Republica Moldova a fost declarată drept una din prioritățile naţionale (art. 1), iar Guvernul și-a asumat sarcina de a aproba politica de edificare a societăţii informaţionale în Republica Moldova (lit. a) art. 2)[503].

În anul 2009 Republica Moldova a aderat la Convenția de la Budapesta. Conform art. 2 al acestei convenții, „fiecare parte va adopta măsurile [...] necesare pentru a incrimina ca infracțiune [...] accesarea intenționată și fără drept a ansamblului ori a unei părți a unui sistem informatic”[504]; „O parte poate condiționa o astfel de incriminare de comiterea încălcării

---

[496] Ibidem.
[497] Ibidem.
[498] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.
[499] Ibidem.
[500] Ibidem.
[501] Ibidem.
[502] Ibidem.
[503] Decretul Preşedintelui Republicii Moldova privind edificarea societăţii informaţionale în Republica Moldova: nr. 1743 din 19.03.2004. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 50, 300.
[504] Ibidem.

respective prin violarea măsurilor de securitate, cu [...] intenție delictuală [...]”[505]. Așadar, Republica Moldova a incriminat accesul ilegal la informaţia computerizată chiar înainte de a-și asuma angajamentul pe plan internațional de a incrimina o astfel de faptă.

În același context, vorbim despre art. 3 al Directivei 2013/40/UE, potrivit căruia „statele membre adoptă măsurile necesare pentru a garanta că accesarea cu intenție și fără drept a unui sistem informatic sau a unei părți a acestuia este incriminată”[506] „atunci când este săvârșită prin încălcarea unei măsuri de securitate, cel puțin atunci când nu reprezintă un caz minor.”[507] Acest din urmă articol trebuie privit prin prisma Acordului de asociere între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de o parte, și Republica Moldova, pe de altă parte.[508] Or, conform lit. g) parag. (1) art. 16 din acest acord, „părțile cooperează în ceea ce privește prevenirea și combaterea tuturor formelor de activități infracționale [...], cum ar fi [...] criminalitatea informatică.”[509]

Expresia firească a aderării țării noastre la Convenția de la Budapesta o constituie adoptarea Legii nr. 20/2009. Această lege, la fel ca Legea nr. 1069/2000 și Legea nr. 467/2003, stabilește condițiile a căror încălcare constituie temeiul aplicării art. 259 CP RM. Astfel, art. 2 al Legii nr. 20/2009 conține definițiile a două noțiuni necesare interpretării și aplicării art. 259 CP RM: „sistem informatic – orice dispozitiv izolat sau ansamblu de dispozitive [...] care asigură [...], prin executarea unui program, prelucrarea automată a datelor”[510]; „măsuri de securitate – folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori”.[511] Conform art. 6 al aceleiași legi, „proprietarii de sisteme informatice, accesul la care este interzis sau restricţionat pentru anumite categorii de utilizatori, au obligaţia de a avertiza utilizatorii referitor la condiţiile legale de acces şi de utilizare”[512], „precum şi la consecinţele juridice ale accesului nesancţionat la aceste sisteme informatice. Avertizarea trebuie să fie accesibilă oricărui utilizator.”[513] De asemenea, potrivit alin. (1) art. 7 al Legii nr. 20/2009,

---

[505] Ibidem.
[506] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en
[507] Ibidem.
[508] *Acordul de asociere între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de o parte, și Republica Moldova, pe de altă parte*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22014A0830(01)&from=RO
[509] Ibidem.
[510] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.
[511] Ibidem.
[512] Ibidem.
[513] Ibidem.

„furnizorii de servicii sunt obligaţi: [...] b) să comunice [...] despre [...] accesul ilegal la informaţia din sistemul informatic; [...]”[514]; e) să întreprindă măsuri de securitate [...] cu al căror ajutor accesul [...] să fie restricţionat sau interzis utilizatorilor neautorizaţi”.[515]

Așadar, tocmai trei legi – Legea nr. 1069/2000, Legea nr. 467/2003 și Legea nr. 20/2009 – reglementează sistemul de relații sociale din domeniul informatic. Cu toate acestea, cadrul legal extrapenal în materie este deficient. Or, în legile respective lipsesc definițiile unor noțiuni importante („reţea informatică”, „sistem de protecţie”, „canalele de telecomunicaţii” etc.) utilizate în art. 259 CP RM, ceea ce influențează negativ claritatea și previzibilitatea acestui articol.

Așa cum am menționat anterior, legea penală trebuie să fie condiționată sub aspect social. În context, îl vom cita pe A.D. Kos: „Datorită complexității activității legislative, printre normele adoptate, există cele care nu reflectă pe deplin nevoile societății sub aspectul apărării penale”[516]; „Dezavantajele normelor pot consta și în lipsa clarității, a constanței și a univocității suficiente a dispozițiilor legale”[517]; „Prin aceasta se explică eficiența lor scăzută chiar și în condițiile de activitate impecabilă a celor care aplică asemenea dispoziții”[518]. Activitatea impecabilă a celor care aplică dispozițiile penale este un ideal pe care ni-l dorim cu toții. Pentru a realiza acest ideal măcar în parte, este necesară perfecționarea cadrului legal extrapenal care reglementează sistemul de relații sociale din domeniul informatic. Perfecționarea dată trebuie să se exprime, în mod primordial, în definirea de către legiuitor a noțiunilor „reţea informatică”, „sistem de protecţie”, „canalele de telecomunicaţii” etc. În condițiile de lipsă a unei hotărâri explicative a Plenului CSJ cu privire la infracțiunile informatice[519], precum și de interpretare doctrinară neuniformă a noțiunilor date, devine stringentă intervenția legiuitorului.

1.4. Coerența sistemică dintre art. 259 CP RM și prevederile complementare din legislația națională

Orice sistem poate fi privit ca un tot unitar în care elementele structurale: 1) posedă caracteristici comune pentru întregul sistem; 2) formează interconexiuni cu celelalte elemente

[514] Ibidem.
[515] Ibidem.
[516] КОС, А.Д. Направления уголовно-правовой политики в борьбе с преступностью. În: *Право и общество*, 2009, № 4, с. 98-100.
[517] Ibidem.
[518] Ibidem.
[519] Analiza speţelor din practica judiciară, în care a fost aplicat art. 259 CP RM (care va fi efectuată *infra*), demonstrează necesitatea formulării de către instanța supremă a unor explicații în vederea asigurării unei practici unitare de aplicare a art. 259 CP RM.

structurale din același sistem. În contextul dreptului, în general, și al dreptului penal, în particular, metoda analizei sistemice presupune că obiectul analizei îl reprezintă normele penale privite ca parte a unui sistem normativ integral al cărui elemente structurale sunt strâns legate între ele.

Pornind de la aceste premise, se poate afirma că, în sistemul normativ al Republicii Moldova, reglementările privind accesul la informația computerizată formează un sistem. Pentru necesitățile studiului de față, aceste reglementări pot fi clasificate în felul următor: a) reglementările penale privind accesul la informația computerizată, care-și au sediul în art. 259 CP RM; b) reglementările extrapenale privind accesul la informația computerizată. Reglementările din ambele aceste clase posedă numite caracteristici comune, dar și caracteristici individualizante. Totodată, prevederile art. 259 CP RM formează interconexiuni cu reglementările extrapenale privind accesul la informația computerizată. Aceasta se explică prin caracterul de referință (de blanchetă) al prevederilor art. 259 CP RM. Acest articol poate fi interpretat și aplicat doar dacă este privit prin prisma reglementărilor extrapenale privind accesul la informația computerizată. Or, anumite noțiuni din art. 259 CP RM sunt definite în astfel de reglementări. Din această perspectivă se poate susține că art. 259 CP RM își întregește conținutul din contul reglementărilor extrapenale privind accesul la informația computerizată. În cele ce urmează vom dezvolta aceste idei.

Astfel, în conformitate cu pct. 3 din anexa la Legea nr. 299 din 21.12.2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova (în continuare – Legea nr. 299/2017), „creșterea dependenței societății contemporane de globalizarea sistemelor informaționale [...] conduce la sporirea vulnerabilității [...] față de amenințările [...] din domeniile informațional-tehnologic [...].”[520] În pct. 35 din anexa nr. 1 la Hotărârea Parlamentului nr. 257 din 22.11.2018 privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia, se menționează: „Accesarea neautorizată a reţelelor şi serviciilor de comunicaţii electronice, modificarea, ştergerea sau deteriorarea neautorizată de date informatice [...] sunt niște probleme de nivel global”.[521] De asemenea, pct. 35 din Hotărârea Guvernului nr. 857 din 31.10.2013 cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020” prevede: „Globalitatea spaţiului cibernetic este de natură să amplifice riscurile la adresa acestora afectând

[520] Legea privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova: nr. 299 din 21.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 48-57, 122.
[521] Hotărârea Parlamentului privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia: nr. 257 din 22.11.2018. În: *Monitorul Oficial al Republicii Moldova*, 2019, nr. 13-21, 80.

în aceeaşi măsură atât sectorul privat, cât şi cel public”[522]; „Ameninţările din spaţiul cibernetic se materializează prin exploatarea vulnerabilităţilor [...] cel mai adesea în: [...] modificarea, ştergerea sau deteriorarea neautorizată de date informatice [...].”[523]

Prin prisma acestor precepte, putem afirma că informatizarea continuă a societății (care a fost amplificată ca urmare a necesității de a asigura interacționarea la distanță a persoanelor fizice și juridice în condițiile pandemiei de COVID-19) are ca implicație firească sporirea semnificației art. 259 CP RM, care prevede răspunderea pentru accesul ilegal la informația computerizată. Produce oare acest articol efectul așteptat de societate? Eficiența oricărei norme de incriminare depinde de gradul ei de condiționare socială. O normă de incriminare, care nu răspunde necesităților sociale, nu poate fi eficientă. Una dintre condițiile obligatorii ale condiționării sociale a unei norme de incriminare este lipsa de contradicții dintre aceasta și normele extrapenale.[524]

La lit. d) alin. (1) art. 3 al Legii nr. 100 din 22.12.2017 cu privire la actele normative, printre principiile activității de legiferare, este menționat principiul coerenței normelor juridice. Acesta presupune că actul normativ trebuie să se integreze organic în sistemul legislaţiei, fiind excluse contradicțiile cu prevederile din alte acte normative, care au un obiect de reglementare similar. În context, V.E. Mihailov susține: „Fiecare normă din partea specială a Codului penal trebuie să se afle într-o relație de non-contradicție conținutistă și logică [...] cu normele oricărei [...] ramuri de drept”.[525] La rândul său, Iu.V. Oriol enunță: „Esența principiului coerenței sistemice a (dez)incriminării unei fapte constă în necesitatea de a clarifica dacă o asemenea (dez)incriminare contravine sau nu normelor altor ramuri de drept”[526], *„i.e.* dacă nu cumva este (dez)incriminat un comportament permis sau interzis de o altă normă juridică.”[527] În prezentul studiu, ne propunem să analizăm problema coerenței sistemice dintre art. 259 CP RM și prevederile complementare din legislația națională. Cu alte cuvinte, ne propunem să aflăm dacă scopul articolului în cauză nu contravine scopului unor astfel de prevederi.

---

[522] Hotărârea Guvernului cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”: nr. 857 din 31.10.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 252-257, 963.
[523] Ibidem.
[524] STRÎMBEANU, Alexandru. Coerența teleologică dintre art. 259 Cod penal și prevederile complementare din legislația națională. În: *Integrare prin cercetare şi inovare. Ştiinţe juridice şi economice. Vol. 1 (7-8 noiembrie 2020, Chişinău)*. Chișinău: CEP USM, 2020, pp. 13-16. ISBN 978-9975-152-48-8.
[525] МИХАЙЛОВ, В.Є. *Кримінальна відповідальність за зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби: соціальна обумовленість та склад злочину*. Харків: Право, 2011, с. 34. 248 с. ISBN 978-966-458-295-4.
[526] ОРЕЛ, Ю.В. Системно-правовая непротиворечивость и международно-правовая необходимость и допустимость как принципы криминализации деяний против нормальной деятельности органов и учреждений пенитенциарной службы Украины. În: *Известия Гомельского государственного университета имени Ф. Скорины*, 2015, № 5, с. 105-110. ISSN 1609-9672.
[527] Ibidem.

În corespundere cu alin. (3) art. 1 din Codul penal, „prezentul cod se aplică în conformitate cu prevederile Constituţiei Republicii Moldova”.[528] Totodată, din alin. (1) art. 30 al Constituției, rezultă că statul asigură secretul oricăror mijloace legale de comunicare. De asemenea, alin. (3) art. 34 al Constituției prevede: „Dreptul la informaţie nu trebuie să prejudicieze măsurile de protecţie a cetăţenilor sau siguranţa naţională.”[529]

Aceste norme constituționale își găsesc dezvoltarea în unele norme ierarhic subordonate de factură extrapenală.

Astfel, în acord cu alin. (2) art. 4 și alin. (1) art. 7 ale Legii nr. 982 din 11.05.2000 privind accesul la informaţie[530], accesul la anumite informații oficiale poate fi restricţionat pentru motive specifice, ce corespund principiilor dreptului internaţional, inclusiv pentru protecţia securităţii naţionale, a ordinii publice, a moralei societăţii sau pentru ocrotirea sănătăţii.

În aceeași ordine de idei, menționăm prevederile relevante din Legea nr. 467/2003: „Orice informaţie documentată a cărei utilizare ilegală poate prejudicia proprietarul, posesorul, utilizatorul ei sau o altă persoană este protejată”[531] (alin. (2) art. 10); „Resursele informaţionale de stat sunt publice şi accesibile tuturor. Excepţie face informaţia documentată atribuită, conform legii, categoriei de informaţie cu acces limitat”[532] (art. 27); „Încălcarea prezentei legi se pedepseşte pe cale [...] penală, în condiţiile legii”[533] (art. 32).

Din art. 6 al Legii nr. 20/2009, desprindem că „proprietarii de sisteme informatice, accesul la care este interzis sau restricţionat pentru anumite categorii de utilizatori, au obligaţia de a avertiza utilizatorii referitor la condiţiile legale de acces şi de utilizare, precum şi la consecinţele juridice ale accesului nesancţionat la aceste sisteme informatice”.[534] Conform art. 11 al legii în cauză, „răspunderea pentru încălcarea prevederilor acesteia atrage, printre altele, răspundere penală”.[535]

Prevederi remarcante distingem și în Legea nr. 1069/2000: „Se interzice accesul şi conectarea neautorizate la sistemele şi reţelele informatice”[536] (alin. (3) art. 4); „Persoanele juridice şi fizice

---

[528] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[529] Constituția Republicii Moldova. În: *Monitorul Oficial al Republicii Moldova*, 1994, nr. 1, 140.
[530] Legea privind accesul la informaţie: nr. 982 din 11.05.2000. În: *Monitorul Oficial al Republicii Moldova*, 2000, nr. 88-90, 664.
[531] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.
[532] Ibidem.
[533] Ibidem.
[534] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.
[535] Ibidem.
[536] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

care încalcă prevederile prezentei legi poartă răspundere [...] penală [...] conform legislaţiei”[537] (art. 37).

Prezintă interes și anumite dispoziții din anexa la Legea nr. 299/2017: „Interesele naționale în domeniul securității informaționale sunt: [...] asigurarea protecţiei spațiului informațional, [...] a informațiilor [...] cu accesibilitate limitată [...]”[538] (pct. 8); „Obiectivele de bază în domeniul asigurării securităţii informaţionale sunt: [...] m) protecția [...] informaţiei cu accesibilitate limitată [...]”[539] (pct. 12); „Principalele ameninţări la adresa securității informaţionale sunt: [...] k) [...] activitatea [...] orientată spre obţinerea accesului neautorizat la [...] informaţie; l) acțiunile de distrugere, deteriorare [...] a resurselor şi sistemelor informaţionale [...]”[540]; „m) activitatea ilegală a structurilor politice, economice, militare, [...] orientată spre obținerea accesului neautorizat la resursele informaţionale [...]”[541] (pct. 13), etc.

Exemplele de prevederi normative reproduse mai sus ne permit să concluzionăm că art. 259 CP RM formează un tot unitar cu alte norme juridice. În cadrul acestui sistem, unele norme reglementează raporturile de conformare în domeniul accesului la informaţia computerizată, în timp ce altele stabilesc răspunderea pentru încălcarea acestor raporturi. Art. 259 CP RM este interconectat cu normele altor ramuri de drept, fiind în concordanță cu acestea. Acest articol declară infracțional comportamentul interzis de astfel de norme, ce se caracterizează printr-un grad sporit de pericol social. Astfel, sub aspect sistemic, art. 259 CP RM este coerent cu prevederile complementare din legislația națională.[542]

1.5. Analiza de drept comparat a reglementărilor cu privire la accesul ilegal la informația computerizată

Dintre toate statele UE doar Republica Cipriotă și Republica Portugheză nu au în codurile lor penale norme în care să fie incriminate fapte de genul celor care sunt specificate în art. 259 CP RM. În cadrul acestui articol vor fi analizate dispozițiile din codurile penale ale statelor membre ale UE, în care sunt incriminate astfel de fapte. Principalul argument în susținerea unei asemenea analize îl reprezintă Acordul de asociere între Uniunea Europeană și Comunitatea Europeană a

[537] Ibidem.
[538] Legea privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova: nr. 299 din 21.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 48-57, 122.
[539] Ibidem.
[540] Ibidem.
[541] Ibidem.
[542] STRÎMBEANU, Alexandru. Coerența teleologică dintre art. 259 Cod penal și prevederile complementare din legislația națională. În: *Integrare prin cercetare și inovare. Științe juridice și economice. Vol. 1 (7-8 noiembrie 2020, Chișinău)*. Chișinău: CEP USM, 2020, pp. 13-16. ISBN 978-9975-152-48-8.

Energiei Atomice și statele membre ale acestora, pe de o parte, și Republica Moldova, pe de altă parte.[543]

De asemenea, vor fi examinate dispozițiile din codurile penale ale Ucrainei și Georgiei, în care sunt incriminate fapte de genul celor care sunt specificate în art. 259 CP RM. În această ordine de idei, argumentul îl constituie perspectiva europeană comună a Ucrainei, a Republicii Moldova și a Georgiei, relevată în Concluziile Consiliului European privind Ucraina, cererile de aderare ale Ucrainei, Republicii Moldova și Georgiei, Balcanii de Vest și relațiile externe din 23.06.2022: „[...] 10. Consiliul European recunoaște perspectiva europeană a Ucrainei, Republicii Moldova și Georgiei. Viitorul acestor țări și al cetățenilor lor se află în Uniunea Europeană”[544]; „11. Consiliul European a decis acordarea statutului de țară candidată Ucrainei și Republicii Moldova. [...]”.[545]

Scopul, pe care-l urmărim, este să stabilim deosebirile și asemănările dintre art. 259 CP RM, pe de o parte, și dispozițiile din codurile penale ale statelor membre ale UE, ale Ucrainei și Georgiei, în care sunt incriminate fapte de genul celor prevăzute la art. 259 CP RM, pe de altă parte, referitoare la obiectul, latura obiectivă, subiectul și latura subiectivă a infracțiunilor respective.

Această analiză va purcede cu examinarea obiectului juridic generic al infracțiunii. Relațiile sociale din domeniul informaticii şi al telecomunicaţiilor constituie obiectul juridic generic al infracțiunilor prevăzute la art. 259 CP RM și al tuturor celorlalte infracțiuni prevăzute în Capitolul XI din partea specială a CP RM. Aceasta rezultă din titulatura capitolului dat.

În mod similar este conceput obiectul juridic generic în legile penale ale Georgiei, Regatului Belgiei, Republicii Croația, Republicii Finlanda, Republicii Lituania, Republicii Polone, României, Ucrainei și Ungariei.

Astfel, în Codul penal al Georgiei (în continuare – CPG), art. 284 se aseamănă ca esență cu art. 259 CP RM. Art. 284 CPG este inclus în Capitolul XXXV „Infracţiuni cibernetice”.[546] în Codul penal al Regatului Belgiei (în continuare – CP RBl), art. 550bis este apropiat ca esență de art. 259 CP RM. Art. 550bis CP RBl este cuprins de Titlul IXbis „Infracţiunile contra

---

[543] *Acordul de asociere între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de o parte, și Republica Moldova, pe de altă parte*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22014A0830(01)&from=RO

[544] *European Council conclusions on Ukraine, the membership applications of Ukraine, the Republic of Moldova and Georgia, Western Balkans and external relations, 23 June 2022*. [citat 18.12.2020] Disponibil: https://www.consilium.europa.eu/en/press/press-releases/2022/06/23/european-council-conclusions-on-ukraine-the-membership-applications-of-ukraine-the-republic-of-moldova-and-georgia-western-balkans-and-external-relations-23-june-2022/

[545] Ibidem.

[546] *Criminal Code of Georgia*. [citat 18.12.2020] Disponibil:: https://matsne.gov.ge/en/document/view/16426?publication=241

confidenţialităţii şi disponibilităţii sistemelor informatice şi a datelor care sunt stocate, prelucrate sau transmise prin aceste sisteme”.[547] În Codul penal al Republicii Croaţia (în continuare – CP RCr), art. 266 și 268 se aseamănă ca esență cu art. 259 CP RM. Art. 266 și 268 CP RCr sunt incluse în Capitolul XXV „Infracţiuni împotriva sistemelor, programelor şi datelor informatice”.[548] În Codul penal al Republicii Finlanda (în continuare – CP RFi), secț. 8 și 8(a) sunt similare ca esență cu art. 259 CP RM. Aceste două secțiuni fac parte din Capitolul 38 „Infracţiuni privitoare la date şi comunicaţii”.[549] În Codul penal al Republicii Lituania (în continuare – CP RLi), art. 196 și 198(1) corespund ca esență cu art. 259 CP RM. Art. 196 și 198(1) CP RLi sunt amplasate în Capitolul XXX „Infracţiunile împotriva securităţii datelor electronice şi a sistemelor de informaţii”.[550] În Codul penal al Republicii Polone (în continuare – CP RP), art. 267, 268, 268a și 269 sunt apropiate ca esență de art. 259 CP RM. Art. 267, 268, 268a și 269 CP RP sunt cuprinse de Capitolul XXXIII „Infracţiuni contra protecţiei informaţiilor”.[551] În Codul penal al României, art. 360 se aseamănă ca esență cu art. 258 CP RM. Art. 360 CPR este inclus în Capitolul VI „Infracţiuni contra siguranţei şi integrităţii sistemelor şi datelor informatice” din Titlul VII „Infracţiuni contra siguranţei publice”.[552] În Codul penal al Ucrainei, art. 361, care prezintă similarități cu art. 259 CP RM, este amplasat în Capitolul XVI „Infracțiuni în domeniul utilizării mașinilor electronice de calcul (computerelor), a sistemelor și rețelelor informatice și a rețelelor de telecomunicații”.[553] În sfârșit, în Codul penal al Ungariei (în continuare – CPUn), secț. 422 este similară ca esență cu art. 259 CP RM. Această secțiune face parte din Capitolul XLIII „Accesul ilicit la date şi infracţiuni împotriva sistemelor informatice”.[554]

Spre deosebire de legea penală moldavă și legile penale străine menționate mai sus, legea penală bulgară are articole amplasate în două capitole diferite, care corespund ca esență cu art. 259 CP RM. Astfel, art. 216 este cuprins de Secțiunea VII „Distrugerea și deteriorarea” din Capitolul V „Infracţiunii împotriva proprietăţii” al părții speciale a Codului penal al Republicii

[547] *Codul penal al Regatului Belgiei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html
[548] *Codul penal al Republicii Croaţia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Croatia-RO.html
[549] *Codul penal al Republicii Finlanda*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Finlanda-RO.html
[550] *Codul penal al Republicii Lituania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Lituania-RO.html
[551] *Codul penal al Republicii Polone*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Polonia-RO.html
[552] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510
[553] *Кримінальний кодекс України*. [citat 18.12.2020] Disponibil: https://zakon.rada.gov.ua/laws/show/2341-14#Text
[554] *Codul penal al Ungariei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Ungaria-RO.html

Bulgaria[555] (în continuare – CP RBu). Alin. (3) al acestui articol prevede răspunderea persoanei „care, accesând în mod neautorizat un sistem informatic de importanţă [...], distruge sau deteriorează în acest fel patrimoniul altuia”.[556] Alte două articole apropiate ca esență de art. 259 CP RM sunt art. 319a și 319b CP RBu. Acestea sunt cuprinse de Capitolul IX „A” „Infracţiuni informatice” al părții speciale a CP RBu.

Similare în anumite privințe cu concepțiile legislative, caracterizate mai sus, sunt concepțiile ce sunt susținute în legile penale ale Republicii Franceze, Marelui Ducat de Luxemburg și Republicii Malta. Astfel, în Codul penal al Republicii Franceze (în continuare – CP RFr), art. 323-1 este apropiat ca esență de art. 259 CP RM. Art. 323-1 CP RFr este cuprins de Capitolul III „Despre atingeri aduse sistemelor de prelucrare automată a datelor” din Titlul II „Despre alte atingeri aduse bunurilor” al Cărții III „Despre crimele şi delictele împotriva proprietăţii”.[557] În Codul penal al Marelui Ducat de Luxemburg (în continuare – CP MDL), art. 509-1 se aseamănă ca esență cu art. 259 CP RM. Art. 509-1 CP MDL este inclus în Secțiunea VII „Despre anumite infracţiuni în materie informatică” a Capitolului II „Despre fraude” din Titlul IX „Crime şi delicte contra patrimoniului”.[558] În Codul penal al Republicii Malta (în continuare – CP RMa), art. 337C este similar ca esență cu art. 259 CP RM. Art. 337C CP RMa face parte din Subtitlul V „Despre utilizarea abuzivă a computerului” al Titlului IX „Despre crime împotriva patrimoniului şi siguranţei publice”.[559]

Cum putem vedea, diviziunile din legile penale ale Republicii Franceze, Marelui Ducat de Luxemburg și Republicii Malta, care corespund cu Capitolul XI din partea specială a CP RM, sunt amplasate în titluri dedicate infracțiunilor contra proprietății / patrimoniului și/sau siguranţei publice. Astfel, în aceste trei legi penale străine, fie domeniul informaticii este privit nu ca valoare socială distinctă, ci ca parte a proprietății / patrimoniului și/sau a siguranţei publice, fie elementele alcătuitoare ale domeniului informaticii sunt privite nu în calitate de obiecte de atentare, dar în calitate de mijloace de atentare asupra proprietății / patrimoniului și/sau a siguranţei publice.[560]

---

[555] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[556] Ibidem.
[557] *Codul penal al Republicii Franceze*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Franta-RO.html
[558] *Codul penal al Marelui Ducat de Luxemburg*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Luxemburg-RO.html
[559] *Codul penal al Republicii Malta*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Malta-RO.html
[560] STRÎMBEANU, Alexandru. Accesul ilegal la informaţia computerizată: analiza comparativă a normelor din codurile penale ale Republicii Moldova și statelor membre ale Uniunii Europene. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234979

În legile penale ale Republicii Cehe, Republicii Estonia și Republicii Slovace, articolele, apropiate ca esență de art. 259 CP RM, sunt cuprinse de capitolele dedicate infracțiunilor contra proprietății / patrimoniului. Aceste capitole nu includ diviziuni care corespund cu Capitolul XI din partea specială a CP RM. Prin aceasta, legile penale ale Republicii Cehe, Republicii Estonia și Republicii Slovace se deosebesc de legile penale ale Republicii Franceze, Marelui Ducat de Luxemburg și Republicii Malta. Astfel, în Codul penal al Republicii Cehe (în continuare – CP RCe), secț. 230 este similară ca esență cu art. 259 CP RM. Această secțiune face parte din Capitolul V „Infracţiuni contra patrimoniului”.[561] În Codul penal al Republicii Estonia (în continuare – CP RE), § 217 corespunde ca esență cu art. 259 CP RM. § 217 CP RE este amplasat în Subsecțiunea 3 „Utilizarea ilegală” din Secțiunea a 2-a „Infracţiuni contra oricăror forme de proprietate” al Capitolului 13 „Infracţiuni contra patrimoniului”.[562] În Codul penal al Republicii Slovace (în continuare – CP RSl), § 247 este apropiat ca esență de art. 259 CP RM. § 247 CP RSl este cuprins de Capitolul patru „Infracţiuni contra dreptului de proprietate”.[563]

O concepție diferită este promovată în legile penale ale Regatului Danemarcei, Republicii Federale Germania, Greciei, Republicii Italia și Regatului Suediei. În aceste legi penale, articolele, apropiate ca esență de art. 259 CP RM, sunt cuprinse de capitolele dedicate infracțiunilor contra libertății / intimității persoanei. Astfel, în Codul penal al Regatului Danemarcei (în continuare – CP RD), art. 263 se aseamănă ca esență cu art. 259 CP RM. Art. 263 CP RD este inclus în Capitolul 27 „Infracţiuni contra onoarei și a unor drepturi personale”.[564] În Codul penal al Republicii Federale Germania (în continuare – CP RFG), § 202a este similar ca esență cu art. 259 CP RM. § 202a CP RFG face parte din Secțiunea XV „Încălcarea vieții private”.[565] În Codul penal al Greciei (în continuare – CPGr), art. 370C corespunde ca esență cu art. 259 CP RM. Art. 370C CPGr este amplasat în Capitolul XXII „Încălcarea confidenţialităţii”.[566] În Codul penal al Republicii Italia (în continuare – CP RI), art. 615-ter este apropiat ca esență de art. 259 CP RM. Art. 615-ter CP RI este cuprins de Secţiunea a IV-a „Despre delicte împotriva inviolabilităţii domiciliului” din Partea a III-a „Despre delictele

[561] *Codul penal al Republicii Cehe*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Cehia-RO.html
[562] *Codul penal al Republicii Estonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Estonia-RO.html
[563] *Codul penal al Republicii Slovace*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovacia-RO.html
[564] *Codul penal al Regatului Danemarcei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Danemarca-RO.html
[565] *Codul penal al Republicii Federale Germania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Germania-RO.html
[566] *Codul penal al Greciei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Grecia-RO.html

împotriva libertăţii individuale” a Titlului XII „Despre delicte împotriva persoanei”.[567] În Codul penal al Regatului Suediei (în continuare – CP RSu), art. 9c din Capitolul 4 „Infracţiuni contra libertăţii şi integrităţii”[568] se aseamănă ca esență cu art. 259 CP RM.

Spre deosebire de legile penale străine menționate mai sus, legea penală austriacă are articole amplasate în două capitole diferite, care corespund ca esență cu art. 259 CP RM. Astfel, § 118a este cuprins de Titlul V „Violarea sferei private şi a anumitor secrete profesionale” al părții speciale a Codului penal al Republicii Austria[569] (în continuare – CP RA). La rândul său, § 126a, care este, de asemenea, apropiat ca esență de art. 259 CP RM, este cuprins de Titlul VI „Fapte penale contra patrimoniului” al părții speciale a CP RA. Alin. (1) al acestui paragraf prevede răspunderea pentru „fapta persoanei care cauzează un prejudiciu [...] prin aceea că modifică, şterge sau aduce în stare de neîntrebuinţare [...]„ sau ascunde date [...] în legătură cu care nu este autorizată [...].”[570]

În legile penale ale Republicii Letonia și Regatului Ţărilor de Jos (Olanda), articolele, apropiate ca esență de art. 259 CP RM, sunt cuprinse de capitolele dedicate infracțiunilor contra siguranței sau ordinii publice. Astfel, în Codul penal al Republicii Letonia (în continuare – CP RLe), secț. 241 este similară ca esență cu art. 259 CP RM. Secț. 241 CP RLe face parte din Capitolul XX „Infracţiuni împotriva siguranţei generale şi ordinii publice”.[571] În Codul penal al Regatului Ţărilor de Jos (Olanda) (în continuare – CP RȚJ(O)), subsecț. 138ab corespunde ca esență cu art. 259 CP RM. Subsecț. 138ab CP RȚJ(O) este amplasată în Partea a V-a „Infracţiuni grave împotriva ordinii publice” din Cartea a II-a „Infracţiuni grave”.[572]

Doar în Codul penal al Republicii Slovenia (în continuare – CP RSlo), articolul, apropiat ca esență de art. 259 CP RM, este cuprins de capitolul dedicat infracțiunilor economice. Astfel, art. 237 CPSlo este amplasat în Capitolul XXIV „Infracţiuni contra economiei”.[573] Totuși, este necesar de precizat că în acest articol este prevăzută răspunderea pentru accesul ilegal la un sistem informatic comercial.

---

[567] *Codul penal al Republicii Italia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Italia-RO.html
[568] *Codul penal al Regatului Suediei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Suedia-RO.html
[569] *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html
[570] Ibidem.
[571] *Codul penal al Republicii Letonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Letonia-RO.html
[572] *Codul penal al Regatului Ţărilor de Jos (Olanda)*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Olanda-RO.html
[573] *Codul penal al Republicii Slovenia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovenia-RO.html

În fine, în Codul penal al Regatului Spaniei (în continuare – CP RSp), art. 264, care este apropiat ca esență de art. 259 CP RM, este cuprins de Titlul XIII „Delicte împotriva patrimoniului şi împotriva ordinii socio-economice”.[574]

Ca o sinteză a concepțiilor privind obiectul juridic generic al infracțiunilor asemănătoare ca esență cu cele prevăzute la art. 259 CP RM, prevăzute de legile penale ale majorității statelor membre ale UE, ale Georgiei și Ucrainei, se poate spune că este diferit titularul valorii sociale apărate de aceste legi: posesorul informației computerizate, indiferent dacă acesta este persoană fizică sau persoană juridică; persoana fizică, a cărei libertate sau intimitate a fost lezată; statul, al cărui siguranță a fost amenințată.

Următorul semn constitutiv al infracțiunii, asupra căruia ne îndreptăm privirea, este obiectul material sau imaterial. Din analiza art. 259 CP RM rezultă că acest obiect îl constituie: informaţia computerizată; calculatoarele; sistemul informatic; reţeaua informatică; sistemele de protecție.

În corespundere cu cele mai multe dintre articolele care corespund ca esență cu art. 259 CP RM, care fac parte din legile penale ale statelor membre ale UE, ale Georgiei și Ucrainei, sistemul informatic și/sau datele informatice reprezintă obiectul material sau imaterial al infracțiunilor respective:

– sistemul informatic (art. 284 CPG);

– sistemul informatic sau o parte a unui sistem informatic (§ 118a CP RA); datele prelucrate, transmise sau disponibile electronic (§ 126a CP RA). Conform alin. (2) § 74 CP RA, „în sensul prezentei legi termenul „date” desemnează atât date cu caracter personal şi date fără caracter personal, cât şi programe”[575];

– datele stocate, prelucrate sau transmise prin sisteme informatice; sistemul informatic (art. 550bis CP RBl);

– datele informatice dintr-un sistem informatic (art. 216 și 319b CP RBu);

– sistemul informatic sau o parte a acestuia, alt echipament tehnic de prelucrare a datelor; datele stocate în sisteme sau medii informatice (secț. 230 CP RCe);

– sistemul informatic sau datele informatice (art. 266 CP RCr); datele sau programele informatice (art. 268 CP RCr);

– informaţiile sau programele altor persoane, care sunt destinate utilizării într-un sistem informatic (art. 263 CP RD);

---

[574] *Codul penal al Regatului Spaniei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Spania-RO.html

[575] *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html

– sistemul informatic (§ 217 CP RE);

– sistemul informatic sau o parte a acestuia; datele sau informaţiile cuprinse într-un sistem informatic (secț. 8 din Capitolul 38 CP RFi);

– sistemul sau o parte a unui sistem de prelucrare automată de date; datele incluse în sistemul de prelucrare automată de date (art. 323-1 CP RFr);

– datele stocate sau transmise electronic sau magnetic sau în alt mod care nu este imediat perceptibil (§ 202a CP RFG);

– programele de calculator; sistemul informatic sau datele transmise prin sistemele de telecomunicaţii (art. 370C CPGr);

– sistemul automatizat de prelucrare a datelor sau o parte din acesta (secț. 241 CP RLe);

– datele electronice; software (art. 196 CP RLi); sistemul informatic (art. 198$^{(1)}$ CP RLi);

– sistemul de prelucrare sau de transmitere automată a datelor; datele conţinute în sistemul de prelucrare sau de transmitere automată a datelor (art. 509-1 CP MDL);

– date, software sau documentaţia justificativă păstrată în computer (art. 337C CP RMa);

– sistemul computerizat sau o parte a acestuia; datele salvate, procesate sau transferate prin intermediul dispozitivului sau sistemului computerizat (subsecţ. 138ab CP RȚJ(O));

– informații; sistemul informatic sau o parte a acestuia (art. 267 CP RP); informaţiile înregistrate pe un suport de date informatic (art. 268 CP RP); datele informatice (art. 268a CP RP);

– sistemul informatic (art. 360 CPR);

– sistemul informatic; informațiile din sistemul informatic sau din suportul de date; programul de calculator (§ 247 CP RSl);

– datele sau programele de calculator; sistemul informatic (art. 237 CP RSlo);

– datele, programele sau documentele electronice; sistem informatic care are legătură cu un altul; date informatice (art. 264 CP RSp);

– datele destinate prelucrării automate (art. 9c din Capitolul 4 CP RSu);

– sistemul informatic (automatizat) (art. 361 CPU).

Nu oricare sistem informatic, ci doar cel de maximă importanță constituie obiectul material al unora dintre infracțiunile prevăzute de articolele care corespund ca esență cu art. 259 CP RM, care fac parte din legile penale ale statelor membre ale UE:

– sistemul informatic care este parte esenţială a infrastructurii critice (§ 118a CP RA). Conform pct. 11 alin. (1) § 74 CP RA, „infrastructura critică este reprezentată de amenajări, instalaţii, sisteme sau părţi din acestea care joacă un rol esenţial pentru menţinerea siguranţei

publice”[576], „apărarea naţională sau protecţia populaţiei civile faţă de pericole de război, capacitatea operaţională a tehnologiilor publice de informare şi comunicare”[577], „prevenirea şi combaterea catastrofelor, sănătatea publică, alimentarea publică cu apă, energie şi bunuri vitale, domeniul îndepărtării deşeurilor şi al canalizării sau circulaţia publică”[578];

– sistemul informatic de importanţă pentru o întreprindere, instituţie, persoană juridică sau persoană fizică (art. 216 CP RBu); sistemul informatic care este parte integrantă a unei infrastructuri critice (art. 319b CP RBu);

– sistemul informatic conţinând un secret de stat, informaţii clasificate străine sau informaţii rezervate strict uzului oficial; sistemul informatic folosit într-un sector vital (§ 217 CP RE);

– sistemul informatic sau de telecomunicaţii protejat de măsuri de siguranţă; sistemele informatice sau de telecomunicaţii de interes militar sau referitoare la ordinea publică ori la siguranţa publică sau la sănătate sau la protecţia civilă sau de interes public (art. 615-ter CP RI);

– sistemul informatic al statului (alin. (2) secț. 241 CP RLe);

– sistemul de informaţii de importanţă strategică pentru securitatea naţională sau de o importanţă majoră pentru guvernul de stat, economia sau sistemul financiar (art. 198$^{(1)}$ CP RLi).

Nu oricare date informatice, ci doar date informatice de o anumită categorie pot să reprezinte obiectul imaterial al unora dintre infracțiunile prevăzute de articolele care corespund ca esență cu art. 259 CP RM, care fac parte din legile penale ale statelor membre ale UE:

– datele pentru crearea unei semnături electronice; informaţiile care constituie secretul de stat ori un alt secret protejat prin lege (art. 216 CP RBu);

– datele electronice ale unui sistem de informaţii de importanţă strategică pentru securitatea naţională sau de o importanţă majoră pentru guvernul de stat, economia sau sistemul financiar (art. 196 CP RLi);

– datele informatice de o importanţă deosebită pentru apărarea naţională, siguranţa în comunicaţii, funcţionarea guvernului sau a unei alte instituţii de stat sau a autoconducerii locale (art. 269 CP RP);

– datele cu caracter personal, secrete private, secrete comerciale sau secrete profesionale (secț. 422 CPUn).

Mijloacele de protecție sunt indicate ca obiect material sau imaterial al unora dintre infracțiunile prevăzute de articolele care corespund ca esență cu art. 259 CP RM, care fac parte din legile penale ale statelor membre ale UE:

---

576 Ibidem.
577 Ibidem.
578 Ibidem.

– dispozitivul de securitate specific din interiorul sistemului informatic (§ 118a CP RA);

– mijloace de protecţie (§ 217 CP RE);

– sisteme de protecţie a prelucrării datelor (secţ. 241 CP RLe);

– mijloacele de protecţie ale sistemului informatic (art. 198(1) CP RLi).

Echipamente sau dispozitive informatice apar ca obiect material sau imaterial al unora dintre infracțiunile prevăzute de articolele care corespund ca esență cu art. 259 CP RM, care fac parte din legile penale ale statelor membre ale UE:

– echipament tehnic (art. 196 CP RLi);

– dispozitiv computerizat (subsecţ. 138ab CP RȚJ(O));

– suportul de date sau dispozitivul de procesare automată, de stocare sau de transmitere a datelor informatice (art. 269 CP RP);

– suportul de date sau o parte a acestuia; hardware (§ 247 CP RSl).

În fine, alte categorii de bunuri pot reprezenta obiectul material al unora dintre infracțiunile prevăzute de articolele care corespund ca esență cu art. 259 CP RM, care fac parte din legile penale ale statelor membre ale UE:

– obiectul critic al sistemului informatic (art. 284 CPG);

– componente esenţiale ale infrastructurii critice (§ 126a CP RA);

– patrimoniul altuia (art. 216 CP RBu).

Următorul element constitutiv al infracțiunii, care va fi examinat, este latura obiectivă.

Din analiza art. 259 CP RM rezultă că fapta prejudiciabilă este alcătuită din două acțiuni componente:

1) acţiunea principală de acces ilegal la informaţia computerizată;

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

Un conținut asemănător al faptei prejudiciabile îl are infracțiunea prevăzută la alin. (3) art. 216 CP RBu. Această normă prevede răspunderea persoanei „care, accesând în mod neautorizat un sistem informatic de importanţă [...], distruge sau deteriorează în acest fel patrimoniul altuia.”[579] Un conținut apropiat, dar totuși diferit, îl are fapta prejudiciabilă prevăzută la alin. 1 art. 9c din Capitolul 4 CP RSu. Norma dată prevede răspunderea „persoanei care încearcă să obţină acces neautorizat la anumite date destinate prelucrării automate”[580] „sau, fără permisiune,

[579] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html

[580] *Codul penal al Regatului Suediei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Suedia-RO.html

modifică, distruge, blochează sau adaugă în baza de date o astfel de informaţie[581] „[ori] care, fără permisiune, printr-o altă măsură similară, blochează sau împiedică grav folosirea unor astfel de date”.[582] Un conținut apropiat, dar mai elaborat, îl are fapta prejudiciabilă prevăzută în alin. (2) secț. 230 CP RCe: „Fapta persoanei care dobândeşte acces la sisteme sau medii informatice şi a) foloseşte în mod neautorizat datele stocate în acele sisteme sau medii informatice”[583], „b) şterge sau distruge, degradează, modifică sau corupe calitatea datelor stocate în acele sisteme sau medii informatice, sau le aduce în stare de neîntrebuinţare fără a fi autorizată”[584], „c) falsifică sau modifică datele stocate în acele sisteme sau medii informatice astfel încât să fie considerate autentice”[585], „sau să fie tratate ca fiind autentice, indiferent dacă acele date pot fi accesate sau înţelese direct”[586] sau d) introduce date în sisteme sau medii informatice sau efectuează orice altă intervenţie asupra [...] calculatorului sau ale altui echipament tehnic de prelucrare a datelor, fără a fi autorizată.”[587]

În cazul celorlalte legi penale străine analizate, acțiunile, care în art. 259 CP RM au rolul de acţiune principală și acţiune adiacentă, sunt incriminate ca infracțiuni distincte în alineate diferite ale aceluiași articol, în articole diferite din aceeași diviziune a legii penale sau chiar în articole diferite din diviziuni distincte ale legii penale.

În cazul infracțiunilor prevăzute la art. 259 CP RM, daunele în proporții mari sau daunele în proporții deosebit de mari reprezintă urmările prejudiciabile care constituie semnul obligatoriu al laturii obiective.

În cazul infracțiunilor similare prevăzute de legile penale străine analizate, urmările prejudiciabile, după caz, au un efect agravant sau nu-l au: daunele în proporții considerabile (lit. d) alin. (2) art. 284 CPG); prejudicii cauzate datelor, care depăşesc suma de 5.000 euro (alin. (2) § 126a CP RA); prejudiciu, cauzat datelor, care depăşeşte suma de 300.000 euro (alin. (4) § 126a CP RA); consecinţe grave (alin. (5) art. 319a CP RBu); daune semnificative sau alte consecinţe grave (alin. (2) art. 319b CP RBu); pagube substanţiale; tulburarea gravă a activităţilor unui organ al administraţiei publice centrale, al administraţiei publice locale, ale unei instanţe de judecată sau ale unei alte autorităţi publice; tulburarea gravă a activităţilor unei persoane juridice sau ale unei persoane fizice autorizate (alin. (4) secț. 230 CP RCe); pagube considerabile (alin. (5) secț. 230 CP RCe); pagube semnificative (pct. 1 alin. (2) § 217 CP RE); consecințe grave

[581] Ibidem.
[582] Ibidem.
[583] *Codul penal al Republicii Cehe*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Cehia-RO.html
[584] Ibidem.
[585] Ibidem.
[586] Ibidem.
[587] Ibidem.

(alin. (2) secț. 241 CP RLe); daune majore (alin. 1 art. 196 CP RLi); daune patrimoniale semnificative (§ 3 art. 268 CP RP); daună patrimonială considerabilă (§ 2 art. 268a CP RP); daune pe scară largă (alin. (1) § 247 CP RSl); beneficii materiale importante sau pierderi materiale importante (alin. (1) art. 237 CP RSlo); prejudiciu special sau afectarea unui interes general (pct. 2 alin. 3 art. 264 CP RSp); daunele în proporții considerabile (alin. 4 art. 361 CPU). Apropiată, dar totuși diferită, este abordarea urmărilor prejudiciabile în alin. 1 art. 9c din Capitolul 4 CP RSu: „La stabilirea gravităţii faptei se va lua în considerare [...] dacă fapta a provocat daune serioase sau [...] a fost de natură deosebit de gravă."[588]

Conform alin. 3 art. 196 CP RLi, lipsa de gravitate a prejudiciului se consideră temei de aplicare a răspunderii contravenționale: „Persoana care săvârşeşte fapta prevăzută în prezentul articol şi produce un prejudiciu minor se consideră că a săvârşit o contravenţie [...]."[589]

În anumit legi penale străine examinate, anumite semne secundare ale laturii obiective pot să aibă un caracter indispensabil, obligatoriu. De exemplu, în alin. (4) art. 319b CP RBu este specificat mijlocul special de săvârșire a infracțiunii: program informatic, parolă, cod de acces sau alte date de acces la un sistem informatic sau la o parte a acestuia, destinate afectării a mai mult de un sistem informatic. În cazuri mai frecvente este menționată metoda specială de săvârșire a infracțiunii: eliminarea sau ocolirea mijloacelor de protecţie (alin. (1) § 217 CP RE); folosirea unui cod de acces care nu îi aparţine făptuitorului în mod licit sau spargerea unei protecţii (alin. (1) secț. 8 din Capitolul 38 CP RFi); folosirea unui instrument tehnic special sau ocolirea sistemului de protecţie printr-o metodă tehnică, prin utilizarea unei vulnerabilităţi din sistemul de informaţii sau prin alte mijloace evident frauduloase (alin. (2) secț. 8 din Capitolul 38 CP RFi); manieră deosebit de metodică (alin. (1) secț. 8(a) din Capitolul 38 CP RFi); forţarea dispozitivului de asigurare (alin. (1) § 202a CP RFG); folosirea violenţei asupra lucrurilor sau persoanelor sau înarmarea evidentă (pct. 2) alin. 2 art. 615-ter CP RI); spargerea sistemelor de protecţie a prelucrării datelor (alin. (1) secț. 241 CP RLe); încălcarea unei măsuri de securitate; intervenţie tehnică; utilizarea de semnale false sau de cheie falsă; asumarea unei identităţi false (alin. 1 subsecţ. 138ab CP RȚJ(O)). Doar în legea penală ucraineană, timpul săvârșirii infracțiunii este menționat ca semn secundar cu efect agravant al laturii obiective a infracțiunii. Astfel, conform alin. 5 art. 361 CPU, răspunderea se agravează dacă infracțiunea este săvârșită pe timp de război.

---

[588] *Codul penal al Regatului Suediei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Suedia-RO.html

[589] *Codul penal al Republicii Lituania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Lituania-RO.html

În legile penale germană și belgiană, pregătirea de infracțiune este echivalată cu infracțiunea consumată. Astfel, conform § 202c CP RFG, răspunde „persoana care pregăteşte o faptă prevăzută la § 202a sau § 202b prin aceea că [...] facilitează [...] accesul la 1. parole sau alte coduri de siguranţă care permit accesul la date”[590] „sau 2. programe informatice al căror scop este săvârşirea unei astfel de fapte.”[591] În mod similar, în § 5 art. 550bis CP RBl este prevăzută răspunderea celui „care, fără a avea dreptul, [...] pune la dispoziţie [...] orice dispozitiv [...] pentru a permite comiterea infracţiunilor prevăzute la §§ 1 la 4.”[592]

În legea penală belgiană, tentativa de infracțiune este echivalată cu infracțiunea consumată. Potrivit § 4 art. 550bis CP RBl, „tentativa de comitere a oricăreia din infracţiunile prevăzute la §§ 1 şi 2 este pedepsită cu aceleaşi pedepse”.[593]

Un alt element constitutiv al infracțiunii, care va fi analizat, este latura subiectivă.

În legea penală belgiană, sunt prezentate într-o manieră variată nu doar tipurile de intenție, ci și formele de vinovăție. De exemplu, în alin. 2 § 1 și § 2 art. 550bis CP RBl este specificată „intenţia frauduloasă”.[594] În pct. 3° § 3 art. 550bis CP RBl se folosește formularea „chiar și fără intenție”[595], ceea ce vorbește despre posibilitatea săvârșirii infracțiunii din imprudență.

În mai multe legi penale străine examinate este indicat scopul special al infracțiunii: „cu intenţia: 1. de a cunoaşte sau de a facilita unei alte persoane neautorizate accesul la date cu caracter personal, cunoaştere care lezează interese confidenţiale protejate ale persoanei vătămate sau 2. de a produce un dezavantaj unei alte persoane prin utilizarea datelor salvate în sistem şi care nu îi sunt destinate şi la care îşi creează acces sau prin utilizarea sistemului informatic”[596] (alin. (1) § 118a CP RA); „cu scopul de a face rău”[597] (§ 2 art. 550bis CP RBl); „pentru crearea unei semnături electronice”[598] (alin. (3) art. 319a CP RBu); „scopul obţinerii unui folos patrimonial”[599] (alin. (3) art. 319b CP RBu); „a) cu intenţia de a produce prejudicii altcuiva sau de a câştiga foloase ilegale pentru sine sau alţii, sau b) cu intenţia de a limita funcţionalitatea unui sistem informatic sau a altui echipament tehnic de prelucrare a datelor, fără a fi

---

590 *Codul penal al Republicii Federale Germania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Germania-RO.html
591 Ibidem.
592 *Codul penal al Regatului Belgiei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html
593 Ibidem.
594 Ibidem.
595 Ibidem.
596 *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html
597 *Codul penal al Regatului Belgiei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html
598 *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
599 Ibidem.

autorizată”[600] (alin. (2) secț. 230 CP RCe); „scopul de a obţine informaţii despre secretele comerciale ale unei societăţi”[601] (art. 263 CP RD); „scopul dobândirii de bunuri”[602] (alin. (2) secț. 241 CP RLe); „scopul obţinerii de date informatice”[603] (alin. (2) art. 360 CPR); „scopul de a provoca daune sau alte prejudicii altei persoane, sau de a obţine beneficii injuste pentru sine sau pentru altă persoană”[604] (alin. (1) § 247 CP RSl); „pentru a obţine beneficii materiale ilegale pentru sine sau pentru o terţă persoană sau pentru a provoca daune bunurilor altei persoane”[605] (alin. (1) art. 237 CP RSlo).

Ultimul element constitutiv al infracțiunii, care va fi examinat, este subiectul.

Din sancțiunile la cele două alineate ale art. 259 CP RM reiese că nu numai persoana fizică, dar și persoana juridică poate avea calitatea de subiect al infracțiunii. În mod similar, persoana juridică este menționată ca subiect al infracțiunii în alin. (3) § 217 CP RE, alin. 4 art. 196 și alin. 3 art. 198(1) CP Rli și alin. 4 art. 264 CP RSp.

În dispoziția de la alin. (1) art. 259 CP RM este reliefată calitatea specială a subiectului infracțiunilor de acces ilegal la informația computerizată: „[...] al unei persoane care nu este autorizată [...], depăşeşte limitele autorizării ori nu are permisiunea [...] să efectueze [...] operaţiuni într-un sistem informatic [...]”.[606] În unele cazuri, în articolele similare ca esență cu art. 259 CP RM este indicată – explicit sau implicit – calitatea specială a subiectului: „cu folosirea situației de serviciu”[607] (lit. b) alin. 2 art. 284 CPG); „în legătură cu care [persoana] nu este autorizată sau este autorizată doar împreună cu o altă persoană”[608] (alin. (1) § 126a CP RA); „În cazul în care făptuitorul este în serviciul deţinătorului legal al sistemului informatic sau al datelor, fapta din alineatul precedent se pedepseşte doar dacă este interzisă expres în regulamentul intern sau prin decizia scrisă a deţinătorului sau a unui angajat competent al acestuia”[609] (alin. 3 art. 370C CPGr); „dacă fapta este comisă de un funcţionar public sau de un

---

[600] *Codul penal al Republicii Cehe*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Cehia-RO.html
[601] *Codul penal al Regatului Danemarcei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Danemarca-RO.html
[602] *Codul penal al Republicii Letonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Letonia-RO.html
[603] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510
[604] *Codul penal al Republicii Slovace*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovacia-RO.html
[605] *Codul penal al Republicii Slovenia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovenia-RO.html
[606] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[607] *Criminal Code of Georgia*. [citat 18.12.2020] Disponibil: https://matsne.gov.ge/en/document/view/16426?publication=241
[608] *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html
[609] *Codul penal al Greciei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Grecia-RO.html

însărcinat cu o funcţie publică, [...] sau de cel care practică fie şi abuziv profesia de detectiv particular [...]”[610] (pct. 1) alin. 2 Art. 615-ter CP RI); „În sensul prezentului Subtitlu: (a) [...] o persoană acţionează fără autorizaţie în cazul în care nu este autorizată corespunzător de către o persoană îndreptăţită legal”[611]; „(b) [...] o persoană este îndreptăţită în cazul în care [...] are drept de control asupra activităţilor definite în alin. (1)(a)-(j) sau în art. 4(a) şi (b) din prezentul Subtitlu”[612] (alin. (2) art. 337C CP RMa).

În unele cazuri, participanții secundari la infracțiune se echivalează cu autorul infracțiunii: „cel care ordonă comiterea uneia din infracţiunile prevăzute la §§ 1 la 5 sau care incită la comiterea acestora”[613] (§ 6 art. 550bis CP RBl); „de o persoană, care acţionează la comanda sau în îndeplinirea deciziei unui grup infracţional organizat”[614] (pct. 1 alin. (5) art. 319b CP RBu).

În fine, în unele cazuri, anumite forme de participație la infracțiune pot constitui temeiuri de agravare a răspunderii penale: „săvârşirea infracțiunii în cadrul unui grup infracţional”[615] (alin. (4) § 118a CP RA); „de două sau mai multe persoane care s-au înţeles între ele în prealabil pentru comiterea faptei”[616] (alin. (2) art. 319a CP RBu); „în calitate de membru al unui grup organizat”[617] (alin. (4) secț. 230 CP RCe); „dacă fapta este comisă în cadrul unei organizaţii criminale”[618] (pct. 1 alin. 3 art. 264 CP RSp).

1.6. Sinteza problematicii tratate și a rezultatelor obținute în Capitolul 1

Considerăm necesară formularea anumitor concluzii după ce am investigat abordările doctrinare și normative privind răspunderea penală pentru accesul ilegal la informația computerizată:

1) la soluţionarea problemelor, care au fost stabilite în procesul de analiză a infracţiunilor specificate în art. 259 CP RM, un loc proeminent îl ocupă lucrările elaborate de către: S.

[610] *Codul penal al Republicii Italia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Italia-RO.html
[611] *Codul penal al Republicii Malta*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Malta-RO.html
[612] Ibidem.
[613] *Codul penal al Regatului Belgiei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html
[614] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[615] *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html
[616] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[617] *Codul penal al Republicii Cehe*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Cehia-RO.html
[618] *Codul penal al Regatului Spaniei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Spania-RO.html

Bacinschi; A. Barbăneagră; A. Borodac; S. Brînza; S. Copețchi; S. Crijanovschi; L. Dumneanu; M. Gheorghiță; L. Gîrla; S. Grișciuc-Bucica; D. Gurev; N. Lazareva; V. Stati, etc. (Republica Moldova); Gh. Alecu; A. Crăciunescu; M. Dobrinoiu; A.T. Drăgan; C. Duvac; G. Florescu; V. Florescu; L.C. Kövesi; C. Manea; T. Medeanu; G. Zlati, etc. (România); D.S. Azarov; S.Ia. Burda; D.O. Ricika; N.A. Rozenfeld; A.Ia. Skiba; T.I. Sozanski, etc. (Ucraina); I.R. Beghișev; A.M. Doronin; A.N. Popov; V.G. Stepanov-Eghianț, etc. (Federaţia Rusă);

2) opiniile doctrinare, care conduc spre ideea că obiectul juridic generic al infracţiunilor care sunt prevăzute de art. 259 CP RM îl constituie relaţiile sociale din domeniul informaticii şi al telecomunicaţiilor, au ca fundament titlul Capitolului XI al părții speciale a Codului penal al Republicii Moldova;

3) divergențele doctrinare privind conținutul, pe care îl are obiectul juridic generic al infracţiunilor ce sunt prevăzute în art. 259 CP RM, impune examinarea posibilității de modificare a titlului Capitolului XI al părții speciale a Codului penal al Republicii Moldova;

4) doar unii autori ai materialelor ştiinţifice la tema tezei atestă caracterul biobiectual al infracţiunilor prevăzute la art. 259 CP RM;

5) în doctrina de specialitate nu se acordă atenție suficientă stabilirii înțelesului noțiunilor „informație computerizată”, „sistem informatic”, „rețea informatică” și „calculator”. Interpretarea doctrinară a acestor noțiuni nu întotdeauna se întemeiază pe reglementările naționale cu privire la accesul la informaţia computerizată și pe reglementările de sorginte internațională privind interzicerea accesului ilegal la informaţia computerizată;

6) nu toți autorii materialelor ştiinţifice la tema tezei consideră că urmările prejudiciabile și legătura cauzală constituie semne obligatorii ale laturii obiective a acestor infracțiuni;

7) în planul examinării acțiunii principale, nu întotdeauna este suficient analizată noțiunea de acces la informația computerizată. De asemenea, nu toți doctrinarii analizează temeinic condițiile în care accesul la informația computerizată are un caracter ilegal;

8) în planul examinării acțiunii adiacente, doctrinarii propun propriile definiții ale noțiunilor care vizează modalitățile normative ale acesteia. Însă, nu întotdeauna, aceste definiții permit delimitarea cu exactitate a noțiunilor respective între ele;

9) unii doctrinari, fără a lua în seamă modificările care au fost operate în art. 259 CP RM, consideră că infracțiunile, prevăzute de acest articol, sunt formale. Acești teoreticieni susțin că respectivele infracțiuni se consideră consumate din momentul săvârșirii faptei prejudiciabile. O asemenea abordare contribuie la confundarea tentativei sau a pregătirii de infracțiune cu infracțiunea consumată, ceea ce poate genera erori în procesul de aplicare a art. 259 CP RM;

10) unii doctrinari consideră că infracțiunile, care sunt prevăzute de art. 259 CP RM, se comit doar cu intenție directă. Această opinie decurge din raportarea de către aceiași autori a infracțiunilor, prevăzute la art. 259 CP RM, la categoria de infracțiuni formale. Totuși, opinia doctrinară majoritară se bazează pe textul art. 259 CP RM, din care decurge caracterul obligatoriu al producerii daunelor în proporții mari / deosebit de mari;

11) nu toți doctrinarii acordă atenție cuvenită interpretării acelui fragment din alin. (1) art. 259 CP RM, care vizează calitatea specială a subiectului infracțiunii. Aceasta deși caracteristicile subiectului infracțiunilor, ce sunt prevăzute de art. 259 CP RM, pot fi stabilite doar cu condiția interpretării fragmentului respectiv prin prisma reglementărilor extrapenale cu privire la accesul la informaţia computerizată;

12) factorii, care determină necesitatea de a atribui ilicitate infracțională accesului ilegal la informaţia computerizată, sunt de ordin social-juridic și social-economic: intensificarea schimbului de informații între persoanele fizice, persoanele juridice și state; penetrarea tehnologiilor informaționale în toate domeniile activității umane; utilizarea masivă a comunicațiilor prin satelit, a calculatoarelor și a rețelelor de calculatoare, etc.;

13) nevoia de a incrimina accesul ilegal la informaţia computerizată a fost condiționată de interzicerea sau restricționarea accesului la o astfel de informație pentru anumite persoane. Această interdicție sau restricționare, sfidată de către făptuitor, determina intrarea acestuia în sistemul computerizat, cu încălcarea sistemului de protecţie, pentru a apela informații pe care făptuitorul nu era autorizat să le acceseze;

14) nu forma computerizată a informației, dar caracterul prohibit sau restricționat al accesării acesteia condiționează necesitatea incriminării faptelor prevăzute la art. 259 CP RM;

15) prevederile art. 259 CP RM formează interconexiuni cu reglementările extrapenale privind accesul la informația computerizată. Aceasta se explică prin caracterul de referință (de blanchetă) al prevederilor art. 259 CP RM. Acest articol poate fi interpretat și aplicat doar dacă este privit prin prisma reglementărilor extrapenale privind accesul la informația computerizată;

16) cadrul legal extrapenal din domeniul informatic este deficient. Or, în legile respective (Legea nr. 1069/2000, Legea nr. 467/2003 și Legea nr. 20/2009) lipsesc definițiile unor noțiuni importante („reţea informatică”, „sistem de protecţie”, „canalele de telecomunicaţii” etc.) utilizate în art. 259 CP RM, ceea ce influențează negativ claritatea și previzibilitatea acestui articol;

17) ca o sinteză a concepțiilor privind obiectul juridic generic al infracțiunilor asemănătoare ca esență cu cele prevăzute la art. 259 CP RM, prevăzute de legile penale ale majorității statelor membre ale UE, ale Georgiei și Ucrainei, se poate spune că este diferit titularul valorii sociale

apărate de aceste legi: posesorul informației computerizate, indiferent dacă acesta este persoană fizică sau persoană juridică; persoana fizică, a cărei libertate sau intimitate a fost lezată; statul, al cărui siguranță a fost amenințată;

18) în corespundere cu cele mai multe dintre articolele care corespund ca esență cu art. 259 CP RM, care fac parte din legile penale ale statelor membre ale UE, ale Georgiei și Ucrainei, doar sistemul informatic și/sau datele informatice reprezintă obiectul material sau imaterial al infracțiunilor respective;

19) în cazul celor mai multe dintre legile penale străine analizate, acțiunile, care în art. 259 CP RM au rolul de acţiune principală și acţiune adiacentă, sunt incriminate ca infracțiuni distincte în alineate diferite ale aceluiași articol, în articole diferite din aceeași diviziune a legii penale sau chiar în articole diferite din diviziuni distincte ale legii penale;

20) problema ştiinţifică importantă constă în fundamentarea concepției de interpretare a art. 259 CP RM și de calificare a infracțiunilor în baza acestui articol fără a fi încălcat principiul legalității, această fundamentare având ca efect identificarea erorilor de aplicare a art. 259 CP RM și a defectelor ce caracterizează dispoziția acestui articol, astfel fiind creată baza teoretică necesară pentru a perfecționa practica de aplicare a art. 259 CP RM și pentru a îmbunătăți calitatea acestui articol;

21) direcţiile de soluţionare a problemei ştiinţifice importante se exprimă în: evaluarea condițiilor sociale și juridice care au determinat incriminarea accesului ilegal la informația computerizată; stabilirea gradului de coerența sistemică dintre art. 259 CP RM și prevederile complementare din legislația națională; analiza de drept comparat a reglementărilor cu privire la accesul ilegal la informația computerizată; identificarea conținutului obiectului juridic generic și al obiectului juridic special al infracțiunilor ce sunt prevăzute de art. 259 CP RM; definirea noțiunilor care desemnează entitățile ce reprezintă obiectul material (imaterial) al acestor infracțiuni; definirea noțiunii de acces la informația computerizată; analiza condițiilor în care accesul la informația computerizată are caracter ilegal; identificarea momentului de consumare și a urmărilor prejudiciabile în cazul infracțiunilor ce sunt specificate în art. 259 CP RM; stabilirea calității speciale a subiectului acestor infracțiuni, etc.

2. ANALIZA DE DREPT PENAL A INFRACȚIUNILOR PREVĂZUTE LA ART. 259 CP RM

2.1. Obiectul infracțiunilor prevăzute la art. 259 CP RM

2.1.1. Obiectul juridic al infracțiunilor prevăzute la art. 259 CP RM

În legătură cu infracțiunile prevăzute în Capitolul XI al părții speciale a Codului penal (din rândul cărora fac parte infracțiunile ce sunt prevăzute în art. 259 CP RM), A. Borodac a exprimat următorul punct de vedere: „Obiectul general al acestor infracțiuni îl constituie relațiile sociale a căror existență și normală desfășurare e condiționată de ocrotirea ordinii de drept a Republicii Moldova în domeniul informaticii."[619] Considerăm nepotrivită o asemenea caracterizare nici pentru obiectul juridic general, nici pentru obiectul juridic generic, care derivă din cel general.

Precedentul proxim al Capitolului XI al părții speciale a Codului penal al Republicii Moldova l-a constituit Capitolul VI[1] al părții speciale a Codului penal al Republicii Moldova din 1961, care avea titlul „Infracţiuni în domeniul tehnologiilor informaţionale".[620] Din interpretarea acestui titlu reiese că relațiile sociale referitoare la tehnologiile informaționale constituia obiectul juridic al faptelor infracționale specificate în Capitolul VI[1] al părții speciale a Codului penal din 1961, printre care distingem infracțiunile de acces ilegal (nesancţionat) la informaţia computerizată, prevăzute la art. 176[1]. O astfel de concepție este apropiată de cea consacrată în proiectul Convenției ONU privind cooperarea în combaterea criminalității informaționale (în continuare – Proiectul), în textul căreia se folosește formularea „infracțiuni în domeniul tehnologiilor informaționale și ale comunicațiilor (TIC)".[621]

Sintagma „infracțiuni în domeniul tehnologiilor informaționale" este utilizată nu doar în cadrul unor texte normative, dar și în literatura de specialitate.[622]

Cu toate acestea, considerăm nereușită concepția pusă la baza sintagmei în cauză.

---

[619] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 362. 622 p. ISBN 9975-9788-7-8.

[620] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.

[621] *Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности*. [citat 23.01.2021] Disponibil: https://www.mid.ru/documents/10180/3024875/Проект+конвенции+по+преступности+с+правками+секр+ООН.pdf/c93e68c9-9994-4769-951d-057c4881b8fd

[622] ХИСАМОВА, З.И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий. În: *Юридический мир*, 2016, № 2, с. 58-62. ISSN 1811-1475; АБРАМЯН, Т.А. Актуальные проблемы привлечения к ответственности лиц за преступления в сфере информационных технологий. În: *Юрис*т, 2018, № 5, с. 68-72. ISSN 1812-3929.

Potrivit lit. f) art. 4 al Proiectului, prin „tehnologii informaționale și ale comunicațiilor (TIC)" se înțelege „ansamblul de procedee, de procese de producție și de mijloace de software și hardware integrate în scopul formării, transformării, transferului, utilizării și stocării informațiilor."[623] Conform art. 3 al Legii nr. 467/2003, tehnologie informaţională se consideră „totalitatea de metode, procedee şi mijloace de prelucrare şi transmitere a informaţiei şi regulile de aplicare a acesteia."[624] De asemenea, în conformitate cu art. 2 al Legii nr. 1069/2000, prin „tehnologiile informaţiei" se înțelege „tehnologiile specifice informaticii, precum şi acelei părţi a comunicaţiei aferente traficului informatic în reţelele informatice."[625]

O sintagmă apropiată sub aspect semantic – „prin intermediul tehnologiilor informaţionale sau comunicaţiilor electronice" – este folosită în art. 175[1]. Deși sintagma „tehnologie informaţională" nu este utilizată expres în alte norme penale, recurgerea la asemenea tehnologii poate reprezenta metoda de comitere a multor altor infracțiuni.

Așadar, sintagma „tehnologie informaţională" caracterizează metoda de comitere a unor infracțiuni care sunt prevăzute de capitole diferite ale părții speciale a Codului penal al Republicii Moldova. Sintagma dată nu poate desemna factorul de grupare doar a infracțiunilor prevăzute în Capitolul XI din partea specială a Codului penal al Republicii Moldova. Implicit aceasta o confirmă L.V. Ivanova, care opinează: „Infracțiunile cibernetice trebuie privite ca fapte intenționate săvârșite prin utilizarea tehnologiei IT[626]"[627]; „Din rândul infracțiunilor cibernetice fac parte infracțiunile cibernetice „speciale" și infracțiunile cibernetice „de drept comun."[628] Cel mai probabil, infracțiunile, prevăzute în Capitolul XI din partea specială a Codului penal al Republicii Moldova, ar reprezenta, în opinia lui L.V. Ivanova, infracțiunile cibernetice „speciale"; celelalte infracțiuni, prevăzute de alte capitole din partea specială a Codului penal al Republicii Moldova, ar constitui infracțiunile cibernetice „de drept comun".

Ca urmare, este întemeiată renunțarea legiuitorului la titlul „Infracţiuni în domeniul tehnologiilor informaţionale", care era atribuit Capitolului VI[1] din Partea specială a Codului penal din 1961. Sintagma „infracţiuni în domeniul tehnologiilor informaţionale", ca și sintagma

---

[623] *Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности*. [citat 23.01.2021] Disponibil: https://www.mid.ru/documents/10180/3024875/Проект+конвенции+по+преступности+с+правками+секр+ООН.pdf/c93e68c9-9994-4769-951d-057c4881b8fd

[624] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.

[625] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

[626] „IT" este englezismul care desemnează abrevierea pentru sintagma „Information Technology" („tehnologia informației").

[627] ИВАНОВА, Л.В. Виды киберпреступлений по российскому уголовному законодательству. În: *Юридические исследования*, 2019, № 1, с. 25-33. ISSN 2409-7136.

[628] Ibidem.

„infracțiuni cibernetice”, nu sunt potrivite pentru a desemna grupul de infracțiuni prevăzute în Capitolul XI din partea specială a Codului penal al Republicii Moldova.[629]

Odată cu adoptarea Codului penal în vigoare, s-a produs o schimbare de paradigmă.

Titlul inițial al Capitolului XI din partea specială a Codului penal al Republicii Moldova a fost „Infracţiuni în domeniul informaticii”. Ulterior, a fost adoptată Legea nr. 254 din 09.07.2004 pentru modificarea şi completarea Legii telecomunicaţiilor nr. 520-XIII din 7 iulie 1995 şi a Codului penal al Republicii Moldova.[630] Prin această lege, Codul penal a fost completat cu art. 261^1 „Accesul neautorizat la reţelele şi serviciile de telecomunicaţii”, iar titlul Capitolului XI din partea specială a Codului penal al Republicii Moldova a fost modificat, devenind „Infracțiuni în domeniul informaticii și telecomunicațiilor”. Acest titlu nu a fost de lungă durată, deoarece, prin Legea nr. 278 din 18.12.2008 pentru modificarea şi completarea Codului penal al Republicii Moldova[631], titlul capitolului XI din partea specială a Codului penal al Republicii Moldova a fost modificat, devenind „Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor”. În mod regretabil, în Nota informativă la proiectul care se află la temelia ultimei dintre legile menționate, nu este prezentat niciun argument în susținerea modificării operate.[632]

Indiferent de titlul atribuit Capitolului XI din partea specială a Codului penal al Republicii Moldova, la stabilirea obiectului juridic generic al infracțiunilor corespunzătoare, trebuie să ia în vedere voința legiuitorului. Nu este admisibilă nicio improvizare, care ar echivala cu ignorarea acestei voințe.

Tocmai având în vedere titlul Capitolului XI al părții speciale a Codului penal al Republicii Moldova, S. Brînza, V. Stati[633] și A.T. Drăgan[634] consideră că obiectul juridic generic al faptelor infracționale specificate în acest capitol îl reprezintă relaţiile sociale din domeniul informaticii şi al telecomunicaţiilor.

---

[629] STRÎMBEANU, Alexandru. Obiectul juridic generic al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): aspectul *de lege lata*. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234980

[630] Legea pentru modificarea şi completarea Legii telecomunicaţiilor nr. 520-XIII din 7 iulie 1995 şi a Codului penal al Republicii Moldova: nr. 254 din 09.07.2004. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 189-192, 848.

[631] Legea 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, 98.

[632] *Proiectul legii pentru completarea și modificarea Codului penal al RM (art. 21, 196^1, 196^2 ș.a.)*. [citat 23.01.2021] Disponibil: old.parlament.md/lawprocess/laws/december2008/278-XVI-18.12.2008/

[633] BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005, p. 493. 804 p. ISBN 9975-79-324-X; STATI, Vitalie. Răspunderea penală pentru infracţiunile în domeniul informaticii şi telecomunicaţiilor. În: Analele Ştiinţifice ale Universităţii de Stat din Moldova. Seria „Ştiinţe socioumanistice”. Vol. 1. Chişinău: CEP USM, 2005, pp. 387-394. ISSN 1811-2668; BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011, p. 254. 1324 p. ISBN 978-9975-53-028-7; BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 342. 1300 p. ISBN 978-9975-53-470-3.

[634] DRĂGAN, Alin Teodorus. *Frauda informatică: analiza juridico-penală a infracțiunii*: tz. de doct. în drept. Chișinău, 2017, p. 119. 179 p.

Observăm că informatica și telecomunicațiile reprezintă perechea de valori sociale fundamentale, care sunt protejate contra infracțiunilor prevăzute în Capitolul XI al părții speciale a Codului penal al Republicii Moldova. În corespundere cu art. 2 al Legii nr. 1069/2000, prin „informatică" se înţelege „domeniul de activitate care include prelucrarea şi transportarea datelor cu ajutorul sistemelor automatizate de calcul şi al mijloacelor de telecomunicaţie"[635] În conformitate cu art. 2 al Legii nr. 520 din 07.07.1995 a telecomunicaţiilor (abrogate), prin „telecomunicaţii" se înțelege „orice transmisiune, emisie sau recepţie de semne, semnale, înscrieri, imagini, sunete sau informaţii [...] prin fir, radio, prin sisteme optice sau alte sisteme electromagnetice."[636]

Rețelele informatice, asociate celor de telecomunicații, au devenit indispensabile în soluționarea celor mai variate probleme cotidiene, de la ținerea corespondenței de afaceri prin Internet până la achitarea online a mărfurilor și a serviciilor. În pct. 7) din Preambulul Directivei (UE) 2018/1972 a Parlamentului European și a Consiliului din 11.12.2018 de instituire a Codului european al comunicațiilor electronice, se vorbește despre „convergența sectoarelor telecomunicațiilor și [...] tehnologiei informației.".[637] Această convergență este luată în considerare atât în definiția noțiunii „informatică" din art. 2 din cadrul Legii nr. 1069/2000, cât și în titlul Capitolul XI al părții speciale a Codului penal al Republicii Moldova. Drept urmare, este reușită juxtapunerea în acest titlu a noțiunilor „informatică" și „telecomunicaţii".

Cu toate acestea, titlul Capitolului XI din partea specială a Codului penal nu corespunde definiției din Hotărârea Guvernului nr. 857 din 31.10.2013 cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020": „Prin „securitate cibernetică" se înţelege starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive"[638] *„prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor [...] din spaţiul cibernetic* (evid. ns.)".[639]

Această necorespundere are drept cauză primară discrepanța dintre titlul Capitolului XI din partea specială a Codului penal și concepția promovată în Convenţia de la Budapesta.[640]

---

[635] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[636] Legea telecomunicaţiilor: nr. 520 din 07.07.1995. În: *Monitorul Oficial al Republicii Moldova*, 1995, nr. 65-66, 713.
[637] *Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11.12.2018 de instituire a Codului european al comunicațiilor electronice*. [citat 23.01.2021] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32018L1972&from=ro
[638] Hotărârea Guvernului cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020": nr. 857 din 31.10.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 252-257, 963.
[639] Ibidem.
[640] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561

Având în vedere prevederile Convenției de la Budapesta, S. Brînza și V. Stati propun următoarea clasificare: *„1) infracţiuni contra confidenţialităţii şi integrităţii datelor şi sistemelor informatice (prevăzute la art. 259, 260, 260[1]-260[4], 261 CP RM)”*[641]; *„2) infracţiuni informatice în accepţiune strictă (prevăzute la art. 260[5] şi 260[6] CP RM)* (evid. ns.)*”*[642]; 3) infracţiuni în domeniul telecomunicaţiilor (prevăzută la art. 261[1] CP RM).”[643] În Convenția de la Budapesta, Titlul 2 „Infracţiuni informatice” din Secţiunea 1 cuprinde art. 7 „Falsificarea informatică” și art. 8 „Frauda informatică”. Însă, din denumirea Capitolului XI din partea specială a Codului penal rezultă că sintagma „infracțiuni informatice” se referă nu doar la falsificarea informatică și la frauda informatică.

Probabil, anume această lipsă de congruență dintre prevederile legii penale autohtone și prevederile Convenției de la Budapesta i-a determinat pe unii doctrinari să stabilească conținutul obiectului juridic generic al faptelor infracționale, ce sunt prevăzute în Capitolul XI al părții speciale a Codului penal, fără a ține seama de voința legiuitorului, exprimată în titlul acestui capitol.[644] Suntem de părerea că o opinie doctrinară, chiar de o valoare științifică incontestabilă, nu poate substitui voința legiuitorului. În general, în cazul în care legea penală este imperfectă, sarcina unui doctrinar este să semnaleze prezența imperfecțiunii respective și să propună îmbunătățirea calității legii penale. Asumându-ne această sarcină, ne propunem să identificăm soluția optimă în vederea reformulării titlului Capitolului XI al părții speciale a Codului penal.

Este de consemnat că versiunea în limba rusă a acestui capitol este «Информационные преступления и преступления в области электросвязи». Așadar, sintagma „infracțiuni informatice” a fost tradusă ca «информационные преступления». Aceasta deși versiunea în limba rusă a Legii nr. 1069/2000 se numește «Закон об информатике».

Apropiată de sintagma „infracțiuni informaționale” este sintagma „infracțiuni contra securității informaționale”, utilizată în denumirea Capitolului 30 din Codul penal model al CSI[645]

---

[641] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 345-346. 1300 p. ISBN 978-9975-53-470-3.
[642] Ibidem, p. 346.
[643] Ibidem, p. 346.
[644] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 568. 836 p. ISBN 9975-61-291-1; BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 362. 622 p. ISBN 9975-9788-7-8; BARBĂNEAGRĂ, Alexei et al. *Codul penal comentat şi adnotat*. Chişinău: Cartier, 2005, p. 434. 656 p. ISBN 9975-29-338-X; ГРИЩУК-БУЧКА, Светлана. Уголовно-правовая характеристика преступлений против компьютерной безопасности (по законодательству Республики Молдова). În: *Securitatea informaţională 2010. Conferinţă internaţională (Chişinău, 15-16 aprilie 2010)*. Chișinău: ASEM, 2010, pp. 97-101. ISBN 978-9975-75-509-2.
[645] *Модельный Уголовный кодекс. Рекомендательный законодательный акт для Содружества Независимых Государств*. [citat 06.03.2022] Disponibil: docs.cntd.ru/document/901781490

și a Capitolului 31 din Codul penal al Republicii Belarus.[646] Referitor la denumirea Capitolului 31 din Codul penal al Republicii Belarus, N.A. Sivițkaia afirmă în termeni critici: „Circumstanțierea de către legiuitor a obiectului juridic generic al acestor infracțiuni este neclară. [...] Nu s-a pus accentul pe natura informatică a securității informațiilor protejate."[647]

Din această perspectivă, nu putem agrea viziunile lui V. Moraru, M. Guzun,[648] R. Gojan, Iu. Stan[649] și A.-M. Tîrziu[650], care confundă noțiunile „securitatea informațională" și „securitatea informatică (cibernetică)". În mod evident, securitatea informațională nu poate fi echivalată cu securitatea informațiilor de natură informatică. Mai grav este că noțiunile „securitatea informațională" și „securitatea informatică (cibernetică) sunt privite ca interschimbabile în cadrul unui act normativ (de exemplu, în Hotărârea Parlamentului nr. 153 din 15.07.2011 pentru aprobarea Strategiei securităţii naţionale a Republicii Moldova.[651]

T. Bragaru, V. Briceag, V. Malcoci și V. Galaicu argumentează: „Securitatea informațională [...] reflectă o realitate sistemică [...] complexă, înglobând în sine [...] securitatea informatică [...]."[652] Un punct de vedere similar îl exprimă D.S. Azarov: „Conceptul de securitate informațională este evident mult mai larg decât cel de securitate a relațiilor sociale în domeniul informațiilor de natură informatică"[653]; „Securitatea informațională constituie securitatea întregului spațiu informațional. Informațiile de natură informatică corespund [...] nu întregului flux de informații".[654] În viziunea acestor autori, sintagma „securitatea informațională" se referă la securitatea informațiilor de orice gen, la securitatea acestora împotriva anumitor amenințări.

O părere cumva diferită o au A. Smochină și A. Grișciuc-Bucica, care susțin că „termenul „informație" din sintagma „securitate informațională" indică direcția de activitate prin

---

[646] *Уголовный Кодекс Республики Беларусь: № 275-З от 9 июля 1999 г.* [citat 06.03.2022] Disponibil: https://kodeksy-by.com/ugolovnyj_kodeks_rb.htm

[647] СИВИЦКАЯ, Н.А. Объект компьютерных преступлений в УК Белоруссии. În: *Информационное право*, 2007, № 3, с. 25-29. ISSN 1999-480X.

[648] MORARU, Victor, GUZUN, Mihai. Informația și securitatea informațională ca obiect al protecției juridico-penale. În: *Revista de Ştiinţe Penale*, 2006, Anuar, pp. 150-159. ISSN 1812-3392.

[649] GOJAN, Roman, STAN, Iulian. Infracțiunile informaționale și spionajul informațional. În: *Securitatea informaţională 2013. Conferința internațională „Securitatea informaţională" (Chișinău, Moldova, 19 aprilie 2013)*. Chișinău: ASEM, 2013, pp. 103-110. ISBN 978-9975-75-640-2.

[650] TÎRZIU, Andreea-Maria. Protecția și securitatea informațiilor la nivelul autorităților publice naționale din România. În: *Sesiunea de comunicări ştiinţifice „Oraşul inteligent"*. București: Editura Economică, 2015, pp. 120-138. ISSN 2501-1677.

[651] Hotărârea Parlamentului pentru aprobarea Strategiei securităţii naţionale a Republicii Moldova: nr. 153 din 15.07.2011. În: *Monitorul Oficial al Republicii Moldova*, 2011, nr. 170-175, 499.

[652] BRAGARU, Tudor, BRICEAG, Valentin, MALCOCI, Viorel, GALAICU, Valeriu. Securitatea informației vis-a-vis de securitatea informațională. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe exacte şi economice"*, 2019, nr. 2, pp. 38-47. ISSN 1814-3199.

[653] АЗАРОВ, Д.С. *Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)*. Київ: Атіка, 2007, с. 51-52. 304 с. ISBN 966-326-230-3.

[654] Ibidem, с. 51-52.

intermediul căreia se aduce atingere obiectului de protecție”[655]; „În acest caz, conceptul „securitate informațională” ar trebui interpretat ca starea de protecție a acestui obiect împotriva amenințărilor de ordin informațional.”[656] Această părere își găsește consacrare în legislație. Astfel, în Legea nr. 299 din 21.12.2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova, în pct. 10 din anexă, sunt definite două noțiuni relevante: „securitate informaţională – starea de protecție a resurselor informaţionale, precum și a persoanei, societăţii şi statului, în spaţiul informațional”[657]; „spaţiu informaţional – mediul de activitate [...] asociat cu formarea, crearea, transformarea, transmiterea, difuzarea, utilizarea și stocarea informaţiilor”[658], „care produce efecte la nivel de conştiinţă individuală şi/sau socială, de infrastructură informaţională şi de informaţie.”[659] Definiția noțiunii de securitate informaţională este formulată, de asemenea, în art. 1 din Codul serviciilor media audiovizuale: „securitate informaţională – starea de protecţie a resurselor informaţionale, a persoanei, a societăţii şi a statului”[660], „inclusiv prezenţa unui ansamblu de măsuri pentru asigurarea protecţiei persoanei, a societăţii şi a statului de eventuale tentative de dezinformare şi/sau de informare manipulatorie din exterior”[661] „şi pentru neadmiterea agresiunii mediatice îndreptate împotriva Republicii Moldova”.[662] Înainte de a fi abrogat, Codul audiovizualului, în dispoziția de la lit. z^5) art. 2 conținea definiția aceleiași noțiuni.[663] Din aceste definiții desprindem că prin „securitate informațională” se înțelege starea de protecție a persoanei, statului, societății împotriva unor informaţii care produc efecte distructive la nivel de conştiinţă individuală şi/sau socială. Bineînțeles, nu această concepție este pusă la baza denumirii Capitolului XI din partea specială a Codului penal al Republicii Moldova.

În alt context, în Codul penal al Kazahstanului, Capitolul 7 din partea specială poartă denumirea „Delicte penale în sfera informatizări și comunicațiilor.”[664] Ar fi oare potrivită implementarea unei astfel de concepții în titlul Capitolului XI din partea specială a Codului penal

---

[655] СМОКИНЭ, Андрей, ГРИЩУК-БУЧКА, С.К. вопросу о правовом соотношении понятий: «информационная безопасность», «защита информации» и «кибербезопасность». În: *Studii Juridice Universitare*, 2013, nr. 1-2, pp. 81-88. ISSN 1857-4122.
[656] Ibidem.
[657] Legea privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova: nr. 299 din 21.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 48-57, 122.
[658] Ibidem.
[659] Ibidem.
[660] Codul serviciilor media audiovizuale al Republicii Moldova: nr. 174 din 08.11.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 462-466, 766.
[661] Ibidem.
[662] Ibidem.
[663] Codul audiovizualului al Republicii Moldova: nr. 260 din 27.07.2006. În: *Monitorul Oficial al Republicii Moldova*, 2006, nr. 131-133, 679.
[664] *Уголовный кодекс Республики Казахстан*. [citat 06.03.2022] Disponibil: https://online.zakon.kz/Document/?doc_id=31575252

al Republicii Moldova? Considerăm că nu, nu ar fi potrivită. O asemenea concepție ar fi prea îngustă pentru a caracteriza ceea ce reunește la nivel de grup infracțiunile prevăzute de art. 259-261[1] CP RM.

În corespundere cu art. 2 al Legii nr. 1069/2000, prin „informatizare" se înțelege „ansamblul organizat de acţiuni destinate creării, implementării, întreţinerii şi perfecţionării sistemelor automatizate de calcul şi transport de date"[665] „în procesul de colectare, stocare, prelucrare şi difuzare a informaţiei".[666] Potrivit art. 3 al Legii nr. 467/2003, noțiunea de informatizare este definită într-o manieră similară: „proces organizatoric social-economic şi tehnico-ştiinţific de creare a unor condiţii optime pentru satisfacerea necesităţilor informaţionale"[667] „şi realizarea drepturilor cetăţenilor, autorităților publice, instituțiilor publice şi persoanelor juridice în baza formării şi utilizării resurselor informaţionale."[668]

În același timp, în acord cu art. 1 al Legii nr. 467/2003, obiectul de reglementare al acesteia îl constituie „raporturile juridice care apar în procesul de creare, formare şi utilizare a resurselor informaţionale automatizate de stat, nu și raporturile care apar la crearea şi funcţionarea resurselor informaţionale nestatale."[669] Așadar, cel puțin din perspectiva Legii nr. 467/2003, domeniul informatizării constituie o parte doar a sectorului public. Pentru comparație, în acord cu Legea nr. 1069/2000, obiectul de reglementare al acesteia îl reprezintă raporturile juridice din sfera informaticii, la care participă statul, precum și persoanele juridice şi persoanele fizice de drept public sau de drept privat. Astfel, domeniul informaticii nu se limitează la sectorul public.[670]

Din aceste considerente, noțiunea „informatizare" nu ar fi capabilă să redea întreaga complexitate a relațiilor sociale care sunt protejate contra infracțiunilor ce sunt prevăzute de art. 259-261 CP RM.

În altă privință, de ce propunem pentru Capitolul XI al părții speciale a Codului penal sintagma „infracţiuni contra securității comunicațiilor electronice" în locul sintagmei actuale „infracțiuni în domeniul telecomunicațiilor"?

---

[665] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[666] Ibidem.
[667] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.
[668] Ibidem.
[669] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.
[670] STRÎMBEANU, Alexandru. Obiectul juridic generic al infracțiunilor de acces ilegal la informația computerizată (art. 259 din Codul penal al Republicii Moldova): aspectul *de lege ferenda*. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234982

Or, după cum am menționat anterior, noțiunea „telecomunicații” a fost definită în Legea nr. 520 din 07.07.1995 a telecomunicaţiilor. Această lege nu mai este în vigoare, deoarece a fost abrogată la data când a intrat în vigoare Legea nr. 241 din 15.11.2007 a comunicaţiilor electronice[671] (în continuare – Legea nr. 241/2007). Astfel, la nivel normativ, conceptul „telecomunicații” a fost substituit prin conceptul „comunicații electronice”. Actuala denumire a Capitolului XI din partea specială a Codului penal este anacronică, întrucât nu ține cont de această substituire.

Prin „comunicații electronice” se înțelege comunicațiile care alcătuiesc reţeaua de comunicaţii electronice. Această concluzie reiese din art. 2 al Legii nr. 241/2007, potrivit căruia prin „reţea de comunicaţii electronice” se are în vedere „sistemele de transmisie şi, după caz, echipamentele de comutare sau rutare, precum şi alte resurse care permit transmiterea semnalelor”[672] „prin suport fizic, electromagnetic sau prin orice alte mijloace, incluzând reţelele de comunicaţii prin satelit, reţelele fixe (cu comutare de circuite sau comutare de pachete, inclusiv Internet)”[673] „şi reţelele mobile terestre, reţelele de transport al energiei electrice, în cazul în care acestea sunt utilizate şi pentru transmiterea semnalelor, reţelele utilizate pentru difuzarea programelor audiovizuale”[674], „reţelele de televiziune prin cablu, indiferent de tipul informaţiei transmise”.[675] Așadar, noțiunea „comunicații electronice” derivă din noțiunea „reţea de comunicaţii electronice”.

În alin. 21 art. 2 al Directivei (UE) 2018/1972 a Parlamentului European și a Consiliului din 11.12.2018 de instituire a Codului european al comunicațiilor electronice, identificăm definiția noțiunii „securitatea rețelelor și serviciilor”: „capacitatea rețelelor și serviciilor de comunicații electronice de a rezista, la un nivel de încredere determinat, oricărei acțiuni”[676] „care afectează disponibilitatea, autenticitatea, integritatea sau confidențialitatea acestor rețele și servicii”[677], „a datelor stocate, transmise ori prelucrate sau a serviciilor aferente oferite de rețelele ori serviciile de comunicații electronice respective sau accesibile prin intermediul acestora”.[678] Din noțiunea „securitatea rețelelor și serviciilor de comunicații electronice” derivă noțiunea „securitatea comunicațiilor electronice”.

---

[671] Legea comunicaţiilor electronice: nr. 241 din 15.11.2007. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 51-54, 155.
[672] Ibidem.
[673] Ibidem.
[674] Ibidem.
[675] Ibidem.
[676] *Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11.12.2018 de instituire a Codului european al comunicațiilor electronice*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32018L1972&from=ro
[677] Ibidem.
[678] Ibidem.

În următorul capitol al tezei vom argumenta că securitatea datelor informatice şi a comunicaţiilor electronice ar trebui să reprezinte valoarea socială fundamentală ce este protejată împotriva infracțiunilor ce sunt specificate în Capitolul XI al părții speciale a Codului penal al Republicii Moldova. Care este structura relațiilor sociale privitoare la securitatea datelor informatice şi a comunicaţiilor electronice?

După S. Brînza, „structural, relaţiile sociale presupun trei elemente: 1) subiecte, 2) conţinut şi 3) obiect. [...] În calitate de subiecte sociale, adică de participanţi la viaţa socială, pot evolua oamenii”[679], „priviţi individual [...] sau încadraţi în anumite organizaţii, colective, diverse comunităţi sociale [...]. Conţinutul relaţiei sociale poate fi definit ca totalitate a facultăţilor sociale pe care le au participanţii la viaţa socială”[680]. „[...] Se cere a detaşa în cadrul tuturor relaţiilor sociale un obiect specific de legătură, caracterul conexiunii dintre participanţii la relaţia socială. [...]”.[681] „Acţiunea sau abstenţiunea, pe care subiectele relaţiei sociale au interesul să le săvârşească, determină apariţia sau modificarea oricărui tip de relaţie socială”.[682] „În alţi termeni, conduita subiectelor relaţiei sociale reprezintă un factor obiectiv care mediază relaţia dintre subiecţii sociali”.[683]

Oricare relație socială presupune interacționarea, relaționarea a doi sau mai multor subiecți. O relație este socială în virtutea legăturii dintre membrii societății, care îndeplinesc rolul de participanți în cadrul respectivei relații. Dacă lipsesc subiecții relației sociale, atunci lipsește relația socială însăși.

În Legea nr. 1069/2000, subiecții relațiilor sociale cu privire la securitatea datelor informatice sunt descriși în felul următor: „persoanele care activează în cadrul sistemelor şi reţelelor informatice”[684] (alin. (2) art. 4 și alin. (1) art. 28); „persoanele care creează şi furnizează produse informatice sau care prestează servicii informatice”[685] (alin. (1) art. 14); „subiecte ale dreptului de proprietate în domeniul informaticii”[686] (alin. (2) art. 29); „proprietarul produselor informatice”[687] (alin. (4) art. 29) etc. În Legea nr. 20/2009, subiecții relațiilor respective sunt

[679] BRÎNZA, Serghei. *Obiectul infracţiunilor contra patrimoniului*. Chișinău: Tipografia Centrală, 2005, p. 58. 675 p. ISBN 9975-70-414-X.
[680] Ibidem, p. 58.
[681] Ibidem, p, 60.
[682] Ibidem, p, 62.
[683] Ibidem, p. 62.
[684] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[685] Ibidem.
[686] Ibidem.
[687] Ibidem.

descrişi în astfel de termeni: „proprietarii de sisteme informatice”[688] (art. 6); „furnizorii de servicii informatice”[689] (art. 7); „persoane responsabile” (lit. b) alin. (1) art. 7) etc. În Legea nr. 241/2007, subiecţii relaţiilor sociale cu privire la securitatea comunicaţiilor electronice sunt descrişi în modul următor: „persoanele care activează în domeniul comunicaţiilor electronice”[690] (alin. (2) art. 5); „furnizorii de reţele publice de comunicaţii electronice”[691] (alin. (1) art. 18); „furnizorii de reţele publice de comunicaţii electronice și/sau servicii de comunicaţii electronice”[692] (alin. (1) art. 20); „furnizorii de servicii de acces la Internet” (alin. (2^1) art. 20); „consumatori”[693] (alin. (6) art. 64) etc.

În cadrul oricărei relaţii sociale, participanţii la ele au anumite drepturi subiective și/sau obligaţii corelative. În lipsa acestor drepturi și obligaţii, relaţia socială ar fi o formă fără conţinut, o abstracţie.

Referitor la conţinutul relaţiilor sociale referitoare la securitatea datelor informatice, în Legea nr. 1069/2000 se menţionează: „drepturile şi obligaţiile statului, ale persoanelor juridice şi fizice în procesul creării, administrării, utilizării şi întreţinerii sistemelor informatice”[694] (art. 1); „Orice persoană este în drept să deţină date, programe şi echipamente”[695], „precum şi să prelucreze date şi programe, cu obţinerea unor produse informatice pentru uz propriu, dacă aceasta nu contravine prevederilor prezentei legi”[696] (alin. (1) art. 16); „Persoanele [...] au dreptul să obţină de la titularii bazelor de date [...] confirmarea că aceştia deţin sau nu date care se referă la persoana respectivă”[697] (alin. (1) art. 20); „Persoanele care activează în cadrul sistemelor şi reţelelor informatice sunt obligate să asigure protecţia şi confidenţialitatea datelor, cu excepţia celor [...] determinate ca date publice”[698] (alin. (1) art. 28) etc. În Legea nr. 20/2009, conţinutul relaţiilor sociale cu privire la securitatea datelor informatice este reprezentat de obligaţiile proprietarilor de sisteme informatice (art. 6) și de obligaţiile furnizorilor de servicii informatice (art. 7). În Legea nr. 241/2007, referitor la la conţinutul relaţiilor sociale cu privire la securitatea comunicaţiilor electronice, se prevede: „drepturile şi obligaţiile statului, ale persoanelor fizice şi

---

[688] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.
[689] Ibidem.
[690] Legea comunicaţiilor electronice: nr. 241 din 15.11.2007. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 51-54, 155.
[691] Ibidem.
[692] Ibidem.
[693] Ibidem.
[694] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[695] Ibidem.
[696] Ibidem.
[697] Ibidem.
[698] Ibidem.

juridice în procesul creării, gestionării şi utilizării reţelelor de comunicaţii electronice”[699] (alin. (1) art. 1); „drepturile şi obligaţiile utilizatorilor pe întreg teritoriul Republicii Moldova”[700] (alin. (2) art. 1); „dreptul de acces al furnizorului la reţelele sale de comunicaţii electronice”[701] (alin. (5) art. 18); „dreptul de a utiliza una sau mai multe frecvenţe sau canale radio”[702] (alin. (1) art. 26) etc.

Privitor la obiectul relațiilor sociale cu privire la securitatea datelor informatice, în Legea nr. 1069/2000 se menționează despre: „accesul oricărei persoane juridice şi fizice la serviciile informatice publice şi la informaţiile ce se conţin în sistemele informatice”[703] (alin. (1) art. 3); „circulaţia datelor şi programelor între doi sau mai mulţi utilizatori”[704] (art. 2); „circulaţia datelor pe teritoriul Republicii Moldova”[705] (alin. (1) art. 13) etc. În Legea nr. 20/2009, obiectul relațiilor sociale referitoare la securitatea datelor informatice este caracterizat, de exemplu, prin cuvintele „comunicare transmisă printr-un sistem informatic”[706] (art. 2). În Legea nr. 241/2007, referitor la obiectul relațiilor sociale cu privire la securitatea comunicaţiilor electronice, se menționează despre: „accesul oricărei persoane fizice sau juridice la serviciile de comunicaţii electronice accesibile publicului”[707] (alin. (1) art. 3); „accesul tuturor utilizatorilor finali de pe teritoriul Republicii Moldova la serviciul universal”[708] (lit. f) alin. (6) art. 8) etc.

În altă ordine de idei, concretizarea primară a obiectului juridic generic se realizează prin stabilirea obiectului juridic special. După V. Grosu, „obiectul juridic special al infracţiunii este valoarea socială concretă (și, implicit, relaţiile sociale corespunzătoare) căreia i se aduce atingere prin infracţiune.”[709] „Obiectul juridic special al infracţiunii este obiectul infracţiunii, așa cum acesta este descris prin norma incriminatoare”.[710] În viziunea lui I. Macari, obiectul juridic

---

[699] Legea comunicaţiilor electronice: nr. 241 din 15.11.2007. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 51-54, 155.
[700] Ibidem.
[701] Ibidem.
[702] Ibidem.
[703] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[704] Ibidem.
[705] Ibidem.
[706] Legea privind prevenirea și combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.
[707] Legea comunicaţiilor electronice: nr. 241 din 15.11.2007. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 51-54, 155.
[708] Ibidem.
[709] BOTNARU, Stela, ȘAVGA, Alina, GRAMA, Mariana, GROSU, Vladimir. *Drept penal. Partea generală*. Chișinău: Cartier, 2005, p. 153. 624 p. ISBN 9975-79-318-5; GRAMA, Mariana, BOTNARU, Stela, ȘAVGA, Alina, GROSU, Vladimir. *Dreptul penal: partea generală. Vol. I*. Chișinău: Tipografia Centrală, 2012, p. 182. 328 p. ISBN 978-9975-53-080-4.
[710] BOTNARU, Stela, ȘAVGA, Alina, GRAMA, Mariana, GROSU, Vladimir. *Drept penal. Partea generală*. Chișinău: Cartier, 2005, p. 153. 624 p. ISBN 9975-79-318-5; GRAMA, Mariana, BOTNARU, Stela, ȘAVGA,

special al infracţiunii „îl formează acea valoare socială concretă asupra căreia a atentat infractorul”.[711] Într-o altă lucrare de-a sa, I. Macari afirmă că obiectul juridic special al infracţiunii „îl constituie valoarea socială concretă, ocrotită de lege, asupra căreia e îndreptată fapta infracțională a vinovatului”.[712]

În paginile de mai jos vom prezenta punctele de vedere ale unor teoreticieni din alte state cu privire la obiectul juridic special al infracțiunilor care sunt prevăzute de articolele corespondente cu art. 259 CP RM.

Astfel, în primul rând, vom reproduce părerile unor penaliști din România, privitoare la obiectul juridic special al infracțiunilor ce sunt prevăzute de art. 360 CPR sau la art. 42[713] din Legea României nr. 161/2003[714]: „relaţiile sociale care se nasc şi se dezvoltă în legătură cu siguranţa şi integritatea unui sistem informatic şi implicit a unor date informatice”[715] (C. Duvac); „relaţii sociale, precum: patrimoniul organizaţiei, instituţiei, persoanei respective, încrederea publică în măsurile de siguranţă ale integrităţii datelor, cele privind concurenţa etc.”[716] (M. Gorunescu și S. Corlățeanu). Opinii similare au alți autori români.[717]

În doctrina juridică de specialitate din Ucraina, opiniile, referitoare la obiectul juridic special al infracțiunilor ce sunt prevăzute de art. 361 CPU („Imixtiunea neautorizată în funcționarea mașinilor electronice de calcul (computerelor), a sistemelor automate, a rețelelor de computere

---

Alina, GROSU, Vladimir. *Dreptul penal: partea generală. Vol. I*. Chișinău: Tipografia Centrală, 2012, p. 182. 328 p. ISBN 978-9975-53-080-4.

[711] BORODAC, Alexandru, BUJOR, Valeriu, BRÎNZA, Serghei. *Drept penal. Partea generală*. Chișinău: Știința, 1994, p. 76. 368 p. ISBN 5-376-01847-4.

[712] MACARI, Ivan. *Dreptul penal al Republicii Moldova. Partea generală*. Chișinău: CE USM, 2002, p. 95. 308 p. ISBN 9975-70-190-6.

[713] Acest articol conținea următoarele prevederi: „(1) Accesul, fără drept, la un sistem informatic constituie infracţiune şi se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă.”* „(2) Fapta prevăzută la alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoare de la 6 luni la 5 ani.”* „(3) Dacă fapta prevăzută la alin. (1) sau (2) este săvârşită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani.”*

* Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.

Art. 42 din Legea României nr. 161/2003 a fost abrogat la 01.02.2014 prin Legea României nr. 187 din 24.10.2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal.**

** Monitorul Oficial al României, 2012, nr. 757.

[714] Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.

[715] DUVAC, Constantin. Accesul ilegal la un sistem informatic în reglementarea noului Cod penal. În: *Revista română de dreptul proprietăţii intelectuale*, 2012, nr. 1, pp. 88-109. ISSN 1584-7241.

[716] GORUNESCU, Mirela, CORLĂŢEANU, Sorin. Delictele informatice potrivit noului Cod penal. În: *Revista de Drept Penal*, 2007, nr. 1, pp. 52-53. ISSN 1223-0790.

[717] DOBRINOIU, Maxim. *Infracţiuni în domeniul informatic*. Bucureşti: C.H. Beck, 2006, p. 147. 401 p. ISBN 978-973-655-941-9; FLORESCU, Valentin, FLORESCU, Gabriela. Analiza infracţiunilor informatice incriminate în legislaţia în vigoare şi din perspectiva noului Cod penal. În: *Revista Română de Informatică şi Automatică*, 2012, vol. 22, nr. 2, pp. 21-38. ISSN 1841-4303; VASIU, Ioana, VASIU, Lucian. *Informatică juridică şi drept informatic*. Cluj-Napoca: Editura Albastră, 2002, p. 166. 225 p. ISBN 973-650-068-3.

sau a rețelelor de telecomunicații”[718]), sunt: „Obiectul juridic principal al acestor infracțiuni trebuie considerat a fi reprezentat de relațiile sociale în domeniul datelor informatice”[719], „care apar și există în legătură cu desfășurarea de către o persoană (persoane) a unor activități privind datele informatice, relații care sunt vătămate efectiv sau potențial în rezultatul comiterii infracțiunii”[720]; „Obiectul juridic secundar al acestor infracțiuni îl constituie relațiile sociale de proprietate asupra datelor informatice”[721] (D.S. Azarov); „dreptul de proprietate asupra datelor informatice”[722] (M.V. Karcevski). Opinii asemănătoare au alți autori ucraineni.[723]

În doctrina penală a Federației Ruse, punctele de vedere privitoare la obiectul juridic special al infracțiunilor ce sunt prevăzute de art. 272 CP FR[724] („Accesul ilegal la informația computerizată”) sunt: „Subiectul aduce atingere, pe de o parte, relațiilor sociale privind asigurarea integrității și siguranței informației computerizate, iar, pe de altă parte, drepturilor constituționale de inviolabilitate a vieții private, a secretului personal și a celui familial”[725] (R.R. Gaifutdinov); „relațiile sociale privite ca relații care asigură securitatea (inviolabilitatea) informației computerizate”[726] (Iu. Leapunov și V. Maksimov). Puncte de vedere apropiate au alți autori ruși.[727]

---

[718] *Кримінальний кодекс України*. [citat 18.12.2020] Disponibil: https://zakon.rada.gov.ua/laws/show/2341-14#Text.

[719] АЗАРОВ, Д.С. *Кримінальна відповідальність за злочини у сфері комп'ютерної інформації*: автореф. дис. на здоб. науков. ступ. канд. юрид. наук. Київ, 2003, с. 7-8. 18 с.

[720] Ibidem, с. 7.

[721] Ibidem, с. 8.

[722] КАРЧЕВСЬКИЙ, М.В. Злочини у сфері використання комп'ютерної техніки. Київ: Атіка, 2010, с. 54, 127. 168 с.

[723] *Уголовный кодекс Украины: научно-практический комментарий* / Отв. ред. Е.Л. СТРЕЛЬЦОВ. Харьков: Одиссей, 2007, с. 682. 864 с. ISBN 978-966-633-611-1; КОЗАК, Н.С. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. În: *Збірник наукових праць Ірпінської фінансово-юридичної академії (економіка, право)*, 2013, № 2, с. 154-159.

[724] Уголовный кодекс Российской Федерации. În: *Собрание законодательства Российской Федерации*, 1996, № 25.

[725] ГАЙФУТДИНОВ, Р.Р. Уголовно-правовая характеристика посягательств на персональные данные, обрабатываемые в автоматизированных системах. În: *Ученые записки Казанского университета. Серия Гуманитарные науки*, Том 156, № 4, 2014, с. 158-164. ISSN 2541-7738.

[726] ЛЯПУНОВ, Ю., МАКСИМОВ, В. Ответственность за компьютерные преступления. În: *Законность*, 1997, № 1, с. 8-15. ISSN 0869-4486.

[727] ГУЗЕЕВА, О.С. *Квалификация преступлений в сфере компьютерной информации*. Москва: АГП РФ, 2016, с. 29. 60 с.; САФОНОВ, О.М. *Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования*: дис. на соиск. учен. степ. канд. юрид. наук. Москва, 2015, с. 83. 222 с.; ШАРКОВ, А.Е. *Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Ставрополь, 2004, с. 12. 24 с.; ЕФРЕМОВА, М.А. *Уголовно-правовая охрана информационной безопасности*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Москва, 2018, с. 47. 59 с.; СПИРИНА, С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Волгоград, 2001, с. 15. 24 с.; МАЛЫШЕНКО, Д.Г. *Уголовная ответственность за неправомерный доступ к компьютерной информации*: дис. на соиск. учен. степ. канд. юрид. наук. Москва, 2002, с. 40. 166 с.; ОЗЕРОВА, А.С. О необходимости изменения подхода к понятию «информация» в законодательстве и

În teoria dreptului penal al Republicii Belarus, viziunile relative la obiectul juridic special al infracțiunilor ce sunt prevăzute de art. 349 CP RBe[728] („Accesul neautorizat la informația computerizată”) sunt: „obiectul juridic principal al acestor infracțiuni îl formează securitatea informatică, iar drepturile și interesele legitime ale proprietarilor și utilizatorilor datelor informatice constituie obiectul juridic secundar al acestora”[729] (A.I. Lukașov); „ordinea de accesare a informației computerizate, care îi acordă subiectului dreptul de a face cunoștință cu aceasta”[730]; „relațiile sociale în care se realizează ordinea stabilită de cunoaștere și de gestionare a datelor informatice”[731] (N.A. Ahramenka). Opinii similare au alți autori bieloruși.[732]

Nu în ultimul rând, în doctrina juridică de specialitate a Republicii Kazahstan, în legătură cu obiectul juridic special, pe care îl au infracțiunile ce sunt specificate în art. 205 („Accesul ilegal la informațiile protejate, la sistemul informatic sau la rețeaua de telecomunicații”[733]) al Codului penal al Republicii Kazahstan din 03.07.2014 sau la art. 227^2 („Accesul ilegal la informație, la sistem de informatic sau la rețeaua informatică ori cea de comunicații”[734]) al Codului penal al Republicii Kazahstan din 16.07.1997, sunt exprimate următoarele puncte de vedere: „relațiile sociale cu privire la [protecția] resurselor electronice, a sistemelor informatice și a sistemului de informatică și de comunicații împotriva amenințărilor interne și externe”[735] (A.B. Bekmagambetov, V.P. Revin și V.V. Revina); „relațiile sociale [...] care asigură: a) confidențialitatea informației computerizate protejate de lege; b) securitatea informației

---

судебной практике. În: *Правоведение*, 2019, Т. 63, № 1, с. 137-156. ISSN 0131-8039; НОВОСЕЛОВ, Г.П. *Учение об объекте преступления. Методологические аспекты*. Москва: Норма, 2001, с. 56. 208 с. ISBN 5-89123-533-1.

[728] *Уголовный Кодекс Республики Беларусь: № 275-З от 9 июля 1999 г.* [citat 06.03.2022] Disponibil: https://kodeksy-by.com/ugolovnyj_kodeks_rb.htm

[729] ЛУКАШОВ, А.И. *Уголовное право Республики Беларусь. Особенная часть* / Под общ. ред. А.И. ЛУКАШОВА. Минск: Гревцов, 2009, с. 648. 892 с. ISBN 978-985-6826-49-1.

[730] *Научно-практический комментарий к Уголовному кодексу Республики Беларусь* / Под общ. ред. А.В. БАРКОВА, В.М. ХОМИЧА. Минск: ГИУСТ БГУ, 2007, с. 761. 1007 с. ISBN 978-985-6739-60-9.

[731] *Научно-практический комментарий к Уголовному кодексу Республики Беларусь* / Под общ. ред. А.В. БАРКОВА, В.М. ХОМИЧА. Минск: ГИУСТ БГУ, 2010, с. 814. 1064 с. ISBN 978-985-491-021-5.

[732] НИКИТЕНКО, О.Г. Несанкционированный доступ к компьютерной информации. În: *Теория и практика совершенствования законодательства и правоприменения: традиции и новации: материалы междунар. науч. конф. студентов, магистрантов и аспирантов (Минск, 30-31 окт. 2009 г.)*. Минск, 2010, с. 189-190. ISBN 978-985-518-379-3; *Уголовное право. Особенная часть* / Под ред. В.А. КАШЕВСКОГО. Минск: Академия МВД, 2012, с. 502. 736 с. ISBN 978-985-427-775-2; ТАНАНА, Ю.Н. Границы уголовно-правовой охраны информационной безопасности. În: *Уголовная политика Республики Беларусь: состояние и пути совершенствования: сб. материалов III Междунар. науч.-практ. конф. (Барановичи, 11-13 мая 2017 г.)*. Барановичи: БарГУ, 2017, с. 161-162. ISBN 978-985-498-763-7.

[733] *Уголовный кодекс Республики Казахстан*. [citat 06.03.2022] Disponibil: https://online.zakon.kz/Document/?doc_id=31575252

[734] Ibidem.

[735] БЕКМАГАМБЕТОВ, А.Б., РЕВИН, В.П., РЕВИНА, В.В. *Уголовное право Республики Казахстан. Особенная часть*. Москва: Издательский дом Академии Естествознания, 2017, с. 150. 396 с. ISBN 978-5-91327-448-9.

computerizate și a computerelor”[736]; „c) securitatea exploatării unui computer, a sistemului informatic sau a rețelei informatice ori de comunicații”[737] (A.T. Ismagulova și A.M. Galiaskarova); „dreptul asupra informației, care aparține deținătorului acesteia sau unor terțe persoane”[738] (I.Ș. Borceașvili).

Toate opiniile exprimate de către teoreticienii din alte state, citate mai sus, prezintă, fără îndoială, interes științific. Totuși, aceste opinii sunt, în mare parte, irelevante pentru studiul de față. Or, normele din legile penale ale altor state, ce sunt corespondente cu art. 259 CP RM, au un conținut diferit de cel al art. 259 CP RM. Obiectul juridic special al unei infracțiuni poate fi stabilit doar în rezultatul analizei legii penale care prevede răspunderea pentru acea infracțiune. Obiectul juridic special al unei infracțiuni nu poate fi stabilit în rezultatul analizei legilor penale ale altor state. În rezultatul unei asemenea analize ar fi prezentat într-un mod distorsionat conținutul pe care îl are obiectul juridic special al infracțiunilor ce sunt prevăzute de art. 259 CP RM.[739]

Examinarea opiniilor exprimate de către teoreticienii din alte state, citate mai sus, arată că unii dintre aceștia identifică un singur obiect juridic special al infracțiunilor prevăzute de articolele corespondente cu art. 259 CP RM. Alți autori evidențiază două obiecte ale acestor infracțiuni: 1) obiectul juridic principal; 2) obiectul juridic secundar.

Într-adevăr, unele infracțiuni lezează nu un obiect juridic special, două două astfel de obiecte. În primul dintre aceste cazuri vorbim despre infracțiuni uniobiectuale, iar în ultimul caz infracțiunile sunt biobiectuale. În cazul infracțiunilor biobiectuale, distingem obiectul juridic principal și cel secundar. Principal este acel obiect juridic pe care legiuitorul, în procesul de creație normativă, dorește să-l ocrotească primordial împotriva faptei incriminate în norma corespunzătoare. Secundar este acel obiect juridic pe care legiuitorul, în procesul de creație normativă, dorește să-l protejeze adiacent, deoarece obiectul juridic secundar este lezat numai datorită lezării obiectului juridic principal.

Sarcina noastră este să stabilim dacă infracțiunile, ce sunt prevăzute la art. 259 CP RM, sunt uniobiectuale sau biobiectuale. Întru realizarea acestei sarcini, considerăm necesară analiza părerilor expuse în teoria dreptului penal al Republicii Moldova.

---

[736] ИСМАГУЛОВА, А.Т., ГАЛИАСКАРОВА, А.М. *Уголовные правонарушения в сфере информатизации и связи в Республике Казахстан*. Костанай: New Line Media, 2016, с. 64. 160 с. ISBN 978-601-7798-10-9.
[737] Ibidem, с. 64.
[738] *Комментарий к Уголовному кодексу Республики Казахстан* / Под ред. И.Ш. БОРЧАШВИЛИ. Алматы: Жеті жарғы, 2007, с. 510. 992 с. ISBN 9965-11-261-4.
[739] STRÎMBEANU, Alexandru. Obiectul juridic special al infracțiunilor de acces ilegal la informația computerizată (art. 259 din Codul penal al Republicii Moldova): premise conceptuale. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313468

Unii autori autohtoni nu recunosc în mod tranșant caracterul bivalent al obiectului juridic special al infracțiunilor analizate. Astfel, M. Gheorghiță consideră că infracțiunile, prevăzute la art. 259 CP RM, lezează acele relații sociale „care apar în procesul colectării, prelucrării, păstrării și prezentării informației computerizate și a resurselor informaționale”[740]; „În urma accesului ilegal la informația computerizată protejată de lege, pot fi cauzate prejudicii considerabile intereselor legale ale personalității, societății sau statului [...].”[741] În ceea ce privește ultima propoziție precitată, nu este clar în care context pot fi prejudiciate interesele nominalizate: în contextul obiectului juridic principal sau al obiectului juridic secundar? În aceeași privință, păreri echivoce exprimă A. Borodac[742] și N. Lazareva.[743]

Dimpotrivă, alți autori recunosc în mod tranșant caracterul bivalent al obiectului juridic special al infracțiunilor ce sunt prevăzute de art. 259 CP RM.[744] Aceste păreri coincid sub aspectul atestării bivalenței obiectului juridic special al infracțiunilor ce sunt prevăzute de art. 259 CP RM. Însă, aceste păreri diferă între ele într-o măsură mai pronunțată sau mai redusă în ceea ce privește conținutul obiectului juridic principal și al obiectului juridic secundar ale infracțiunilor examinate.

Această lipsă de uniformitate a opiniilor doctrinare ne determină să ne asumăm, pe lângă sarcina de a stabili numărul de obiecte juridice speciale ale infracțiunilor prevăzute la art. 259 CP RM, o altă sarcină. Ne referim la identificarea conținutului pe care îl pot avea obiectul juridic principal și obiectul juridic secundar ale acestor infracțiuni, în ipoteza în care infracțiunile prevăzute la art. 259 CP RM se vor dovedi a fi biobiectuale.

Despre criteriul de stabilire a conținutului, pe care-l are obiectul juridic special al infracțiunii, menționează E.V. Bocearov și I.V. Șulga: „Conținutul obiectului juridic special este dezvăluit în

---

[740] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 568. 836 p. ISBN 9975-61-291-1.

[741] Ibidem, p. 568.

[742] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 362. 622 p. ISBN 9975-9788-7-8.

[743] ЛАЗАРЕВА, Наталья. Проблемы квалификации преступлении в области информатики и электросвязи. În: *Закон и жизнь*, 2007, № 12, с. 49-56. ISSN 1810-309X.

[744] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 567. 860 p. ISBN 978-9975-105-20-0; ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 13. 592 с. ISBN 978-9975-4158-2-8; BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chişinău: Cartier, 2005, p. 495. 804 p. ISBN 9975-79-324-X; STATI, Vitalie. Răspunderea penală pentru infracţiunile în domeniul informaticii şi telecomunicaţiilor. În: Analele Ştiinţifice ale Universităţii de Stat din Moldova. Seria „Ştiinţe socioumanistice”. Vol. 1. Chişinău: CEP USM, 2005, pp. 387-394. ISSN 1811-2668; BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011, p. 259. 1324 p. ISBN 978-9975-53-028-7; BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 347. 1300 p. ISBN 978-9975-53-470-3; POALELUNGI, Mihai et al. *Manualul judecătorului pentru cauze penale*. Chișinău: Tipografia Centrală, 2013, p. 703. 1192 p. ISBN 978-9975-53-231-0.

titlurile articolelor incluse în anumite capitole din Codul penal”.[745] Considerăm că titlurile articolelor, incluse în partea specială a Codului penal, nu întotdeauna sunt suficient de informative pentru a elucida caracteristicile obiectului juridic special al faptei infracționale. Scopul titlului de articol, inclus în partea specială a Codului penal (a denumirii marginale a infracțiunii), este de a facilita identificarea componenței unei infracțiuni în textul Codului penal. Din aceste considerente mai pertinentă este părerea lui Iu. Leapunov și V. Maksimov: „Obiectul juridic special se stabilește pe baza titlurilor și dispozițiilor unor articole concrete”.[746] Așadar, interpretarea titlului de articol, inclus în partea specială a Codului penal, trebuie să fie secundată de interpretarea dispoziției acelui articol, pentru a se putea revela conținutul obiectului juridic special al infracțiunii. În calitate de criteriu suplimentar ar putea apărea luarea în considerare a conținutului obiectului juridic generic al infracțiunii. Or, obiectul juridic special al infracțiunii trebuie să derive din obiectul juridic generic al infracțiunii. Cu alte cuvinte, juridic special al infracțiunii reprezintă necesarmente o parte a obiectului juridic generic al infracțiunii, care este un întreg.

Să nu uităm că în art. 259 CP RM este prevăzută răspunderea pentru două infracțiuni. Așa cum menționează pe bună dreptate S. Brînza și V. Stati, sub auspiciul art. 259 CP RM, „sunt reunite două variante-tip de infracțiuni şi o singură variantă agravată de infracțiune”.[747] Aceiași autori afirmă: „La alin. (1) și lit. h) alin. (2) art. 259 CP RM, sunt prevăzute două infracțiuni de sine stătătoare. [...]”.[748]; „Explicația faptului că art. 259 CP RM stabilește răspunderea pentru două infracțiuni de sine stătătoare constă în următoarele: nu există o componență „de bază” de acces ilegal la informaţia computerizată”[749], „componență care: 1) nu ar presupune producerea unor daune având o mărime concretă și 2) pe care s-ar grefa în calitate de circumstanțe agravante”[750]: „a) producerea unor daune în proporţii mari; b) producerea unor daune în proporţii deosebit de mari.”[751] „Iată de ce cauzarea de daune în proporţii deosebit de mari nu poate fi privită în calitate de circumstanță agravantă pentru infracțiunea prevăzută la alin. (1) art. 259 CP RM, infracțiune care presupune producerea unor daune în proporții mari”.[752] „În alți termeni, cauzarea de daune în proporții deosebit de mari nu poate fi privită ca apendice, ca adaos, ca

[745] БОЧАРОВ, Е.В., ШУЛЬГА, И.В. *Уголовное право Российской Федерации*. Владивосток: ВГУЭС, 2015, с. 7. 44 с. ISBN 978-5-9273-2385-2.
[746] ЛЯПУНОВ, Ю., МАКСИМОВ, В. Ответственность за компьютерные преступления. În: *Законность*, 1997, № 1, с. 8-15. ISSN 0869-4486.
[747] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 346. 1300 p. ISBN 978-9975-53-470-3.
[748] Ibidem, p. 346.
[749] Ibidem, p. 346.
[750] Ibidem, p. 346.
[751] Ibidem, p. 346.
[752] Ibidem, p. 346.

supliment, ca anexă la componența de infracțiune specificată la alin. (1) art. 259 CP RM, care deja presupune cauzarea de daune în proporții mari."[753]

Susținem aceste argumente și, de aceea, considerăm că, pentru fiecare dintre cele două infracțiuni prevăzute la art. 259 CP RM, trebuie stabilit obiectul juridic special. Odată ce aceste infracțiuni diferă în anumite privințe, nu este posibil ca ele să aibă același obiect juridic special.

În partea specială a Codului penal al Republicii Moldova, componențele de infracțiuni sunt grupate în capitole, în dependență de obiectul juridic generic. Așadar, obiectul juridic generic reprezintă factorul unificator pentru un grup de infracțiuni prevăzute de un capitol anumit al părții speciale a Codului penal al Republicii Moldova. Pe cale de deducție, putem menționa că, în cadrul unui capitol al părții speciale a Codului penal al Republicii Moldova, componențele de infracțiuni sunt individualizate în dependență de obiectul juridic special. Tocmai obiectul juridic special reprezintă factorul ce particularizează o infracțiune anumită în raport cu o altă infracțiune.

Obiectul juridic special al infracțiunii îl formează acea valoare socială și acele relații sociale aferente care sunt întotdeauna vătămate sau puse în pericol de vătămare în rezultatul săvârșirii unei infracțiuni. În cazul infracțiunilor ce sunt specificate în alin. (1) și lit. h) alin. (2) art. 259 CP RM, proporțiile daunelor cauzate reprezintă factorul ce le particularizează una în raport cu cealaltă. Mărimea categorisită legalmente a acestor proporții – mare sau deosebit de mare – determină gradul de gravitate a pericolului care amenință obiectul juridic special al faptelor infracționale analizate. Din această cauză, valoarea socială și relațiile sociale aferente afectate în rezultatul comiterii infracțiunii care este prevăzută de alin. (1) art. 259 CP RM, presupunând cauzarea de daune în proporții mari, nu pot să coincidă cu valoarea socială și relațiile sociale alăturate, ce sunt afectate în rezultatul săvârșirii infracțiunii care este prevăzută la lit. h) alin. (2) art. 259 CP RM. Or, în cazul acestei din urmă infracțiuni se cauzează daune în proporții deosebit de mari.

După cum s-a relevat mai sus, regula este că obiectul juridic special decurge, rezultă, se desprinde din obiectul juridic generic. Informatica și telecomunicațiile reprezintă perechea de valori sociale fundamentale, care sunt protejate contra infracțiunilor prevăzute în Capitolul XI al părții speciale a Codului penal al Republicii Moldova. Ceea ce înseamnă că obiectul juridic special al infracțiunilor, prevăzute la art. 259 CP RM, trebuie să decurgă din relaţiile sociale din domeniul informaticii şi al telecomunicaţiilor.

[753] Ibidem, p. 346.

Particularizând, este necesar să constatăm că denumirea art. 259 CP RM – „Accesul ilegal la informaţia computerizată” – sugerează că informatica este domeniul de relații sociale de care aparține obiectul juridic special al infracțiunilor, care sunt prevăzute de art. 259 CP RM. Această ipoteză este valabilă cu condiția că infracțiunile analizate sunt uniobiectuale. În ipoteza în care ele sunt biobiectuale, obiectul juridic principal trebuie este cel care se desprinde din relațiile sociale din domeniul informaticii.

Considerăm că infracțiunile, ce sunt prevăzute de art. 259 CP RM, sunt biobiectuale. Despre aceasta ne vorbește structura faptei prejudiciabile prevăzute de acest articol. Astfel, fapta prejudiciabilă analizată include două componente: 1) acţiunea principală de acces ilegal la informaţia computerizată; 2) acţiunea adiacentă de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice.

Astfel, acţiunea principală aduce atingere obiectului juridic principal al infracțiunilor prevăzute la art. 259 CP RM, pe când acţiunea adiacentă aduce atingere obiectului juridic secundar al acestor infracțiuni.

Cât privește obiectul juridic principal, acesta urmează a fi stabilit pe baza interpretării titlului art. 259 CP RM, precum și a acelei părți din dispoziția alin. (1) art. 259 CP RM în care este descrisă acțiunea principală: „accesul ilegal la informaţia computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică [...].”[754] Din interpretarea acestor elemente ale art. 259 CP RM se poate deduce că, incriminând faptele reunite sub denumirea marginală de acces ilegal la informaţia computerizată, legiuitorul urmărește să stabilească un echilibru rezonabil între dreptul unor persoane de a accesa în mod liber informația computerizată și dreptul altor persoane de a nu permite accesul ilegal la o asemenea informație. Conform art. 55 din Constituția Republicii Moldova, „orice persoană îşi exercită drepturile şi libertăţile constituţionale cu bună-credinţă, fără să încalce drepturile şi libertăţile altora”.[755] Dreptul la informație este un drept prevăzut de art. 34 din Constituție. Dreptul de a accesa în mod liber informația computerizată nu este decât o versiune a acestui drept constituțional. Din alin. (2) art. 54 al Constituției reiese că dreptul la informație poate fi restrâns. Important este ca această restrângere: 1) „să fie prevăzută de lege”[756]; 2) „să corespundă normelor unanim recunoscute ale dreptului internaţional”[757]; 3) „să fie necesară în interesele

[754] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[755] Constituția Republicii Moldova. În: *Monitorul Oficial al Republicii Moldova*, 1994, nr. 1, 140.
[756] Ibidem.
[757] Ibidem.

securităţii naţionale, integrităţii teritoriale, bunăstării economice a ţării, ordinii publice, în scopul prevenirii tulburărilor în masă şi infracţiunilor”[758], „protejării drepturilor, libertăţilor şi demnităţii altor persoane, împiedicării divulgării informaţiilor confidenţiale sau garantării autorităţii şi imparţialităţii justiţiei”.[759]

Restrângerea dreptului de a accesa în mod liber informația computerizată, prevăzută de art. 259 CP RM, îndeplinește aceste trei condiții. Această restrângere se bazează pe lege și are drept scop protejarea interesului legitim al unei persoane, al societății sau al statului. Aceasta rezultă din descrierea subiectului infracțiunii, care se face în alin. (1) art. 259 CP RM: „persoană care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea persoanei competente”[760] „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.”[761].[762]

În aparență, obiectul juridic principal al infracțiunilor prevăzute la art. 259 CP RM l-ar constitui relaţiile sociale cu privire la accesul autorizat sau permis la informaţia computerizată, apărate împotriva cauzării de: 1) daune în proporții mari în rezultatul accesului ilegal la informaţia computerizată (în cazul infracțiunii prevăzute la alin. (1)); 2) daune în proporții deosebit de mari în rezultatul accesului ilegal la informaţia computerizată (în cazul infracțiunii prevăzute la lit. h) alin. (2)).

Însă, această ipoteză nu este validă decât în parte. Explicația constă în faptul că „accesul ilegal la informaţia computerizată nu poate să antreneze de sine stătător producerea urmărilor prejudiciabile”[763]; „Iată de ce, acţiunea principală se poate afla în legătură cauzală cu urmările prejudiciabile numai dacă este însoţită de acţiunea adiacentă.”[764] Sprijinim această opinie a lui S. Brînza și V. Stati. Din ea rezultă că urmările prejudiciabile, descrise în alin. (1) și lit. h) alin. (2) art. 259 CP RM, se află într-o legătură de cauzalitate directă nu cu acțiunea principală din componența faptei prejudiciabile specificate în aceste norme, ci cu acțiunea adiacentă din cadrul faptei respective. De bună seamă, daunele în proporții mari sau deosebit de mari se produc nu în rezultatul accesului ilegal la informaţia computerizată, ci în rezultatul distrugerii, deteriorării,

---

[758] Ibidem.
[759] Ibidem.
[760] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[761] Ibidem.
[762] STRÎMBEANU, Alexandru. Obiectul juridic special al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): reflecții, abordări și soluții. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313472
[763] BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011, p. 268. 1324 p. ISBN 978-9975-53-028-7.
[764] Ibidem, p. 268.

modificării, blocării sau copierii informaţiei computerizate ori al dereglării funcţionării calculatoarelor, a sistemului sau a reţelei informatice.

Pe cale de consecință, obiectul juridic principal al infracțiunilor ce sunt specificate în art. 259 CP RM îl formează relaţiile sociale cu privire la accesul permis sau autorizat la informaţia computerizată. Acest obiect este același pentru ambele infracțiuni specificate în art. 259 CP RM.

După ce am stabilit conținutul obiectului juridic principal al infracțiunilor specificate la art. 259 CP RM, se impune să identificăm conținutul obiectului juridic secundar al acestor infracțiuni.

După părerea lui A.N. Popov și L.S. Aistova, „obiectul juridic secundar al infracțiunii [...] este întotdeauna reliefat în dispoziția normei de incriminare”.[765] Această teză este infirmată de conținutul dispoziției de la alin. (1) art. 259 CP RM. În această dispoziție nu este relevat în mod expres obiectul juridic secundar al infracțiunilor prevăzute de acest articol. În schimb, în dispoziția de la alin. (1) art. 259 CP RM este descrisă acţiunea adiacentă: „distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice.”[766]

Așa cum am afirmat mai sus, acţiunea adiacentă, descrisă în art. 259 CP RM, aduce atingere obiectului juridic secundar al faptelor infracționale ce sunt prevăzute de acest articol. Concretizând, suntem de părerea că: distrugerea sau deteriorarea informaţiei computerizate aduce atingere integrității acesteia; modificarea informaţiei computerizate aduce atingere autenticității acesteia; blocarea informaţiei computerizate aduce atingere disponibilității acesteia; copierea informaţiei computerizate aduce atingere ireproductibilității acesteia; dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice aduce atingere funcționalității acestora.

I.I. Ciugunikov menționează: „Relațiile sociale protejate printr-o normă penală obțin calitatea de obiect juridic secundar atunci când atingerea adusă acestora reprezintă o infracțiune.”[767] Considerăm prea categorică această afirmație. În cazul infracțiunilor prevăzute la art. 259 CP RM, daunele în proporții mari sau deosebit de mari se produc nu în rezultatul comiterii acțiunii principale, ci în rezultatul săvârșirii acțiunii adiacente. Aceasta determină necesitatea stabilirii unui obiect juridic special pentru fiecare dintre cele două acțiuni care alcătuiesc fapta

[765] ПОПОВ, А.Н., АИСТОВА, Л.С. *Объект преступления*. Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации, 2014, с. 16. 40 с.

[766] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

[767] ЧУГУНІКОВ, І.І. Додатковий об’єкт злочину: проблема визначення та класифікації. În: *Правове життя сучасної України: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.)*. Одеса: Гельветика, 2020, Т. 3, с. 151-155. ISBN 978-966-992-106-2.

prejudiciabilă prevăzută la art. 259 CP RM. Fără îndoială, infracțiunile, prevăzute la art. 259 CP RM, sunt infracțiuni biobiectuale. Ele sunt biobiectuale, deoarece așa le-a conceput legiuitorul.

Următoarea sarcină, pe care ne-o asumăm, este să stabilim dacă structura bivalentă a obiectului juridic special al infracțiunilor, prevăzute la art. 259 CP RM, condiționează caracterul complex al acestora.

În cazul infracțiunilor ce sunt specificate în art. 259 CP RM, nici acțiunea principală, nici acțiunea adiacentă nu reprezintă de felul lor infracțiuni. În partea specială a Codului penal al Republicii Moldova nu există norme în care ar fi incriminate distinct fie accesul ilegal la informaţia computerizată, fie distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei ori dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice.

S.N. Romaniuk afirmă: „Pentru a fi considerată infracțiune unică complexă, o faptă trebuie să includă câteva acțiuni alcătuitoare, dintre care este necesar ca doar una să reprezinte o infracțiune de sine stătătoare”[768], „dacă ar fi privită în afara contextului infracțiunii unice complexe.”[769] Ideea lui S.N. Romaniuk își găsește confirmarea în alin. (2) art. 35 CPR. Potrivit acestei norme, „infracțiunea este complexă când în conținutul său intră [...] *o acțiune sau o inacțiune care constituie prin ea însăși o faptă prevăzută de legea penală* (evid. ns.)”[770].[771] Din definiția, formulată în această normă, rezultă că este suficient ca o singură componentă a infracțiunii unice complexe să reprezinte o faptă cu relevanță penală, care, în afara contextului infracțiunii unice complexe, ar reprezenta o infracțiune distinctă. Această poziție a legiuitorului român nu este tăgăduită de legiuitorul moldovean. Astfel, art. 28 CP RM prevede: „Infracţiunea unică reprezintă o acţiune (inacţiune) sau un sistem de acţiuni (inacţiuni) care se califică conform dispoziţiei unei singure norme a legii penale.”[772] Din această dispoziție nu reiese în niciun mod că, în cazul în care infracţiunea unică reprezintă un sistem de acţiuni (inacţiuni), toate aceste acțiuni (inacțiuni) trebuie să fie prevăzute de norme ale legii penale.

Concluzia noastră este următoarea: noțiunea de infracțiune biobiectuală se intersectează cu noțiunea de infracțiune complexă, fără însă a se echivala cu această noțiune. De aceea, infracțiunea biobiectuală, ca și infracțiunea complexă, reprezintă tipuri distincte de infracțiuni unice. Infracțiunile, prevăzute la art. 259 CP RM, sunt infracțiuni biobiectuale, însă nu sunt infracțiuni complexe.

---

[768] РОМАНЮК, С.Н. *Сложные единичные преступления*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Тюмень, 2008, с. 11. 22 с.
[769] Ibidem, с. 11.
[770] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[771] În legea penală autohtonă lipsește o normă corespondentă.
[772] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

2.1.2. Obiectul material (imaterial) al infracțiunilor prevăzute la art. 259 CP RM

În unele cazuri, valorile și relațiile sociale, apărate de legea penală, sunt lezate nu în mod direct, ci prin intermediul unor entități – cu caracter material sau imaterial – care reprezintă obiectul material sau imaterial al infracțiunii. În ipoteza unor infracțiuni (de exemplu, a celor prevăzute la art. 145-150, 151, 152 etc. din Codul penal), este obligatorie prezența obiectului material. În cazul altor infracțiuni (de exemplu, a celor prevăzute la art. 177, 180, 204, 208^2, 219 etc. din Codul penal), este obligatorie prezența obiectului imaterial. În fine, în situația infracțiunilor prevăzute la art. 136, 165, 165^1, 189, 194, 213^1 etc. din Codul penal, atestăm prezența fie a obiectului material, fie a obiectului imaterial.[773]

În studiul de față este necesar să stabilim dacă valorile și relațiile sociale, apărate de art. 259 CP RM, sunt lezate prin intermediul unor entități: cu caracter exclusiv material; cu caracter exclusiv imaterial; cu caracter material sau imaterial.

În legătură cu infracțiunile prevăzute la art. 259 CP RM, M. Gheorghiță menționează: „Pentru calificarea infracțiunii menționate este necesar de a determina corect obiectul acesteia”[774]; „În limitele componenței analizate, în calitate de obiect nemijlocit al infracțiunii se prezintă tehnica electronică de calcul drept complex de mijloace informaționale, purtător de informații”[775]; „Informația pură nu prezintă o particularitate fizică și, prin urmare, nu poate să figureze în calitate de obiect al infracțiunii.”[776] În continuare, în legătură cu aceleași infracțiuni, M. Gheorghiță afirmă: „În calitate de obiect al săvârșirii infracțiunii examinate se prezintă tehnica computerizată, adică diferite tipuri de mașini electronice de calcul, aparatura de calcul [...][777], „precum și diferite mijloace de telecomunicații, cu ajutorul cărora tehnica de calcul se conectează la rețelele informaționale [...]”.[778] Folosind formulări ca „obiectul infracțiunii”, „obiectul nemijlocit al infracțiunii” și „obiect al săvârșirii infracțiunii”, autorul precitat are în vedere, de fapt, entitatea prin intermediul căreia se aduce atingere obiectului juridic special al faptelor infracționale ce sunt specificate în art. 259 CP RM. Totodată, putem observa că, în

---

[773] STRÎMBEANU, Alexandru. Anumite aspecte ale obiectului material (imaterial) al infracțiunilor prevăzute la art. 259 CP RM. În: *Conferinţa ştiinţifică internaţională „Infracţiunea – Răspunderea penală – Pedeapsa. Drept şi Criminologie”, Ediţia a 2-a (24-25 martie 2022, Chişinău): Culegere de comunicări*. Chişinău: CEP USM, 2022, pp. 231-242. ISBN 978-9975-62-476-3.

[774] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 568. 836 p. ISBN 9975-61-291-1.

[775] Ibidem, p. 568.

[776] Ibidem, p. 568.

[777] Ibidem, p. 569.

[778] Ibidem, p. 569.

opinia lui M. Gheorgiță, informația nu este privită ca obiect material al faptelor infracționale în cauză.

Pe de altă parte, N. Lazareva consideră că obiectul material al faptelor infracționale, care sunt prevăzute de art. 259 CP RM, îl reprezintă „informația computerizată”.[779] Trebuie să precizăm că N. Lazareva utilizează sintagma «предмет преступления» atunci când relatează despre entitatea prin intermediul căreia se aduce atingere obiectului juridic special al infracțiunilor ce sunt specificate în art. 259 CP RM. În mod obișnuit, această sintagmă desemnează entitatea materială prin intermediul căreia se aduce atingere obiectului juridic special al unei infracțiuni. În limba rusă nu există un echivalent al sintagmei „obiectul imaterial al infracțiunii”. Drept urmare, nu excludem ca sintagma «предмет преступления» să se refere în anumite cazuri la entitatea imaterială prin intermediul căreia se aduce atingere obiectului juridic special al unei infracțiuni. De exemplu, V.V. Vorobiov consideră că „obiectul material al infracțiunii («предмет преступления») include obiecte atât din lumea materială, cât și din lumea imaterială (de exemplu, informația)”.[780]

Totuși, chiar unii doctrinari români folosesc sintagma „obiectul material al infracțiunii” pentru a se referi, printre altele, la entitatea imaterială prin intermediul căreia se aduce atingere obiectului juridic special al unei infracțiuni. Astfel, M. Dobrinoiu consideră că „obiectul material al infracţiunilor, prevăzute la art. 42[781] al Legii României nr. 161/2003[782], îl reprezintă „entităţile materiale care compun sistemele informatice [...] şi [...] datele informatice spre care se îndreaptă atenţia făptuitorului.”[783] O părere asemănătoare o exprimă C. Duvac.[784]

La baza unor asemenea puncte de vedere este pusă concepția, conform căreia, indiferent de caracterul – material sau imaterial – al entității prin intermediul căreia se aduce atingere obiectului juridic special al infracțiunii, această entitate trebuie denumită „obiect material al infracțiunii”. De exemplu, D. Vasiloi susține: „Nimic nu împiedică analizarea obiectului material

---

[779] ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista ştiinţifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.

[780] ВОРОБЬЁВ, В.В. О предмете преступления, его месте в составе преступления и особенностях в компьютерных преступлениях. În: *Символ науки*, 2015, № 6, с. 221-223. ISSN 2410-700X.

[781] Acest articol a fost abrogat prin Legea României nr. 187 din 24 octombrie 2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal.*

* *Monitorul Oficial al României*, 2012, nr. 757.

[782] Se are în vedere Legea României nr. 161 din 19.04.2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei.*

* *Monitorul Oficial al României*, 2003, nr. 279.

[783] DOBRINOIU, Maxim. *Infracţiuni în domeniul informatic*. Bucureşti: C.H. Beck, 2006, p. 148. 401 p. ISBN 978-973-655-941-9.

[784] DUVAC, Constantin. Accesul ilegal la un sistem informatic în reglementarea noului Cod penal. În: *Revista română de dreptul proprietăţii intelectuale*, 2012, nr. 1, pp. 88-109. ISSN 1584-7241.

prin prisma unor elemente incorporale/intangibile”[785]; „Astfel, chiar dacă însuși numele de obiect material ar arăta la prima vedere că în conținutul acestuia nu pot intra elemente incorporale”[786], „considerăm că acest fapt nu prezintă un real impediment în vederea acceptării tezei menționate anterior.”[787] În mod similar, P.P. Andrușko și M.P. Bikmurzin propun ca noțiunea „obiectul material al infracțiunii” să fie extinsă asupra unor entități de natură imaterială.[788]

Pe marginea acestor păreri este util să fie reprodus punctul de vedere al lui A. Reșetnicov: „Trebuie de menţionat că în doctrina penală există o tendinţă de a opera cu un concept eclectic, care desemnează generic atât obiectul material al infracţiunii, cât şi obiectul imaterial al infracţiunii”[789]; „În principiu, concepţia dată ar putea fi susţinută, dacă nu ar fi existat un impediment major: promotorii concepţiei date desemnează conceptul eclectic respectiv prin sintagma „obiectul material al infracţiunii”.”[790]; „ Cu alte cuvinte, ei identifică partea cu întregul. Ceea ce este inacceptabil sub aspect logic”.[791] Totuși, același autor caracterizează deopotrivă obiectul material al infracțiunii și obiectul imaterial al infracțiunii, fără a le distinge: „Este entitatea capabilă să satisfacă necesităţile subiectelor relaţiei sociale. Însă, aceste subiecte sunt împiedicate să-şi satisfacă necesităţile, deoarece intervine subiectul infracţiunii”[792]; „Ca şi cum substituindu-se subiectelor relaţiei sociale, el intenţionează să-şi satisfacă, pe seama lor, necesităţile pe care le implică entitatea materială (imaterială) corespunzătoare”[793]; „Săvârşind infracţiunea, subiectul [...] face să nu-şi găsească valorificare facultăţile [...] de a avea conduita pe care şi-o dorește cu privire la entitatea materială (imaterială), ce trebuia să-i satisfacă necesităţile.”[794]

Conceptul eclectic, despre care vorbește A. Reșetnicov, nu poate să reflecte pe deplin adevărul. Or, acest concept cuprinde nu numai entitățile din lumea materială, ci și informația, energia, obiectele de proprietate intelectuală, serviciile, avantajele, alte foloase de natură imaterială etc. O astfel de abordare nu ia în considerare clasificarea bunurilor în cele corporale

---

[785] VASILOI, Djulieta. Unele raționamente ale noțiunii de „obiect imaterial” al infracțiunii. În: *Legea și viața*, 2020, nr. 8-9, pp. 39-41. ISSN 1810-309X.
[786] Ibidem.
[787] Ibidem.
[788] АНДРУШКО, П.П. *Кримінально-правова охорона прав інтелектуальної власності в Україні*. Київ: Форум, 2004, с. 35. 160 с. ISBN 966-95843-8-8; БИКМУРЗИН, М.П. *Предмет преступления: теоретико-правовой анализ*. Москва: Юрлитинформ, 2006, с. 160. 184 с. ISBN 5-93295-226-1.
[789] REŞETNICOV, Artur. Obiectul material al infracţiunii şi obiectul imaterial al infracţiunii: necesitatea delimitării. În: *Revista Națională de Drept*, 2007, nr. 9, pp. 25-30. ISSN 2587-411X.
[790] Ibidem.
[791] Ibidem.
[792] Ibidem.
[793] Ibidem.
[794] Ibidem.

(„res corporales”) și cele incorporale *(„res incorporales”)*, cunoscută încă din timpul dreptului privat roman. În context, G.-I. Luncan susține că „bunurile incorporale [...] nu au o existență materială, palpabilă, regăsindu-se în exclusivitate în ordinea juridică, nu și în ordinea naturală.”[795]

Despre bunurile incorporale se vorbește în art. 132^1 CP RM. Mențiuni despre bunurile incorporale găsim în Codul civil (art. 476, 605, 676, 744, 1384, 2611)[796]. În Hotărârea Guvernului nr. 857 din 31.10.2013 cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”, este utilizată sintagma „patrimoniu imaterial”.[797] Sintagmele „active imateriale” și „obiecte imateriale” sunt folosite în Hotărârea Guvernului nr. 880 din 22.11.2012 cu privire la Strategia naţională în domeniul proprietăţii intelectuale până în anul 2020.[798] Aceasta demonstrează că legislația Republicii Moldova conține toate premisele necesare pentru a face distincția dintre obiectul material al infracțiunii și obiectul imaterial al infracțiunii.

Sintagma „obiectul imaterial al infracțiunii” este utilizată în actele instanței de contencios constituțional, și anume în: pct. 31 din Decizia Curții Constituționale a Republicii Moldova nr. 109 din 07.11.2017 de inadmisibilitate a sesizării nr. 138g/2017 privind excepţia de neconstituţionalitate a unor prevederi din articolul 243 alineatul (1) literele a) și c) din Codul penal al Republicii Moldova nr. 985-XV din 18 aprilie 2002 (spălarea banilor)[799]; pct. 37 din Decizia Curții Constituționale a Republicii Moldova nr. 36 din 19.04.2018 de inadmisibilitate a sesizărilor nr. 173g/2017 și nr. 37g/2018 privind excepţia de neconstituţionalitate a articolului 220 din Codul penal și a articolului 89 din Codul contravențional (proxenetismul și practicarea prostituției)[800], etc.

---

[795] LUNCAN, Gabriel-Ilie. *Corporalitatea bunurilor și calitatea de bun a unui lucru*. [citat 06.03.2022] Disponibil: https://www.juridice.ro/701050/corporalitatea-bunurilor-si-calitatea-de-bun-a-unui-lucru.html

[796] De asemenea, în art. 477 din Codul civil prezintă interes noțiunile „conținut digital” și „bun digital: „(1) Conținut digital se consideră datele produse și livrate în formă digitală, cum sunt programele de calculator, aplicațiile, jocurile, muzica, înregistrările video sau textele”*, „indiferent dacă sunt accesate prin descărcare sau prin flux continuu, de pe un suport material sau prin orice alte mijloace.”*; „[...] (3) Bun digital al unei persoane se consideră: a) conținutul digital la care ea are dreptul; b) contul la o poștă electronică, la o rețea sau alt cont online, la care ea are dreptul”.*

* Codul civil al Republicii Moldova: nr. 1107 din 06.06.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 82-86, 661.

[797] Hotărârea Guvernului cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”: nr. 857 din 31.10.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 252-257, 963.

[798] Hotărârea Guvernului cu privire la Strategia naţională în domeniul proprietăţii intelectuale până în anul 2020: nr. 880 din 22.11.2012. În: *Monitorul Oficial al Republicii Moldova*, 2012, nr. 245-247, 951.

[799] Decizia Curții Constituționale a Republicii Moldova de inadmisibilitate a sesizării nr. 138g/2017 privind excepţia de neconstituţionalitate a unor prevederi din articolul 243 alineatul (1) literele a) și c) din Codul penal al Republicii Moldova nr. 985-XV din 18 aprilie 2002 (spălarea banilor): nr. 109 din 07.11.2017. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 58-66, 34.

[800] Decizia Curții Constituționale a Republicii Moldova de inadmisibilitate a sesizărilor nr. 173g/2017 și nr. 37g/2018 privind excepţia de neconstituţionalitate a articolului 220 din Codul penal și a articolului 89 din Codul

Nu putem ignora nici faptul că noțiunea „obiectul imaterial al infracțiunii” este utilizată pe larg în doctrina penală a Republicii Moldova.[801]

V. Stati formulează definiția noțiunii „obiectul imaterial al infracțiunii”: „entitatea incorporală asupra căreia se îndreaptă nemijlocit acțiunea infracțională, prin al cărei intermediu se aduce atingere obiectului juridic al infracțiunii”.[802] Cu referire la entitățile imateriale, prin al căror intermediu se aduce atingere obiectului juridic al infracțiunii, G. Zlati folosește noțiunea „bun virtual”.[803] Este nelipsită de interes și constatarea făcută de N.D. Popa, potrivit căreia recurgerea la noțiunea „obiect material” „pentru a desemna entitățile imateriale nu este cea mai bună soluție, deoarece respectivele entități redau o realitate de altă natură decât cea materială, tangibilă”.[804]

În legătură cu infracțiunile ce sunt prevăzute de art. 259 CP RM, S. Brînza și V. Stati afirmă: „Obiectul material sau, după caz, imaterial al infracţiunii în cauză este constituit din: informaţia computerizată; calculatoare; sistemul informatic; reţeaua informatică”.[805] Un punct de vedere similar este exprimat de către L. Dumneanu și D. Gurev.[806]

---

contravențional (proxenetismul și practicarea prostituției): nr. 36 din 19.04.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 195-209, 104.

[801] A se vedea, de exemplu: MOȚOC, Costică, GÎRLA, Lilia. Secretul profesional reproductiv ca obiect imaterial al încălcării inviolabilității vieții personale: constatări *de lege lata*, viziuni doctrinare și jurisprudența CtEDO. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2019, nr. 11, pp. 146-159. ISSN 1814-3199; BOTNARENCO, Dorin. Unele reflecții privind noțiunea „contrară legii” din dispoziția art. 307 CP RM. În: *Conferință științifică națională cu participare internațională „Integrare prin cercetare și inovare”. Științe juridice și economice. Rezumate ale comunicărilor. Vol. I*. Chișinău: CEP USM, 2020, pp. 144-148. ISBN 978-9975-152-48-8; BRÎNZA, Serghei, MAREȘ, Mihai. Îmbogățirea ilicită – o analiză comparativă a legislațiilor din Republica Moldova și din România. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2020, nr. 8, pp. 3-16. ISSN 1814-3199; BRÎNZA, Serghei. Justificarea publică a sinuciderii: caracteristici definitorii. În: *Conferință științifică națională cu participare internațională „Integrare prin cercetare și inovare”. Științe juridice și economice. Rezumate ale comunicărilor. Vol. I*. Chișinău: CEP USM, 2020, pp. 9-12. ISBN 978-9975-152-48-8; BRÎNZA, Cristian. Categoriile obiectului material sau imaterial al infracțiunilor de luare de mită și de dare de mită. În: *Conferinţa ştiinţifică naţională cu participare internaţională „Infracţiunea – Răspunderea penală – Pedeapsa. Drept şi Criminologie”, 25-26 martie 2021*. Chişinău: CEP USM, 2021, pp. 308-318. ISBN 978-9975-158-12-1; BRÎNZA, Cristian. Obiectul material sau imaterial al infracțiunilor de luare de mită și de dare de mită: considerații introductive. În: Conferinţa ştiinţifică naţională cu participare internaţională „Infracţiunea – Răspunderea penală – Pedeapsa. Drept şi Criminologie”, 25-26 martie 2021. Chişinău: CEP USM, 2021, pp. 300-307. ISBN 978-9975-158-12-1; PÎRȚAC, Cristina. Studiu comparat privind obiectul infracţiunilor de fals în acte publice (art. 332 CP RM). În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 3, pp. 185-197. ISSN 1814-3199.

[802] STATI, Vitalie. Problema obiectului material în cazul infracțiunii de încălcare a dreptului de autor și drepturilor conexe. În: *Probleme teoretice și practice ale economiei proprietății intelectuale*. Chișinău: AGEPI, 2007, pp. 228-230. ISBN 978-9975-911-02-03.

[803] ZLATI, George. Dematerializarea obiectului material al infracţiunii în contextul evoluţiei tehnologice şi consecinţele acesteia. În: *Dreptul*, 2013, nr. 9, pp. 163-180. ISSN 1811-0770.

[804] POPA, N.D. The concept of material object of the crime in the romanian criminal doctrine. In: *The Juridical Current Journal*, 2010, no. 3, pp. 118-130. ISSN 1224-9173.

[805] BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005, p. 495. 804 p. ISBN 9975-79-324-X; BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011, p. 259. 1324 p. ISBN 978-9975-53-028-7.

[806] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM, 2021, p. 89. 261 p. ISBN 978-9975-158-29-9.

O astfel de poziție este exprimată nu doar de teoreticienii din Republica Moldova. În legătură cu infracțiunea de acces ilegal la un sistem informatic, prevăzută de art. 360 CPR, A.T. Drăgan enunță următoarea opinie: „Obiectul material sau imaterial îl constituie sistemul informatic care este accesat fraudulos și care este reprezentat de entitățile materiale ce alcătuiesc un astfel de sistem [...]”[807], „precum și datele computerizate către care este îndreptată atenția făptuitorului”.[808] F.-V. Onofrei vorbește despre obiectul imaterial în contextul analizei infracțiunii prevăzute la art. 361 CPU[809] (care prezintă similitudini cu art. 259 CP RM).[810]

Asemenea abordări sunt mai reușite decât cea propusă de A.A. Grebenkov: „În cazul accesului ilegal la informațiile computerizate, aceste informații sunt într-adevăr apropiate, ca esență, de obiectul material al infracțiunii)”[811]; „Exercitând accesul ilegal, făptuitorul obține posibilitatea de a cunoaște conținutul informațiilor accesate și de a întreprinde anumite acțiuni asupra acestora. [...])”[812]; „Este însă oare cu adevărat necesară o astfel de „obiectivizare” a informațiilor în acest articol (se are în vedere art. 272 CP FR[813])? [...])”[814]; „Ar fi mai simplu să se recurgă la modificarea dispoziției art. 272 CP FR, după cum urmează: „Accesul ilegal la sistemul informatic, care are ca rezultat distrugerea, blocarea, modificarea sau copierea informațiilor computerizate”)”[815]; „Într-o asemenea formulare, informaţiile computerizate ar fi incluse în sistemul de referință al urmărilor prejudiciabile ale infracţiunii, iar obiectul material al infracțiunii va fi reprezentat de sistemul informatic [...]”.[816]

O astfel de concepție poate prezenta interes din perspectiva *de lege ferenda*, însă nu este compatibilă cu varianta *de lege lata* a art. 259 CP RM.[817]

---

[807] DRĂGAN, Alin Teodorus. Illegal access to a computer system from the standpoint of the current Criminal Code. În: *Journal of Legal Studies “Vasile Goldiş”*, 2019, nr. 23, pp. 33-43. ISSN 1582-5442.
[808] Ibidem.
[809] *Кримінальний кодекс України*. [citat 18.12.2020] Disponibil: https://zakon.rada.gov.ua/laws/show/2341-14#Text
[810] ONOFREI, Flavius-Vasile. Statutul juridic al informaţiei electronice în dreptul penal comparat. În: *Studia Universitatis Moldaviae. Seria „Ştiinţe Sociale”*, 2009, nr. 8, pp. 152-157. ISSN 1814-3199.
[811] ГРЕБЕНЬКОВ, А.А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава. În: *Lex Russica*, 2018, № 4, с. 108-120. ISSN 1729-5920.
[812] Ibidem.
[813] Ibidem.
[814] Ibidem.
[815] Ibidem.
[816] Ibidem.
[817] În context, trebuie să menționăm că, din Proiectul de lege pentru modificarea unor acte normative (modificarea Codului penal și Codului contravențional)*, publicat de Ministerul Justiției, rezultă că sistemul informatic va reprezenta singurul obiect material al infracțiunilor prevăzute la art. 259 CP RM.
* *Proiectul de lege pentru modificarea unor acte normative (modificarea Codului penal și Codului contravențional) (533/MJ/2022)*. [citat 30.12.2022] Disponibil: https://cancelaria.gov.md/ro/content/privind-aprobarea-proiectului-de-lege-pentru-modificarea-unor-acte-normative-modificarea

Infracțiunile, prevăzute la art. 259 CP RM, au obiect imaterial principal care constă în informația computerizată accesată ilegal. Totodată, informația computerizată distrusă, deteriorată, modificată, blocată sau copiată formează obiectul imaterial secundar al acestor infracțiuni. Calculatoarele, sistemul informatic sau reţeaua informatică, a căror funcționare a fost dereglată, formează obiectul material secundar al infracțiunilor ce sunt specificate în art. 259 CP RM.

Informația computerizată (ca și alte asemenea entităţi imateriale), nu poate constitui obiectul material al infracţiunii. De aceea, nu putem agrea următoarele opinii. Astfel, N.F. Ahramenka susține: „Din punct de vedere fizic, informațiile computerizate sunt inseparabile de suportul lor, și anume de un obiect material”[818]; „[Mediile] de stocare, folosite frecvent în prezent, sunt componente ale calculatoarelor, ale sistemelor și rețelelor informatice.”[819] În replică, M.V. Karcevski și D.S. Azarov observă întemeiat că „noţiunile „informaţie” şi „suport de informaţie” nu sunt identice”[820], „deoarece informaţia este un obiect imaterial care, la rândul său, se conţine şi poate fi transmis în timp şi în spaţiu prin intermediul suporturilor materiale.”[821]

N.F. Ahramenka confundă obiectul imaterial al infracțiunii cu suportul material al acestuia. Faptul, că informația computerizată și suportul acesteia reprezintă entități distincte, rezultă chiar din dispoziția art. 259 CP RM: „Accesul ilegal la informaţia computerizată, adică la informaţia din calculatoare, *de pe suporţii materiali* (a se citi – suporturile materiale – *n.a.*) *de informaţie* (evid. ns.), din sistemul sau reţeaua informatică [...]”.[822] Inadmisibilitatea confundării obiectului imaterial al infracțiunii cu suportul material al acestuia rezultă și din art. 320 al Codului civil.

---

[818] КАРЧЕВСЬКИЙ, М.В. *Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину)*: автореф. дис. на здоб. науков. ступ. канд. юрид, 2003, с. 14. 19 с.; АЗАРОВ, Д.С. *Кримінальна відповідальність за злочини у сфере комп'ютерної информації*: автореф. дис. на здоб. науков. ступ. канд. юрид. Київ, 2003, с. 12. 18 с.

[819] АХРАМЕНКА, Н.Ф. Компьютерная информация как предмет преступлений против информационной безопасности. In: *Правовые средства и механизмы противодействия преступности в современном обществе: материалы междунар. науч.- практ. конф. Минск, 16 окт. 2009 г*. Минск: БГУ, 2010, с. 88-90. ISBN 978-985-518-351-9.

[820] КАРЧЕВСЬКИЙ, М.В. *Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину)*: автореф. дис. на здоб. науков. ступ. канд. юрид, 2003, с. 14. 19 с.; АЗАРОВ, Д.С. *Кримінальна відповідальність за злочини у сфере комп'ютерної информації*: автореф. дис. на здоб. науков. ступ. канд. юрид. Київ, 2003, с. 12. 18 с.

[821] КАРЧЕВСЬКИЙ, М.В. *Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину)*: автореф. дис. на здоб. науков. ступ. канд. юрид, 2003, с. 14. 19 с.; АЗАРОВ, Д.С. *Кримінальна відповідальність за злочини у сфере комп'ютерної информації*: автореф. дис. на здоб. науков. ступ. канд. юрид. Київ, 2003, с. 12. 18 с.

[822] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

În cele ce urmează vor fi examinate noțiunile care se referă la obiectul material (imaterial) al infracțiunilor prevăzute la art. 259 CP RM. În primul rând, va fi analizată noțiunea de informație computerizată.

Tranziția de la o societate industrială la o societate informațională este marcată de creșterea rolului informației în toate sferele activității umane. Nimeni nu poate pune la îndoială că informația a devenit unul dintre elementele cheie ale societății moderne. Grație caracteristicilor sale specifice, informația constituie o resursă profitabilă. Acest aspect condiționează posibilitatea folosirii informației în scopuri ilegale. Conform pct. 3 din Anexa la Legea nr. 299 din 21.12.2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova, „creșterea dependenței societății contemporane de globalizarea sistemelor informaționale [...] conduce la sporirea vulnerabilității [...] față de amenințările [...] din domeniile informațional-tehnologic și informațional-mediatic."[823] Într-adevăr, apariția unor oportunități calitativ noi de schimburi de informație la nivel global, regional și național, pe care le oferă tehnologiile informaționale, face ca domeniul informațional să fie extrem de atractiv pentru infractori. Dezvoltarea dinamică a rețelelor de telecomunicații, crearea a numeroase resurse informaționale și baze de date, dezvoltarea unor soluții mai avansate pentru obţinerea, colectarea, stocarea, prelucrarea şi diseminarea informației – toate acestea facilitează comiterea infracțiunilor care au ca obiect imaterial informația în general și informația computerizată în particular.

Odată cu dezvoltarea progresului științific și tehnologic, relațiile în sfera circulației informațiilor computerizate au obținut un puternic impuls. Apariția unui nou tip de relații sociale are ca efect faptul că mai devreme sau mai târziu devine necesară ocrotirea lor. Din art. 259 CP RM rezultă în mod vădit că relațiile în sfera circulației informației computerizate sunt ocrotite datorită faptului că accesarea ilegală a unei asemenea informații sau crearea ilegală de obstacolele în calea utilizării informației computerizate prejudiciază drepturile și interesele ocrotite de lege ale unor persoane fizice sau juridice. În ipoteza faptelor infracționale ce sunt prevăzute de art. 259 CP RM, obiectul juridic special este lezat pe calea influențării nemijlocite asupra informației computerizate. Drept urmare, devine necesară stabilirea înțelesului noțiunii „informație computerizată", care este folosită în art. 259 CP RM.

După părerea lui N.-G. Drăgulănescu, prin „informație" se are în vedere „o colecţie de fapte [...] organizate astfel încât valoarea lor să fie superioară sumei valorilor faptelor respective, în

[823] Legea privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova: nr. 299 din 21.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 48-57, 122.

sine”.[824] În viziunea lui C. Gaindric, „informațiile constituie o colecție ierarhică de date despre anumite aspecte ale lumii reale”[825]; „Informațiile sunt un flux de mesaje din care se creează cunoștințe, de obicei sub forma unui document [...]”[826]; „Informațiile au un destinatar (sau mai mulți) și un expeditor, care informează destinatarul în scopul luării deciziilor.”[827] Din aceste definiții se poate deduce că, în esență, informația reprezintă rezultatul perceperii obiectelor și fenomenelor din lumea înconjurătoare prin mesaje și simboluri care sunt transmise și recepționate în procesul cunoașterii.

În mod aparent, prin „informație computerizată” s-ar înțelege informația percepută computerizat, adică prin intermediul unui computer (calculator). Or, computerul percepe informația indiferent de forma acesteia cu ajutorul unui dispozitiv de introducere a informației (tastatură, mouse, microfon, cameră video etc.), iar apoi codifică informația recepționată în scopul prelucrării ulterioare a acesteia. În acest fel, noțiunea de informație computerizată ar trebui înțeleasă ca informație interpretată de către un program de calculator, de către un alt produs informatic sau de către un ansamblu al acestora.

Totuși, în art. 259 CP RM se pune accentul nu pe forma de percepere a informației computerizate, ci pe mediul în care se află informația la momentul săvârșirii infracțiunii. Astfel, în dispoziția din alineatul (1) al acestui articol se menționează: „informaţia computerizată, adică [...] informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică.”[828] În fond, aceeași abordare a fost promovată în alin. 1 art. 176[1] CP RM din 1961, în care se vorbea despre „accesul ilegal (nesancţionat) la *informaţia ce se păstrează în sistemul computerizat* (evid. ns.)”.[829]

De asemenea, nu forma de percepere a informației computerizate, ci mediul, în care se află informația la momentul săvârșirii infracțiunii, este criteriul pus la baza definirii noțiunii de informație computerizată în unele surse doctrinare. De exemplu, M.A. Zubova este de părerea că „informație computerizată constituie acea manifestare a realității obiective, care poate schimba caracterul relațiilor sociale”[830], „care reprezintă rezultatul activității umane și care este fixată pe

---

[824] DRĂGULĂNESCU, Nicolae-George. Concepte ale societăţii informaţionale „informare” – „informaţie”. În: *Magazin bibliologic*, 2011, nr. 1-2, pp. 3-6. ISSN 1857-1476.
[825] GAINDRIC, Constantin. Cu privire la noțiunile de date, informații, cunoștințe. În: *Akademos*, 2020, nr. 3, pp. 15-18. ISSN 1857-0461.
[826] Ibidem.
[827] Ibidem.
[828] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[829] Ibidem.
[830] ЗУБОВА, М.А. *Компьютерная информация как объект уголовно-правовой охраны*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Казань, 2008, с. 9-10. 28 с.

un suport material, într-un calculator, într-un sistem informatic sau într-o rețea informatică”.[831] Păreri apropiate exprimă alți autori.[832] Din aceste viziuni doctrinare se desprinde că informația computerizată este informația destinată prelucrării pe un calculator, fixată pe un suport care poate fi citit de un calculator sau transmis într-un mediu care face posibilă interacționarea în cadrul unui sistem informatic sau al unei rețele informatice.

În altă ordine de idei, menționăm că în unele surse normative, în locul sintagmei „informație computerizată” se folosește sintagma „date informatice”.

Astfel, la 27.11.2015, prin Rezoluția nr. 43-16 a Adunării Interparlamentare a statelor membre ale CSI, în art. 286 „Accesul ilegal la informaţia computerizată” din Codul penal model al CSI, sintagma „informația computerizată” a fost substituită prin sintagma „date informatice.”[833] Prin aceeași rezoluție, în alin. 1 art. 286 din Codul penal model al CSI, cuvintele „accesul la informația stocată într-un sistem informatic, într-o rețea informatică sau pe un suport informatic”[834] au fost înlocuite prin cuvintele „accesul la datele stocate într-un dispozitiv[835] sau sistem informatic, într-o rețea informatică, pe un suport informatic sau pe un alt suport”.[836] În conformitate cu nota 1 la art. 286 din Codul penal model al CSI, „date informatice [...] înseamnă orice reprezentare de fapte, informaţii sau concepte sub o formă adecvată prelucrării într-un

---

[831] Ibidem, c. 9-10.

[832] СТАРИЧКОВ, М.В. Понятие «компьютерная информация» в российском уголовном праве. În: *Вестник Восточно-Сибирского института МВД России*, 2014, № 1, с. 16-20. ISSN 2312-3184; ГАСАН, Л.И. К вопросу о трактовке несанкционированного доступа к компьютерной информации (ст. 349 УК Республики Беларусь). În: *Правовое обеспечение инновационного развития общества и государства: материалы междунар. науч. конф. студентов, магистрантов и аспирантов. Минск, 29-30 окт. 2010 г*. Минск, 2011, с. 229-230. ISBN 978-985-518-543-8; ГОЛУБЕВ, В. *Компьютерная информация как объект правоотношений*. [citat 07.03.2022] Disponibil: http://www.crime-research.ru/ library/Golubev09_03.html

[833] *Приложение к постановлению МПА СНГ от 27.11.2015 г. № 43-16. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. Изменения в модельный Уголовный кодекс для государств-участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере*. [citat 06.03.2022] Disponibil: www.parliament.am/library/modelayin%20orenqner/336.pdf

[834] Ibidem.

[835] Conform notei 2 la art. 286 din Codul penal model al CSI, prin „dispozitiv informatic” se înțelege „dispozitivul universal controlat de un program, care este conceput pentru stocarea, prelucrarea și transmiterea de date”*, „în rezultatul operării unui număr de comenzi, care este capabil să efectueze multiple operațiuni matematice și logice”*, „precum și să execute alte sarcini de manipulare cu simboluri sau cu informație de alt tip, și care generează rezultate într-o formă care poate fi citită de om sau de un alt dispozitiv informatic.”*

* *Приложение к постановлению МПА СНГ от 27.11.2015 г. № 43-16. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. Изменения в модельный Уголовный кодекс для государств-участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере*. [citat 06.03.2022] Disponibil: www.parliament.am/library/modelayin%20orenqner/336.pdf

[836] *Приложение к постановлению МПА СНГ от 27.11.2015 г. № 43-16. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. Изменения в модельный Уголовный кодекс для государств-участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере*. [citat 06.03.2022] Disponibil: www.parliament.am/library/modelayin%20orenqner/336.pdf

sistem informatic [...]."[837] Observăm că în această definiție a noțiunii „date informatice" accentul se pune nu pe mediul în care se află informația la momentul săvârșirii infracțiunii (ca în definiția noțiunii „informația computerizată), ci pe forma de percepere a informației computerizate.

Există oare temeiuri ca în art. 259 CP RM sintagma „informația computerizată" să fie înlocuită prin sintagma „date informatice". Răspunsul la această întrebare este afirmativ, iar argumentele de rigoare vor fi prezentate mai jos.

Astfel, înainte de toate, sintagma „date informatice" este utilizată în alte articole din Capitolul XI al părții speciale a Codului penal al Republicii Moldova (și anume – în art. 260^1-260^3, 260^5 și 260^6). În afară de aceasta, noțiunea „date informatice" este definită în art. 2 din Legea nr. 20/2009: „date informatice – orice reprezentare de fapte, informaţii sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcţii de către un sistem informatic"[838].[839] Totodată, noțiunea mai largă „date" este definită în alte două legi. Conform art. 2 al Legii nr. 1069/2000, prin „date" se înțelege „fapte, noţiuni, fenomene, evenimente, însuşiri, indici, instrucţiuni etc., reprezentate sub o formă convenţională, adecvată comunicării, interpretării sau prelucrării manuale ori cu mijloace automate".[840] Potrivit art. 3 al Legii nr. 467/2003, „date" înseamnă „informaţia prezentată într-o anumită formă care permite a o comunica, comenta şi prelucra".[841]

De reținut că, în corespundere cu ultimul dintre articolele sus-menționate, prin „informaţie" se înțelege „cunoştinţe despre persoane, subiecte, fapte, evenimente, fenomene, procese, obiecte, situaţii şi idei".[842] Dacă vom compara această definiție cu cea a noțiunii „date", vom vedea că ultima noțiune este mai îngustă decât prima. Or, date constituie informaţia prezentată într-o formă facilă comunicării, comentării şi prelucrării acesteia. În această privință, aderăm la punctul de vedere al lui C. Gaindric: „Diferența dintre informații și date constă în faptul că datele reflectă fapte concrete, evenimente și fenomene [...], iar informațiile apar ca rezultat în procesul de rezolvare a unor probleme"[843]; „Datele sunt o formă de prezentare a informațiilor. Informația este un produs al interacțiunii între date și metode, luate în considerare în contextul acestei

---

[837] Ibidem.
[838] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.
[839] Remarcăm că această definiție este identică cu cea a noțiunii „date informatice" din nota 1 la art. 286 din Codul penal model al CSI.
[840] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[841] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.
[842] Ibidem.
[843] GAINDRIC, Constantin. Cu privire la noțiunile de date, informații, cunoștințe. În: *Akademos*, 2020, nr. 3, pp. 15-18. ISSN 1857-0461.

interacțiuni”[844]; „Cel puțin în sistemele informaționale ea există exact cât durează interacțiunea respectivă, iar restul timpului este păstrată în bazele de date sub formă de date.”[845]

În pct. 2 din Hotărârea Guvernului nr. 811 din 29.11.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020, la subpct. 15), găsim următoarea definiție a noțiunii „spațiu cibernetic”: „mediu virtual, generat de infrastructurile cibernetice, incluzând *conținutul informațional* (evid. ns.) procesat, stocat sau transmis, precum și acțiunile derulate de utilizatori în acest mediu.”[846] În realitate, conținutul informațional, specificat în această definiție, este alcătuit din date informatice, nu dintr-o informație computerizată oarecare. Despre aceasta ne vorbește sintagma „procesat, stocat sau transmis”. Or, informația din mediul virtual este procesată, stocată sau transmisă pentru a fi recepționată de om. În aceste condiții, informația computerizată îmbracă indiscutabil forma de date informatice.

Cele menționate mai sus ne fac să susținem recomandarea din pct. 34 al Proiectului de aviz comun al Comisiei de la Veneția și al Direcției Generale Drepturile Omului și Statul de Drept (DGI) a Consiliului Europei pe marginea Proiectului de lege nr. 161 pentru modificarea și completarea legislației moldovenești din domeniul criminalității informatice: „Se recomandă reformularea integrală a art. 259 din Codul penal, astfel încât să se asigure, în conformitate cu Convenția de la Budapesta[847], „o sancționare exactă a diferitelor fapte concrete care implică accesul ilegal la sistemele informatice[848]; „Sintagma „informația computerizată” ar trebui să fie substituit cu sintagma „date informatice”, având în vedere că această sintagmă este folosită în alte articole din Codul penal[849], „care pun în aplicare Convenția. De asemenea, pentru a asigura coerența cu Convenția și Legea privind criminalitatea informatică[850], „ar trebui să fie utilizate definițiile prevăzute de prezenta lege (punerea în aplicare a Articolului 1 al Convenției)”.[851]

Într-adevăr, în art. 1 din Convenția de la Budapesta, la lit. b) este formulată următoarea definiție a noțiunii „date informatice”: „reprezentare de fapte, informaţii sau concepte sub o

[844] Ibidem.
[845] Ibidem.
[846] Hotărârea Guvernului cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020: nr. 811 din 29.11.2015. În: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 306-310, 905.
[847] *Proiect de aviz comun al Comisiei de la Veneția și al Direcției Generale Drepturile Omului și Statul de Drept (DGI) a Consiliului Europei pe marginea Proiectului de lege nr. 161 pentru modificarea și completarea legislației moldovenești din domeniul criminalității informatice*. [citat 07.03.2022] Disponibil: https://www.parlament.md/LinkClick.aspx?fileticket=IbGsshOB2Ys%3D&tabid=90&language=ro-RO
[848] Ibidem.
[849] Ibidem.
[850] Ibidem.
[851] Ibidem.

formă adecvată prelucrării într-un sistem informatic [...]”.[852] Observăm că această definiție este identică cu cea a noțiunii „date informatice” din art. 2 al Legii nr. 20/2009.

În pct. 25 din Raportul explicativ la Convenția de la Budapesta pot fi identificate anumite explicații referitoare la definiția noțiunii „date informatice” din art. 1 din Convenția de la Budapesta: „Definiția noțiunii „date informatice” se bazează pe definiția noțiunii de date a Organizației Internaționale de Standardizare (ISO)”[853]; „Această definiție conține expresia „potrivit pentru prelucrare”. Aceasta înseamnă că datele sunt reprezentate într-o asemenea formă încât să poată fi procesate direct de sistemul informatic”[854]; „Pentru a clarifica faptul că datele în accepția prezentei convenții trebuie înțelese ca date în formă electronică sau în altă formă direct prelucrabilă, este introdusă noțiunea „date informatice””[855]; „Datele informatice, [...] prelucrate automat, pot fi ținta uneia dintre infracțiunile prevăzute în prezenta convenție [...]”.[856]

Definiția noțiunii „date informatice” de la lit. b) art. 1 din Convenția de la Budapesta a servit ca model nu doar pentru definiția noțiunii omonime din art. 2 al Legii nr. 20/2009, ci și pentru definiția corespunzătoare din alin. 22 art. 93 CP RBu[857], de la lit. i) art. 13 CPGr[858] și din alin. (1) art. 337B CP RMa.[859] Nu diferă prea mult de această paradigmă definițiile din unele legi penale ale statelor din componența SUA (de exemplu, de cele formulate în alin. (7) § 5-41-102 din Codul penal al statului Arkansas[860] și în art. 205.474 din Codul penal al statului Nevada[861]).

În Codul penal al României, în alin. (2) art. 181 este formulată următoarea definiție a noțiunii „date informatice”: „orice reprezentare a unor fapte, informații sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic.”[862] Trebuie de menționat că noțiunea de date informatice este definită, de asemenea, în alin. (5) art. 138 al Codului de procedură penală a României: „Prin date informatice se înțelege orice reprezentare de fapte, informații sau concepte

---

[852] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[853] *Explanatory Report to the Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/16800cce5b
[854] Ibidem.
[855] Ibidem.
[856] Ibidem.
[857] *Codul penal al Republicii Bulgaria*. [citat 07.03.2022] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[858] *Codul penal al Greciei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Grecia-RO.html
[859] *Codul penal al Republicii Malta*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Malta-RO.html
[860] *2010 Arkansas Code. Title 5 – Criminal Offenses*. [citat 06.03.2022] Disponibil: https://law.justia.com/codes/arkansas/2010/title-5/subtitle-4/chapter-41/subchapter-1/5-41-102/
[861] *2009 Nevada Code. Title 15 – Crimes and punishments*. [citat 06.03.2022] Disponibil: https://law.justia.com/codes/nevada/2009/title-15/chapter-205/unlawful-acts-regarding-computers-and-information-services/
[862] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.

sub o formă adecvată prelucrării într-un sistem informatic”[863], „inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic”.[864] Luând în considerare sintagma „inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic”, această definiție se aseamănă cu cea din Legea României nr. 161/2003, în care, la lit. d) alin. (1) art. 35, prin „date informatice” se înţelegea „orice reprezentare a unor fapte, informaţii sau concepte într-o formă care poate fi prelucrată printr-un sistem informatic. În această categorie se include şi orice program informatic[865] care poate determina realizarea unei funcţii de către un sistem informatic”[866].[867]

În legătură cu discrepanța dintre definiția din alin. (2) art. 181 CPR și cea din alin. (5) art. 138 din Codul de procedură penală a României, M. Dunea exprimă următorul raționament: „Rezultă că trebuie admis faptul că noţiunea penală materială de date informatice este chiar şi parţial distinctă (mai restrânsă) faţă de cea procesual penală (altfel spus, punctual: se poate oare considera că, în sensul legii penale substanţiale, un program capabil să determine executarea unei funcţii de către un sistem informatic nu reprezintă parte componentă a conceptului de date informatice, dar că în sens procesual penal acesta se încadrează în noţiunea respectivă)? În cazul unui răspuns afirmativ, ne întrebăm: de ce?; care ar fi justificarea logică a acestei deosebiri? În cazul unui răspuns negativ, ne întrebăm oare de ce această (aparentă) incongruenţă terminologică, această aparentă diferenţă de sferă de cuprindere şi de formulare a unuia şi aceluiaşi concept, în cadrul unitar de referinţă al dreptului penal (fie acesta material / substanţial sau formal / procesual penal)?”.[868]

---

[863] Codul de procedură penală al României: nr. 135 din 01.07.2010. În: *Monitorul Oficial al României*, 2010, nr. 486.

[864] Ibidem.

[865] Potrivit lit. c) alin. (1) art. 35 al Legii României nr. 161/2003, „prin program informatic se înțelege un ansamblu de instrucțiuni care pot fi executate de un sistem informatic în vederea obținerii unui rezultat determinat”.* O definiție apropiată putem identifica în art. 2 al Legii nr. Legii nr. 1069/2000: „program [...] – secvenţă de declaraţii şi instrucţiuni ale unui limbaj de programare, lansată într-un mediu operaţional al calculatorului, pentru îndeplinirea anumitor funcţii ori soluţionarea unor probleme”.**

* Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.

** Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

[866] Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.

[867] Referirea la programul informatic, luată în considerare în definițiile din alin. (5) art. 138 din Codul de procedură penală a României și din lit. d) alin. (1) art. 35 al Legii României nr. 161/2003, apropie aceste definiții de cele ale noțiunii „date informatice” din art. 2 al Legii nr. 20/2009 și de la lit. b) art. 1 din Convenția de la Budapesta.

[868] DUNEA, Mihai. Unele provocări juridico-penale ca urmare a evoluţiei tehnologiei informaţiei (inclusiv a evoluţiei Internetului). În: *Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza” din Iaşi, seria Ştiinţe Juridice*, 2019, nr. 2-bis, pp. 187-200. ISSN 1221-8464.

Considerăm că, din analiza alin. (5) art. 138 din Codul de procedură penală a României (și a lit. d) alin. (1) art. 35 al Legii României nr. 161/2003), nu rezultă că definiția din alin. (5) art. 138 din Codul de procedură penală a României este mai largă decât definiția din alin. (2) art. 181 CPR. Sintagma „inclusiv un program capabil să determine executarea unei funcții de către un sistem informatic" din alin. (5) art. 138 din Codul de procedură penală a României are un caracter de precizare, nu de augmentare. Această concluzie rezultă din următorul fragment din Decizia Înaltei Curți de Casație și Justiție a României nr. 68 din 29.09.2021 referitoare la interpretarea dispozițiilor art. 360 alin. (1) din Codul penal: „Infracțiunea a fost preluată din Legea nr. 161/2003 [...]."[869]; „Chiar dacă Codul penal nu a preluat toate definițiile din Legea nr. 161/2003, aceasta rămâne în continuare un reper pentru înțelegerea elementelor de conținut ale infracțiunii criticate»".[870] În consecință, este întemeiat ca prin „date informatice" să se înțeleagă, printre altele, un program informatic.

În alt context, pentru a stabili cu precizie limitele de aplicare a art. 259 CP RM, este necesară interpretarea cât mai exactă a noțiunilor utilizate în acest articol, inclusiv a noțiunilor „sistem informatic" și „rețea informatică".[871] G. Zlati menționează că „[...] în dreptul penal [...] putem identifica noțiuni cu un caracter predominant tehnic. Acestea sunt esențiale [...] din perspectiva tipicității unor fapte prevăzute de legea penală [...]"[872]; „Uneori lecturarea definiției legale nu este suficientă pentru a înțelege limitele și deficiențele unei anumite noțiuni, motiv pentru care apreciem ca fiind necesară o analiză punctuală".[873]

Din perspectiva tipicității infracțiunilor prevăzute la art. 259 CP RM, noțiunile „sistem informatic" și „rețea informatică" sunt esențiale. În continuare va fi efectuată analiza punctuală a acestor noțiuni.

Conform lit. a) art. 1 din Convenția de la Budapesta, „expresia „sistem informatic" desemnează orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură"[874], „care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor".[875] Din această definiție rezultă următoarele trăsături caracteristice ale sistemului informatic: 1) este fie un dispozitiv izolat, fie un ansamblu

---

[869] Decizia Înaltei Curți de Casație și Justiție a României referitoare la interpretarea dispozițiilor art. 360 alin. (1) din Codul penal: nr. 68 din 29.09.2021. În: *Monitorul Oficial al României*, 2022, nr. 56.
[870] Ibidem.
[871] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Științe Sociale", 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[872] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 29. 658 p. ISBN 978-606-8892-62-7.
[873] Ibidem, p. 29.
[874] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[875] Ibidem.

de dispozitive interconectate ori aflate în legătură; 2) asigură ori dintre care unul sau mai multe elemente asigură prelucrarea automată a datelor informatice; 3) implică asigurarea prelucrării automate a datelor informatice prin executarea unui program informatic.[876]

În Raportul explicativ la Convenția de la Budapesta, în pct. 23, găsim o interpretare care ne ajută să înțelegem mai bine esența unui sistem informatic: „Conform Convenției, un sistem informatic este un dispozitiv format din *hardware* și *software* dezvoltate pentru prelucrarea automată a datelor informatice".[877]; „Sistemul informatic poate include echipamente de intrare, ieșire și stocare. Poate fi autonom sau conectat în rețea cu alte dispozitive similare"[878]; „„Automată" înseamnă fără intervenție umană directă. „Prelucrare a datelor" înseamnă că datele din sistemul informatic sunt operate prin executarea unui program de calculator"[879]; „„Program de calculator" este setul de instrucțiuni care pot fi executate de calculator pentru a obține rezultatul dorit. Un calculator poate rula diferite programe"[880]; „Un sistem informatic constă, de obicei, din diferite dispozitive, care trebuie distinse ca: procesor sau unitate centrală de procesare *și* periferice"[881]; „„Periferic" este dispozitivul care îndeplinește anumite funcții specifice în interacțiune cu unitatea de procesare, cum ar fi: imprimantă; ecran video; cititor/inscriptor CD; dispozitiv de stocare."[882]

În dispoziția de la lit. a) art. 2 al Directivei 2013/40/UE, definiția noțiunii „sistem informatic" prezintă anumite diferențe în raport cu definiția de la lit. a) art. 1 din Convenția de la Budapesta.[883] Conform acestei definiții, „sistem informatic" înseamnă „un dispozitiv sau grup de dispozitive interconectate sau omoloage"[884], „dintre care unul sau mai multe asigură, prin intermediul unui program, prelucrarea automată a datelor informatice"[885], „precum și datele informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor."[886] Din această

---

[876] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Științe Sociale", 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[877] *Explanatory Report to the Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/16800cce5b
[878] Ibidem.
[879] Ibidem.
[880] Ibidem.
[881] Ibidem.
[882] Ibidem.
[883] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Științe Sociale", 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[884] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en
[885] Ibidem.
[886] Ibidem.

definiție ar reieși că sistem informatic se consideră: 1) fie un dispozitiv, fie un grup de dispozitive interconectate sau omoloage, fie datele informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor; 2) în cazul în care constă dintr-un fie dintr-un dispozitiv, fie dintr-un grup de dispozitive interconectate sau omoloage, atunci unul sau mai multe dintre acestea asigură prelucrarea automată a datelor informatice; 3) implică asigurarea prelucrării automate a datelor informatice prin executarea unui program de calculator.[887]

Observăm că fragmentul „precum și datele informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor”[888] este ceea ce deosebește definiția de la lit. a) art. 2 al Directivei 2013/40/UE de cea de la lit. a) art. 1 din Convenția de la Budapesta. În legătură cu acest fragment, susținem opinia exprimată de G. Zlati: „În opinia noastră, legiuitorul român ar trebui să evite o transpunere *verbatim* a definiției sistemului informatic din cuprinsul art. 2 lit. a) din Directiva 2013/40/UE.”[889]; „[...] Observăm cu îngrijorare tentația legiuitorului european de a încerca să impună statelor membre o transpunere *verbatim* a unor directive în materie penală”[890], „cu toate că TFUE (adică Tratatul privind funcționarea UE[891] – *n.a.*) generează obligații în sarcina statelor membre doar în ceea ce privește atingerea scopului urmărit de către un asemenea instrument juridic.”[892] Având în vedere statutul de candidat la aderare la Uniunea Europeană al Republicii Moldova, această opinie ar trebui luată în calcul de către legiuitorul moldovean care, în perspectivă, din exces de zel, ar putea să transpună *mot-a-mot* definiția de la lit. a) art. 2 al Directivei 2013/40/UE în Codul penal al Republicii Moldova. O asemenea transpunere ar fi vulnerabilă sub aspectul clarității și previzibilității legii penale.[893] Or, interpretând dispoziția de la alin. (1) art. 259 CP RM, ar fi imposibil de înțeles ce înseamnă „dereglarea funcționării datelor

[887] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Științe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[888] Ibidem.
[889] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 34. 658 p. ISBN 978-606-8892-62-7.
[890] Ibidem, p. 35.
[891] *Tratatul privind funcționarea Uniunii Europene*. [citat 09.07.2022] Disponibil: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_2&format=PDF
[892] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 34-35. 658 p. ISBN 978-606-8892-62-7.
[893] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Științe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

informatice stocate, prelucrate, recuperate sau transmise de sistemul informatic în vederea exploatării, a utilizării, a protecției și a întreținerii acestui sistem."[894]

Nu excludem ideea ca textul definiției de la lit. a) art. 2 al Directivei 2013/40/UE să fi fost tradus greșit în limba română.[895] De exemplu, definițiile noțiunii de sistem informatic din Codul penal al Republicii Bulgaria și din Codul penal al Republicii Malta au ca model definiția de la lit. a) art. 2 al Directivei 2013/40/UE. Din definițiile din Codul penal al Republicii Bulgaria și din Codul penal al Republicii Malta rezultă că sistemul informatic implică asigurarea prelucrării automate a datelor informatice, *precum și a datelor informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor*. Din definiția din Codul penal al Republicii Bulgaria și din Codul penal al Republicii Malta nu rezultă că sistem informatic se consideră, între altele, datele informatice stocate, prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor.[896]

O altă definiție a noțiunii „sistem informatic" este formulată la lit. f) art. 4 al Convenţiei Naţiunilor Unite asupra utilizării comunicaţiilor electronice în contractele internaţionale. Conform acestei definiții, „sistem informatic" înseamnă „sistemul conceput pentru generarea, trimiterea, primirea, stocarea sau prelucrarea în alt mod a mesajelor de date".[897] Această definiție este adaptată exclusiv necesităților actului normativ din care face parte. Ea nu răspunde necesităților art. 259 CP RM, de aceea urmează a fi ignorată în procesul de interpretare a acestui articol.[898]

Definiții ale noțiunii „sistem informatic" pot fi identificate în legile penale ale unor state. În cazul legilor penale ale statelor europene, observăm că definițiile în cauză au ca model – într-o măsură mai mare sau mai mică – fie definiția de la lit. a) art. 1 din Convenția de la Budapesta, fie

---

[894] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

[895] În limba engleză, definiția în cauză este: ""information system" means a device or group of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data"*, „*as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance* (evid. ns.)".*

* *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en

[896] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale", 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

[897] *United Nations Convention on the Use of Electronic Communications in International Contracts*. [citat 06.03.2022] Disponibil: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-57452_ebook.pdf

[898] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale", 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

definiția de la lit. a) art. 2 al Directivei 2013/40/UE.[899] Ne referim la definițiile din pct. 8 alin. (1) §74 CP RA[900], din pct. 21 art. 93 CP RBu[901], de la lit. h) art. 13 CPGr[902], din alin. (1) art. 337B CP RMa[903], din alin. (6) § 5-41-102 din Codul penal al statului Arkansas și din art. 205.476 din Codul penal al statului Nevada.[904]

Desigur, nu putem face abstracție de definiția din alin. (1) art. 181 CPR: „Prin sistem informatic se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională”[905], „dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.”[906] Remarcăm că această definiție are ca model definiția de la lit. a) art. 1 din Convenția de la Budapesta, nu definiția de la lit. a) art. 2 al Directivei 2013/40/UE.[907] La lit. a) alin. (1) art. 35 al Legii României nr. 161/2003[908], definiția noțiunii „sistem informatic” are exact același conținut ca în alin. (1) art. 181 CPR. Totodată, alin. (4) art. 138 din Codul de procedură penală al României conține o definiție care repetă aproape fidel textul din alin. (1) art. 181 CPR: „Prin sistem informatic se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate ori aflate în relație funcțională”[909], „dintre care unul sau mai multe asigură prelucrarea automată a datelor, cu ajutorul unui program informatic.”[910]

În această ordine de idei, M. Dunea exprimă o opinie care merită a fi luată în considerare: „În Codul de procedură penală legiuitorul (tot penal, în esenţă...) a reglementat, de asemenea (în mod aparent redundant)”[911], „norme de interpretare referitoare (printre altele) la semnificaţia conceptelor de sistem informatic şi date informatice, calificate sub aspect procesual penal drept

---

[899] Ibidem.
[900] *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html
[901] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[902] *Codul penal al Greciei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Grecia-RO.html
[903] *Codul penal al Republicii Malta*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Malta-RO.html
[904] *2009 Nevada Code. Title 15 – Crimes and punishments*. [citat 06.03.2022] Disponibil: https://law.justia.com/codes/nevada/2009/title-15/chapter-205/unlawful-acts-regarding-computers-and-information-services/
[905] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[906] Ibidem..
[907] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[908] Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.
[909] Codul de procedură penală al României: nr. 135 din 01.07.2010. În: *Monitorul Oficial al României*, 2010, nr. 486.
[910] Ibidem.
[911] DUNEA, Mihai. Unele provocări juridico-penale ca urmare a evoluţiei tehnologiei informaţiei (inclusiv a evoluţiei Internetului). În: *Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza” din Iaşi, seria Ştiinţe Juridice*, 2019, nr. 2-bis, pp. 187-200. ISSN 1221-8464.

metode speciale de supraveghere sau cercetare (art. 138 alin. 14 şi 15 din Codul de procedură penală)”[912]; „Firesc ar fi fost, în aprecierea noastră, ca semnificaţia penală stabilită acestor noţiuni prin dispoziţiile generale ale dreptului penal material (substanţial) să fie incidentă ca atare şi în cadrul procesual penal”[913]; „eventual, legiuitorul procesual penal ar fi putut să reitereze prevederile din art. 181 C.pen. ca atare (deşi dispoziţia ar fi fost redundantă şi o trimitere la textul din legea penală materială ar fi fost mai potrivită).”[914] În continuare, același autor recomandă legiuitorului român „să unifice (formal) cele două dispoziţii indicate (art. 181 alin. 12 C. pen. şi art. 138 alin. 15 C.proc.pen.) [...]”.[915]

În aparență, o astfel de unificare terminologică ar trebui să implice procedeul normelor de referire. În context, Decizia Curții Constituționale a României nr. 53 din 25.01.2012 referitoare la excepţia de neconstituţionalitate a dispoziţiilor art. 30 alin. (3) din Codul de procedură penală, precum şi a dispoziţiilor art. 244-246, art. 248 şi 279 din Legea nr. 297/2004, raportate la art. 244 alin. (5) lit. a) pct. 2 şi lit. b) şi alin. (7) lit. a), cu aplicarea art. 276 lit. c) din Legea nr. 297/2004 privind piaţa de capital, statuează: „Pe lângă normele penale generale, speciale, complete şi de trimitere, se uzitează procedeul normelor de referire, care împrumută un element al ipotezei dintr-o altă normă, rămânând apoi legate de aceasta”[916], „astfel încât orice modificare a normei la care s-a făcut referire atrage automat modificarea normei de referire [...]”[917]; „Această normă penală îşi completează conţinutul cu elemente ale unor norme la care se referă expres şi îşi păstrează caracterul dependent în raport cu acestea.”[918] Totuși, există o soluție mai simplă. Art. 602 din Codul de procedură penală al României prevede: „Termenii sau expresiile al căror înțeles este anume explicat în Codul penal au același înțeles și în Codul de procedură penală”.[919] În aceste condiții, fiind superfluă, prevederea de la alin. (4) art. 138 din Codul de procedură penală al României ar trebui abrogată.

În pct. 5 din Decizia Curții Constituționale a României nr. 633 din 17.10.2017 referitoare la excepția de neconstituționalitate a dispozițiilor art. 181 din Codul penal și ale art. 157 și art. 168 din Codul de procedură penală, atrag atenția afirmațiile făcute de autorul sesizării: „Deși

---

[912] Ibidem.
[913] Ibidem.
[914] Ibidem.
[915] Ibidem.
[916] Decizia Curții Constituționale a României referitoare la excepţia de neconstituţionalitate a dispoziţiilor art. 30 alin. (3) din Codul de procedură penală, precum şi a dispoziţiilor art. 244-246, art. 248 şi 279 din Legea nr. 297/2004, raportate la art. 244 alin. (5) lit. a) pct. 2 şi lit. b) şi alin. (7) lit. a), cu aplicarea art. 276 lit. c) din Legea nr. 297/2004 privind piaţa de capital: nr. 53 din 25.01.2012. În: *Monitorul Oficial al României*, 2012, nr. 234.
[917] Ibidem.
[918] Ibidem.
[919] Codul de procedură penală al României: nr. 135 din 01.07.2010. În: *Monitorul Oficial al României*, 2010, nr. 486.

legiuitorul român a procedat la o transpunere fidelă a definițiilor din cuprinsul Convenției privind criminalitatea informatică, această transpunere nu este suficientă”[920], „întrucât nici definițiile reglementate în convenția anterior referită nu sunt suficient de clare, precise și previzibile”[921], „pentru asigurarea garanțiilor specifice principiului legalității incriminării și a pedepsei, ele putând fi interpretate de statele semnatare în mod diferit”[922]; „Acest din urmă aspect face ca aceeași faptă să fie sancționată penal într-un stat și să nu intre sub incidența legii penale în alt stat”[923]; „Se arată, totodată, că, în doctrină, definițiile analizate au fost amplu criticate și se face trimitere la Codurile penale din Arkansas și Nevada, despre care se afirmă că prevăd definiții ale noțiunilor de „sistem informatic” și „date informatice” mult mai clare.”[924] În pofida acestor afirmații, concluzia Curții Constituționale a României a fost următoarea: „Argumentele anterior arătate nu constituie, însă, veritabile critici de neconstituționalitate, ci o modalitate indirectă de invocare a unor pretinse greșeli de interpretare și aplicare a dispozițiilor legale ce reglementează domeniul criminalității informatice, în general, și, în mod special, a unor sintagme din cuprinsul textelor criticate. Or, aceste aspecte excedează atribuțiilor instanței de contencios constituțional [...]”.[925]

Suntem de acord cu această concluzie. În primul rând, definițiile noțiunii „sistem informatic” din Codul penal al statului Arkansas și din Codul penal al statului Nevada (pe care le-am reprodus mai sus) nu excelează prin claritate și previzibilitate și, din această cauză, nu pot să reprezinte un etalon pentru legiuitorul român (sau pentru cel moldovean). În al doilea rând, o definiție legislativă nu poate și nu trebuie să se caracterizeze printr-o abundență de detalii. În acest plan, în Decizia Curții Constituționale a Republicii Moldova nr. 78 din 16.06.2022 de inadmisibilitate a sesizării nr. 4g/2022 privind excepția de neconstituționalitate a unor dispoziții din articolul 322 alin. (1) din Codul penal, comportă interes următorul fragment din pct. 25: „În jurisprudenţa sa, Curtea a notat că legea penală nu poate să exceleze în texte explicative”[926]; „Oricât de clar ar fi redactată o normă juridică, în orice sistem de drept există un element inevitabil de interpretare judiciară, inclusiv într-o normă de drept penal. [...].”[927] De asemenea, în

[920] Decizia Curții Constituționale a României referitoare la excepția de neconstituționalitate a dispozițiilor art. 181 din Codul penal și ale art. 157 și art. 168 din Codul de procedură penală: nr. 633 din 17.10.2017. În: *Monitorul Oficial al României*, 2018, nr. 126.
[921] Ibidem.
[922] Ibidem.
[923] Ibidem.
[924] Ibidem.
[925] Ibidem.
[926] Decizia Curții Constituționale a Republicii Moldova de inadmisibilitate a sesizării nr. 4g/2022 privind excepția de neconstituționalitate a unor dispoziții din articolul 322 alin. (1) din Codul penal: nr. 78 din 16.06.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 201-207.
[927] Ibidem.

Decizia Curții Constituționale a Republicii Moldova nr. 67 din 15.06.2020 de inadmisibilitate a sesizării nr. 27g/2020 privind excepția de neconstituționalitate a unor prevederi din articolul 171 din Codul penal, în pct. 29, se menționează: „Doctrina juridică [poate] constitui un reper obiectiv în funcție de care să poată fi apreciat conținutul unei norme penale și care poate contribui la aplicarea previzibilă a acesteia [...].”[928] Analiza de față are tocmai scopul conturării acelui reper obiectiv în funcție de care să poată fi apreciat conținutul noțiunii „sistem informatic”, folosite în art. 259 CP RM.

În acest context, apare necesitatea delimitării noțiunii în cauză de noțiunea „sistem informațional”. Am putut vedea *supra* că, în Codul penal al Republicii Malta, noțiunea „sistem informaţional” este utilizată în accepțiunea de „sistem informatic”. Considerăm inadmisibilă o asemenea echivalare.[929]

Conform art. 3 al Legii nr. 142 din 19.07.2018 cu privire la schimbul de date și interoperabilitate, prin „sistem informațional” se înțelege „baza de date, banca de date, registrul automatizat, platforma *web*, portalul informațional”[930], „interfața de schimb de date, punctul de acces și/sau cabinetul virtual individual, atât ale furnizorului de date”[931], „cât și ale consumatorului de date, participanți la schimbul de date, care prelucrează, furnizează și distribuie informații”.[932] O definiție diferită în unele privințe ale aceleiași noțiuni este formulată în art. 3 al Legii nr. 467/2003: „sistem informaţional – totalitate de resurse şi tehnologii informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie.”[933] În fine, conform art. 2 al Legii nr. 1069/2000, sistem informațional este „sistemul de prelucrare a informaţiei, împreună cu resursele organizaţionale asociate, cum ar fi resursele umane şi tehnice, care furnizează şi distribuie informaţia.”[934]

Noțiunea „sistem informatic” are un alt înțeles în contextul legislației Republicii Moldova. Astfel, potrivit art. 2 al Legii nr. 20/2009, prin „sistem informatic” se înțelege „orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură care asigură ori dintre care

---

[928] Decizia Curții Constituționale a Republicii Moldova de inadmisibilitate a sesizării nr. 27g/2020 privind excepția de neconstituționalitate a unor prevederi din articolul 171 din Codul penal: nr. 67 din 15.06.2020. În: *Monitorul Oficial al Republicii Moldova*, 2020, nr. 212-220.

[929] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

[930] Legea cu privire la schimbul de date și interoperabilitate: nr. 142 din 19.07.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 295-308, 452.

[931] Ibidem.

[932] Ibidem.

[933] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.

[934] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

unul sau mai multe elemente asigură”[935], „prin executarea unui program, prelucrarea automată a datelor”.[936] Potrivit art. 2 al Legii nr. 1069/2000, sistem informatic înseamnă „ansamblul de programe şi echipamente care asigură prelucrarea automată a datelor”.[937] A doua definiție, spre deosebire de prima, corespunde doar în parte definiției de la lit. a) art. 1 din Convenția de la Budapesta. Însă, nu acest detaliu contează cel mai mult în conjunctura concretă a analizei de față. Contează mai mult acel fapt că sistemul informatic nu se poate exprima în: resursele informaţionale interdependente, destinate păstrării şi furnizării de informaţie; tehnologiile informaţionale interdependente, destinate păstrării, prelucrării şi furnizării de informaţie; metodele destinate păstrării, prelucrării şi furnizării de informaţie; personalul care are sarcina păstrării, prelucrării şi furnizării de informaţie. Elementul comun al celor două noțiuni comparate îl constituie resursele informaţionale interdependente, destinate prelucrării de informaţie, în măsura în care asemenea resurse corespund definițiilor noțiunii „sistem informatic” din art. 2 al Legii nr. 20/2009 și din art. 2 al Legii nr. 1069/2000.[938]

O astfel de concluzie converge cu cele la care ajung unii autori. De exemplu, A. Munteanu și C.O. Șofran susțin: „În contextul teoriei generale a sistemelor, un sistem informațional se constituie din fondul de informații, tehnici de culegere și transmitere”[939], „procedurii de prelucrare a datelor destinate asigurării unei funcționări eficiente a sistemului din care fac parte”[940]; „Acel subsistem al sistemului informațional, care folosește echipamente de prelucrare automată a datelor *(hardware)*”[941] și aplicații pentru echipamentele în cauză (*software* de bază și *software* de aplicații), necesare furnizării de informații sistemului informațional, se numește sistem informatic”.[942] Așadar, relația dintre noțiunile „sistem informatic” și „sistem informațional” este o relație de tip „parte – întreg”. Din această cauză, nu este întemeiată echivalarea acestor două noțiuni.[943]

---

[935] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.
[936] Ibidem.
[937] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[938] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[939] MUNTEANU, Alin, ȘOFRAN, Cristina Ofelia. Sisteme informatice – o privire de ansamblu. În: *Anale. Seria Informatică. Universitatea Tibiscus*, 2004, vol. II, fasc. II, pp. 111-117. ISSN 2065-7471.
[940] Ibidem.
[941] Ibidem.
[942] Ibidem.
[943] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

După ce am analizat definițiile normative ale noțiunii „sistem informatic”, este necesar să examinăm definițiile doctrinare ale acesteia. Comun pentru aceste din urmă definiții este că în ele se pune accentul pe componentele unui sistem informatic.[944] De exemplu, M. Dobrinoiu afirmă că „prin sistem informatic se înţelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relaţie funcţională, dintre care unul sau mai multe asigură prelucrarea automată a datelor cu ajutorul unui program informatic”[945]; „[...] Exemple: computer personal (PC), două sa mai multe calculatoare conectate prin cablu sau fără fir *(wireless)*, reţea de calculatoare” [946], ansamblu de tip calculator – periferice (imprimantă, mediu de stocare extern, scanner etc.)”[947] Opinii similare au V. Florescu și G. Florescu[948], L. Vasiu[949], A. Munteanu și C.O. Șofran.[950]

Așa cum se va putea vedea mai jos, reţeaua de calculatoare nu poate fi privită ca exemplu de sistem informatic. Sub acest aspect, nu putem agrea viziunea propusă de M. Dobrinoiu.[951]

Ideea, potrivit căreia personalul ar reprezenta o parte a sistemului informatic, este promovată în Legea nr. 1069/2000: „Persoanele care activează în cadrul sistemelor [...] informatice sunt obligate să asigure protecţia datelor”[952] (alin. (2) art. 4); „Persoanele care activează în cadrul sistemelor [...] informatice sunt obligate să asigure protecţia şi confidenţialitatea datelor, cu excepţia celor care sunt determinate ca date publice”[953] (alin. (1) art. 28). Însă, o asemenea concepție contravine abordării pe care o atestăm în alte norme din aceeași lege: „Obiecte ale dreptului de proprietate în domeniul informaticii pot fi: a) resursele informaţionale şi datele [...]; b) sistemele informatice”[954] (alin. (1) art. 29); „Subiecte ale dreptului de proprietate în domeniul informaticii pot fi statul – prin autorităţile administraţiei publice, precum şi persoanele juridice şi fizice”[955] (alin. (1) art. 29). Potrivit acestei abordări, pe care o considerăm întemeiată, obiectul nu

---

[944] Ibidem.
[945] DOBRINOIU, Maxim. Accesul ilegal la poşta electronică. În: *Revista de Drept Penal*, 2008, nr. 3, pp. 122-125. ISSN 1223-0790.
[946] Ibidem.
[947] Ibidem.
[948] FLORESCU, Valentin, FLORESCU, Gabriela. Analiza infracţiunilor informatice incriminate în legislaţia în vigoare şi din perspectiva noului Cod penal. În: *Revista Română de Informatică şi Automatică*, 2012, vol. 22, nr. 2, pp. 21-38. ISSN 1841-4303.
[949] VASIU, Lucian. *Informatică juridică şi drept informatic. Suport de curs pentru frecvenţă redusă*. [citat 06.07.2022] Disponibil: file.ucdc.ro/cursuri/8_4_dt4752_Informatica_juridica_Vasiu_Lucian.pdf
[950] MUNTEANU, Alin, ȘOFRAN, Cristina Ofelia. Sisteme informatice – o privire de ansamblu. În: *Anale. Seria Informatică. Universitatea Tibiscus*, 2004, vol. II, fasc. II, pp. 111-117. ISSN 2065-7471.
[951] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[952] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[953] Ibidem.
[954] Ibidem.
[955] Ibidem.

trebuie confundat cu subiectul. Sistemul informatic este un obiect. Totodată, consumatorii informației produse de sistemul informatic, persoanele care contribuie la achiziția, stocarea și prelucrarea informației, precum și specialiștii care gestionează sistemele informatice (analiști, programatori, operatori, ingineri), sunt subiecți.[956]

Unii doctrinari încearcă să clasifice sistemele informatice. Spre exemplu, A. Munteanu și C.O. Șofran menționează: „Clasificarea sistemelor informatice a fost impusă de anumite criterii, și anume: domeniile de activitate cărora li se adresează”[957]; „gradul de concentrare sau dispersare a capacităților de prelucrare și memorare a datelor; modul de tratare a lucrărilor ș.a.m.d.”[958]; „După domeniile de activitate cărora li se adresează sistemele informatice pot fi: economice, științifice, de documentare, de inginerie tehnologică ș.a.m.d.”[959]; „În funcție de gradul de concentrare/dispersare a capacităților de prelucrare și memorare a datelor, distingem: sisteme concentrate și sisteme distribuite.”[960] În contextul examinat, nu este de prisos să subliniem că, indiferent de tipul sistemului informatic, acesta reprezintă obiectul material al infracțiunilor prevăzute la art. 259 CP RM.

Ultimul aspect al analizei noțiunii „sistem informatic” este cel al exemplelor de sisteme informatice.

Comitetul Convenției Consiliului Europei privind criminalitatea informatică (în continuare – CCCECI) a pus la dispoziția statelor semnatare Îndrumări privind interpretarea Convenției de la Budapesta. În legătură cu noțiunea „sistem informatic”, în aceste Îndrumări se explică: „CCCECI este de acord că această definiție (adică definiția noțiunii „sistem informatic” de la lit. a) art. 1 din Convenția de la Budapesta – *n.a.*) include, de exemplu, telefoanele mobile moderne”[961] „care sunt multifuncționale și au printre funcțiile lor capacitatea de a produce, procesa și transmite date, cum ar fi accesarea Internetului, expedierea de e-mailuri, transmiterea de atașamente, încărcarea conținutului sau descărcarea de documente”[962]; „În mod similar, CCCECI recunoaște că asistenții digitali personali (ADP-uri), cu sau fără funcționalitate *wireless*, produc, procesează și transmit date”[963]; „CCCECI subliniază că, atunci când aceste

---

[956] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[957] MUNTEANU, Alin, ȘOFRAN, Cristina Ofelia. Sisteme informatice – o privire de ansamblu. În: *Anale. Seria Informatică. Universitatea Tibiscus*, 2004, vol. II, fasc. II, pp. 111-117. ISSN 2065-7471.
[958] Ibidem.
[959] Ibidem.
[960] Ibidem.
[961] *T-CY Guidance Note no. 1 on the notion of “computer system”*. [citat 06.03.2022] Disponibil: https://rm.coe.int/09000016802e79e6
[962] Ibidem.
[963] Ibidem.

dispozitive îndeplinesc astfel de funcții, ele prelucrează „date informatice” [...]”[964]; „În plus, CCCECI consideră că, atunci când îndeplinesc asemenea funcții, ADP-urile creează „date referitoare la trafic”[965] [...]. Prin urmare, în prelucrarea acestor date, ADP-urile acționează ca un „sistem informatic” [...]. [...]”[966]; „Concluzia: CCCECI este de acord că definiția „sistemului informatic” de la lit. a) art. 1 din Convenția de la Budapesta acoperă formele în curs de dezvoltare de tehnologie”[967], „care depășesc sistemele tradiționale *mainframe* sau *desktop*, cum ar fi telefoanele mobile moderne, telefoanele inteligente, PDA-urile, tabletele sau similare.”[968] Cuvântul „similare” denotă că această listă este deschisă. Este firesc să fie așa, deoarece, datorită progresului tehnico-științific, lista de sisteme informatice se completează în fiecare an cu noi și noi exemple.

În această ordine de idei, suntem de acord cu G. Zlati, care susține: „Dispozitive precum televizoare inteligente, console Playstation, Xbox etc. [...] sunt veritabile sisteme informatice, cu toate consecințele ce derivă dintr-o asemenea calificare”[969]; „Alte sisteme informatice relevante [...] sunt următoarele: [...] b) telefoanele mobile inteligente (iPhone, Samsung etc.). [...]; [...]”[970]; „d) imprimanta, faxul și scanerul. Este important de evidențiat faptul că inclusiv aceste dispozitive intră în accepțiunea noțiunii de sistem informatic ce conțin la rândul lor un mijloc de stocare a datelor informatice”[971]; „Diferența majoră față de alte sisteme informatice fiind aceea că datele informatice stocate pot să fie volatile”[972], „ceea ce implică faptul că decuplarea dispozitivului de la sursa de curent ori oprirea acestuia poate conduce la pierderea iremediabilă a datelor informatice potențial relevante cauzei. [...]”.[973]

În măsura în care asigură prin executarea unui program prelucrarea automată a datelor informatice, televizoarele inteligente, consolele Playstation, Xbox-ul, telefoanele mobile inteligente, imprimanta, faxul, scanerul sau alte asemenea dispozitive reprezintă sisteme informatice.[974]

---

[964] Ibidem.
[965] Ibidem.
[966] Ibidem.
[967] Ibidem.
[968] *T-CY Guidance Note no. 1 on the notion of “computer system”*. [citat 06.03.2022] Disponibil: https://rm.coe.int/09000016802e79e6
[969] ZLATI, George. *Percheziția informatică. Noțiuni de bază*. [citat 07.07.2022] Disponibil: https://www.universuljuridic.ro/perchezitia-informatica-notiuni-de-baza/
[970] Ibidem.
[971] Ibidem.
[972] Ibidem.
[973] Ibidem.
[974] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Științe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

Referitor la bancomat, în pct. 2 al Regulamentului cu privire la cardurile de plată (anexa nr. 1 la Hotărârea BNM nr. 157 din 01.08.2013 cu privire la aprobarea, modificarea, completarea şi abrogarea unor acte normative ale Băncii Naţionale a Moldovei), prezintă interes următoarea definiție: „dispozitiv special este dispozitivul prin intermediul căruia se efectuează operaţiuni cu utilizarea fizică a cardurilor de plată”[975], „care poate fi: a) bancomat (denumit prescurtat, conform uzanţelor internaţionale, ATM), destinat autoservirii deţinătorilor de carduri de plată”[976], „ce permite acestora retragerea mijloacelor băneşti în numerar din conturile de plăţi, transferuri de mijloace băneşti”[977], „depunerea mijloacelor băneşti în conturi şi informarea privind situaţia conturilor şi a operaţiunilor efectuate prin intermediul cardurilor de plată; [...]”.[978] V. Coman afirmă că bancomatul este un sistem informatic.[979] De asemenea, cu privire la bancomate, G. Zlati menționează: „Acestea sunt veritabile sisteme informatice”.[980] Referitor la operațiunile îndeplinite prin intermediul bancomatelor, G. Zlati susține: „Toate aceste operațiuni au la bază funcții logice ce se transpun în procesarea unor date informatice prin intermediul unui program informatic – un sistem de operare [...]”.[981]

În ceea ce privește terminalul de tip POS, conform pct. 2 al Regulamentului cu privire la cardurile de plată (anexa nr. 1 la Hotărârea BNM nr. 157 din 01.08.2013 cu privire la aprobarea, modificarea, completarea şi abrogarea unor acte normative ale Băncii Naţionale a Moldovei), „dispozitiv special este dispozitivul prin intermediul căruia se efectuează operaţiuni cu utilizarea fizică a cardurilor de plată”[982], „care poate fi: [...] c) terminal (denumit, conform uzanţelor internaţionale, POS terminal), destinat deservirii deţinătorilor de carduri de plată, aflat la un prestator de servicii de plată sau la un comerciant”[983], „care permite citirea datelor de pe banda magnetică şi/sau de pe microprocesorul cardului de plată, procesarea acestor date şi a altor date referitoare la operaţiunea iniţiată.”[984] V. Coman consideră că terminalul de tip POS este un

[975] Hotărârea BNM cu privire la aprobarea, modificarea, completarea şi abrogarea unor acte normative ale Băncii Naţionale a Moldovei: nr. 157 din 01.08.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 191-197, 1370.
[976] Ibidem.
[977] Ibidem.
[978] Ibidem.
[979] COMAN, Vasile. *Infracțiuni privind criminalitatea în cyberspațiu: practică judiciară recentă adnotată. Vol. I*. București: Universul Juridic, 2020, p. 350-359. 486 p. ISBN 978-606-39-0627-5.
[980] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 72. 658 p. ISBN 978-606-8892-62-7.
[981] Ibidem, p. 72.
[982] Hotărârea BNM cu privire la aprobarea, modificarea, completarea şi abrogarea unor acte normative ale Băncii Naţionale a Moldovei: nr. 157 din 01.08.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 191-197, 1370.
[983] Ibidem.
[984] Ibidem.

sistem informatic.[985] G. Zlati argumentează în legătură cu astfel de terminale: „Similar cu bancomatele, și aceste dispozitive sunt sisteme informatice, [acestea] putând să preia (citirea instrumentului de plată electronică)”[986], „să prelucreze (analiza datelor informatice citite) și să transmită date informatice în vederea efectuării unui transfer de fonduri”.[987]

Așadar, deoarece asigură prin executarea unui program prelucrarea automată a datelor informatice, bancomatul și terminalul de tip POS reprezintă sisteme informatice.

Bineînțeles, exemplele de sisteme informatice nu se termină aici. După V. Coman, „acțiunea de accesare a unui cont de e-mail sau de Facebook este asimilată cu accesarea unui sistem informatic din perspectiva faptului că, prin logarea la astfel de conturi de poștă electronică”[988], „autorul logării transmite printr-un sistem informatic, sub formă de comenzi, date informatice ce sunt prelucrate de sistemul informatic”[989] „care găzduiește pe un server de tip e-mail (serviciu de tip *webmail*) într-o anumită zonă, date informatice ale conturilor accesate”[990]; „Rețeaua de socializare Facebook reprezintă un „sistem informatic” în sensul art. 181 CP, aceasta fiind o rețea de socializare existentă în mediu virtual [...].”[991] Într-o altă lucrare același autor exprimă o viziune similară.[992] În aceeași privință, M. Dobrinoiu evocă: „Poşta electronică este o facilitate de comunicare oferită cetăţenilor graţie interconectării sistemelor informatice şi cuplarea acestora la diferite tipuri de reţele care suportă protocoale necesare schimbului de mesaje electronice”[993]; „[...] Dacă făptuitorul accesează aplicaţia de poştă electronică cu scopul de a obţine mesajele deja/anterior primite, transmise ori stocate de partea vătămată”[994], „atunci încadrarea corectă este acces ilegal la un sistem informatic [...]”.[995] La rândul său, G. Zlati menționează: „Alte sisteme informatice relevante [...] sunt următoarele: a) servere prin intermediul cărora se furnizează diverse servicii ori pe care sunt găzduite anumite platforme

---

[985] COMAN, Vasile. *Infracțiuni privind criminalitatea în cyberspațiu: practică judiciară recentă adnotată. Vol. I*. București: Universul Juridic, 2020, p. 387-400. 486 p. ISBN 978-606-39-0627-5.
[986] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 74. 658 p. ISBN 978-606-8892-62-7.
[987] Ibidem, p. 74.
[988] COMAN, Vasile. *Accesarea contului de e-mail și de Facebook. Noțiunea de date informatice. Forma agravată prevăzută de art. 360 alin. (3) CP*. [citat 06.03.2022] Disponibil: https://www.universuljuridic.ro/accesarea-contului-de-e-mail-si-de-facebook-notiunea-de-date-informatice-forma-agravata-prevazuta-de-art-360-alin-3-cp/
[989] Ibidem.
[990] Ibidem.
[991] Ibidem.
[992] COMAN, Vasile. *Infracțiuni privind criminalitatea în cyberspațiu: practică judiciară recentă adnotată. Vol. I*. București: Universul Juridic, 2020, p. 320-328. 486 p. ISBN 978-606-39-0627-5.
[993] DOBRINOIU, Maxim. Accesul ilegal la poşta electronică. În: *Revista de Drept Penal*, 2008, nr. 3, pp. 122-125. ISSN 1223-0790.
[994] Ibidem.
[995] Ibidem.

online”[996]; „Există percepția eronată că atunci când se accesează un cont de email, de Facebook, Instagram etc. nu se accesează un sistem informatic ci un serviciu”[997]; „O asemenea concluzie este eronată având în vedere faptul că accesarea unui serviciu [...] implică un acces la sistemul informatic prin intermediul căruia respectivul serviciu este furnizat. [...]; [...]”.[998] Același autor susține: „Cu toate că rețelele de de socializare nu sunt sisteme informatice *per se,* acestea sunt stocate și furnizate prin intermediul unui sistem informatic.”[999]

În suita de sisteme informatice se disting așa-numitele „sisteme informatice subiacente”. Referitor la unul dintre acestea, G. Zlati afirmă: „Alte sisteme informatice relevante [...] sunt următoarele: [...] c) cartelele SIM (Subscriber Identity Module)”[1000]; „Cartelele SIM pot fi catalogate drept sisteme informatice. Deși este adevărat faptul că acestea pot prelucra date informatice *doar cu ajutorul unui alt sistem informatic”*[1001] *(de exemplu, un telefon)* (evid. ns.), cartela SIM conține inclusiv un mini procesor capabil să prelucreze date informatice non volatile. [...]; [...]”.[1002] În subpct. 3) pct. 3 din Regulamentul cu privire la furnizarea serviciilor de comunicații electronice accesibile publicului (Anexa la Hotărârea ANRCETI nr. 48 din 10.09.2013), este formulată următoarea definiție: „Cartelă SIM (Subscriber Identification Module) – cartela fizică (mini, micro sau nano-SIM) în care este încorporat un circuit integrat ce stochează informaţia despre IMSI (International Mobile Subscriber Identity)”[1003], „informaţia despre MSISDN (Mobile Station ISDN Number), informaţia relevantă autentificării şi criptării, setul de servicii la care utilizatorul final are acces, altă informaţie.”[1004] Din această definiție rezultă că, cu ajutorul telefonului în care este integrată, cartela SIM asigură prin executarea unui program prelucrarea automată a datelor informatice (și anume – a informaţiei despre IMSI, a informaţiei despre MSISDN, a informaţiei relevante autentificării şi criptării, a datelor privind

[996] ZLATI, George. *Percheziția informatică. Noțiuni de bază*. [citat 07.07.2022] Disponibil: https://www.universuljuridic.ro/perchezitia-informatica-notiuni-de-baza/
[997] Ibidem.
[998] Ibidem.
[999] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 71. 658 p. ISBN 978-606-8892-62-7.
[1000] ZLATI, George. *Percheziția informatică. Noțiuni de bază*. [citat 07.07.2022] Disponibil: https://www.universuljuridic.ro/perchezitia-informatica-notiuni-de-baza/
[1001] Ibidem.
[1002] Ibidem.
[1003] Hotărârea ANRCETI pentru aprobarea Regulamentului cu privire la furnizarea serviciilor de comunicații electronice accesibile publicului: nr. 48 din 10.09.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 258-261, 1695.
[1004] Ibidem.

setul de servicii la care utilizatorul final are acces, a altei informaţii). În aceste condiții, cartela SIM reprezintă un sistem informatic.[1005]

Privitor la un alt exemplu de sistem informatic subiacent, G. Zlati remarcă: „Un instrument de plată electronică, la fel precum un card SIM, poate deveni un sistem informatic”[1006] „doar atunci când este parte a unui ansamblu de dispozitive interconectate, putând la concret să prelucreze anumite date informatice”.[1007] În pct. 2 al Regulamentului cu privire la cardurile de plată (anexa nr. 1 la Hotărârea BNM nr. 157 din 01.08.2013 cu privire la aprobarea, modificarea, completarea şi abrogarea unor acte normative ale Băncii Naţionale a Moldovei), noțiunea „card de plată” este definită în felul următor: „un suport de informaţie standardizat şi, după caz, personalizat prin intermediul căruia deţinătorul, de regulă, cu utilizarea numărului personal de identificare al său”[1008] „şi/sau a unor alte coduri care permit identificarea sa, în funcţie de tipul cardului de plată are acces la distanţă la contul de plăţi”[1009] „la care este ataşat cardul de plată în vederea efectuării operaţiunilor de plată.”[1010] Din această definiție desprindem că, în măsura în care asigură prin executarea unui program prelucrarea automată a datelor informatice, cardul de plată reprezintă un sistem informatic. O asemenea ipoteză se atestă atunci când cardul de plată este introdus în bancomat, formând astfel un tandem cu acest sistem informatic.[1011]

Cardul de plată apare într-o dublă postură: sistem informatic *și* suport (mijloc) de stocare a datelor informatice. În această ordine de idei, este importantă precizarea lui G. Zlati: „Citirea ori copierea de date informatice stocate pe o cartelă SIM ori un instrument de plată electronică (card bancar)”[1012] „nu va reprezenta o interacțiune cu un sistem informatic, indiferent dacă acestea au sau nu un microprocesor”[1013] „ori dacă ar putea prelucra date informatice prin intermediul propriului sistem de operare. Interacțiunea, în această ipoteză, urmează să fie doar cu un mijloc de stocare a datelor informatice.”[1014] Sub acest aspect, este criticabilă următoarea definiție din

---

[1005] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[1006] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 85. 658 p. ISBN 978-606-8892-62-7.
[1007] Ibidem, p. 85.
[1008] Hotărârea BNM cu privire la aprobarea, modificarea, completarea şi abrogarea unor acte normative ale Băncii Naţionale a Moldovei: nr. 157 din 01.08.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 191-197, 1370.
[1009] Ibidem.
[1010] Ibidem.
[1011] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[1012] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 96. 658 p. ISBN 978-606-8892-62-7.
[1013] Ibidem, p. 96.
[1014] Ibidem, p. 96.

nota de la art. 176[1] CP RM din 1961: „Prin sistem computerizat se subînţeleg computerul, reţelele computerizate locale şi globale, *precum şi suporţii electronici ai informaţiei* (evid. ns.).”[1015]

Nu considerăm reușită abordarea propusă în Proiectul de lege pentru modificarea unor acte normative (modificarea Codului penal și Codului contravențional)[1016], publicat de către Ministerul Justiției. În acest proiect se propune ca definiția noțiunii de sistem informatic să fie formulată în alin. (1) art. 259 CP RM: „Accesul ilegal la sistem informatic, adică la dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură”[1017] „care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor”[1018], „de către o persoană care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării”[1019] „ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic ori să desfăşoare cercetări ştiinţifice”[1020] „sau să efectueze orice altă operaţiune într-un sistem informatic, dacă aceste acțiuni au cauzat daune considerabile.”[1021] V. Stati critică această inițiativă: „Prin aceasta se încalcă regula fixată la lit. d) alin. (1) art. 54 al Legii nr. 100/2017: „Textul proiectului actului normativ se elaborează în limba română, cu respectarea următoarelor reguli”[1022] „[...] noţiunea se redă prin termenul respectiv, evitându-se definiţia acesteia sau utilizarea frazeologică [...].”[1023] Dacă autorii Proiectului doresc să definească noțiunea „sistem informatic” [...], o pot face într-un articol din Capitolul XIII al părții speciale a Codului penal”.[1024] Nu putem să nu susținem aceste considerente.

După ce am analizat noțiunea „sistem informatic”, este necesar să examinăm noțiunea care se referă la un alt exemplu de obiect material secundar al infracțiunilor prevăzute la art. 259 CP RM.

[1015] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
[1016] *Proiectul de lege pentru modificarea unor acte normative (modificarea Codului penal și Codului contravențional) (533/MJ/2022)*. [citat 30.12.2022] Disponibil: https://cancelaria.gov.md/ro/content/privind-aprobarea-proiectului-de-lege-pentru-modificarea-unor-acte-normative-modificarea
[1017] Ibidem.
[1018] Ibidem.
[1019] Ibidem.
[1020] Ibidem.
[1021] Ibidem.
[1022] Legea cu privire la actele normative: nr. 100 din 22.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 7-17, 34.
[1023] Ibidem.
[1024] STATI, Vitalie. Despre „interesul public”, „daunele considerabile” și nu numai: analiza unui proiect de amendare a Codului penal al Republicii Moldova. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4188261

Astfel, *rețeaua informatică* reprezintă principalul instrument care asigură circulația datelor informatice. Cea mai cunoscută rețea informatică este, desigur, Internetul. Prin intermediul acestei rețele informatice globale, sute de milioane de utilizatori transmit și recepționează date informatice. Pentru a înțelege mai bine rolul și locul noțiunii „rețea informatică" în „arhitectura" infracțiunilor prevăzute la art. 259 CP RM, este necesar să analizăm definițiile normative și doctrinare ale acestei noțiuni.[1025]

Înainte de a examina definițiile respective, este cazul că stabilim legătura dintre sistemul informatic și rețeaua informatică.

Din nota la art. 176[1] CP RM din 1961 rezultă că rețeaua informatică este parte a sistemului informatic: „Prin sistem computerizat se subînţeleg computerul, *reţelele computerizate locale şi globale* (evid. ns.), precum şi suporţii electronici ai informaţiei".[1026] Bineînțeles, noțiunea „rețea informatică" și „sistem informatic" nu se pot afla într-o relație de tip „parte – întreg". Suntem de acord cu G. Zlati, care susține: „O rețea (LAN, WAN, WiFi etc.) nu intră în accepțiunea noțiunii de „sistem informatic""[1027]; „Prin intermediul acesteia se poate stabili o legătură între două sau mai multe sisteme informatice, fără a deveni ea însăși un sistem informatic".[1028] În legătură cu definiția noțiunii „sistem informatic" din Legea României nr. 161/2003, același autor afirmă: „Definiţia oferită de art. 35 alin. (1) lit. a) este susceptibilă de critică"[1029]; „Şi aceasta deoarece, textul face trimitere şi la ideea de ansamblu de dispozitive interconectate sau aflate într-o relaţie funcţională"[1030]; „Ori, s-ar putea crede că, din moment ce Internetul este o reţea, putem discuta despre un ansamblu de dispozitive interconectate"[1031]; „Acest raţionament este însă unul eronat. Internetul, este mediul de comunicare"[1032], „capabil să ofere acces la sistemele informatice din cadrul acestuia (spre exemplu, un site *web*) şi în niciun caz un sistem informatic".[1033] Considerăm că, în definiția noțiunii „sistem informatic", prin „ansamblu de dispozitive interconectate sau aflate într-o relaţie funcţională" se are în vedere „ansamblul de tip calculator –

[1025] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale", 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[1026] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
[1027] ZLATI, George. *Tratat de criminalitate informatică. Vol. I.* București: Solomon, 2020, p. 31. 658 p. ISBN 978-606-8892-62-7.
[1028] Ibidem, p. 31.
[1029] ZLATI, George. *Secția penală a I.C.C.J. și sistemele informatice*. [citat 07.07.2022] Disponibil: https://www.penalmente.eu/2011/11/02/sectia-penala-i-c-c-j-si-sistemele-informatice/
[1030] Ibidem.
[1031] Ibidem.
[1032] Ibidem.
[1033] Ibidem.

periferice [...]”.[1034] O rețea, formată din două ori mai multe calculatoare, constituie o rețea informatică, nu un sistem informatic.

O asemenea interpretare este conformă cu următoarea definiție din art. 2 al Legii nr. 1069/2000: „reţea informatică (reţea de calculatoare) – ansamblu de noduri de prelucrare a datelor interconectate în scopul transportului de date”.[1035] Această definiție trebuie comparată cu alta din același articol: „sistem informatic – ansamblul de programe şi echipamente care asigură prelucrarea automată a datelor”.[1036]

Faptul că noțiunile „rețea informatică” și „sistem informatic” nu trebuie confundate rezultă și din definiția formulată în subpct. 7) pct. 2 din Hotărârea Guvernului nr. 811 din 29.11.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020: „infrastructuri cibernetice – infrastructuri din domeniul tehnologiei informației și comunicației, constând din sisteme informatice, aplicații aferente, rețele și servicii de comunicații electronice”.[1037] Așadar, atât sistemele informatice, cât și rețelele informatice (electronice) reprezintă exemple distincte de infrastructuri cibernetice. Interpretarea dată este conformă cu cea din pct. 24 din Raportul explicativ la Convenția de la Budapesta: „Rețea este interconexiunea dintre două ori mai multe sisteme informatice”[1038]; „Conexiunile pot fi la sol (de exemplu, fir sau cablu), fără fir (de exemplu, radio, infraroșu sau satelit) sau ambele”[1039]; „O rețea poate fi limitată geografic la o zonă mică (rețele locale) sau se poate întinde pe o zonă mare (rețele cu zonă largă)”[1040], „iar astfel de rețele pot fi ele însele interconectate. Internetul este o rețea globală formată din multe rețele interconectate, toate folosind aceleași protocoale”[1041]; „Există și alte tipuri de rețele, indiferent dacă sunt sau nu conectate la Internet, capabile să comunice date informatice între sisteme informatice”[1042]; „Sistemele informatice pot fi conectate la rețea ca puncte terminale sau ca mijloace adjuvante în vederea asigurării comunicării în rețea. Este esențial ca schimbul de date informatice să se facă prin rețea.”[1043]

[1034] DOBRINOIU, Maxim. Accesul ilegal la poşta electronică. În: *Revista de Drept Penal*, 2008, nr. 3, pp. 122-125. ISSN 1223-0790.
[1035] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[1036] Ibidem.
[1037] Hotărârea Guvernului cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020: nr. 811 din 29.11.2015. În: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 306-310, 905.
[1038] *Explanatory Report to the Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/16800cce5b
[1039] Ibidem.
[1040] Ibidem.
[1041] Ibidem.
[1042] Ibidem.
[1043] Ibidem.

Observăm că, în pct. 24 din Raportul explicativ la Convenția de la Budapesta, se face distincție dintre rețeaua informatică și sistemul informatic. În mod aparent, în art. 2 al Convenției de la Budapesta, se vorbește despre „accesarea intenţionată şi fără drept a ansamblului ori a unei părţi a unui sistem informatic”.[1044] Astfel, s-ar putea interpreta că, în acest mod, dispoziția art. 2 al Convenției de la Budapesta a deviat de la Recomandarea Comitetului de Miniştri al Consiliului Europei nr. R(89)9 referitoare la criminalitatea în legătură cu utilizarea calculatorului, în care se sugerează incriminarea „accesului ilegal la un sistem computerizat sau la o rețea computerizată prin încălcarea măsurilor de securitate”.[1045] Totuși, în art. 2 al Convenției de la Budapesta se mai specifică: „[...] O parte poate condiţiona o astfel de incriminare de comiterea încălcării respective prin violarea măsurilor de securitate, cu intenţia de a obţine date informatice ori cu altă intenţie delictuală”[1046], „*sau de legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic* (evid. ns.)”.[1047] În acest fel, art. 2 al Convenției de la Budapesta sugerează, deși indirect, necesitatea de a incrimina accesul ilegal nu doar la un sistem informatic, ci și la o rețea informatică.

Distincția dintre rețeaua informatică și sistemul informatic – relevată direct sau indirect în art. 2 al Convenției de la Budapesta, în pct. 24 din Raportul explicativ la Convenția de la Budapesta, precum și în Recomandarea Comitetului de Miniştri al Consiliului Europei nr. R(89)9 referitoare la criminalitatea în legătură cu utilizarea calculatorului – trebuie menținută în continuare în art. 259 CP RM.[1048]

În Codul penal în vigoare al Republicii Moldova lipsește definiția noțiunii de rețea informatică. În alte state, în legile penale există astfel de definiții (de exemplu, în pct. 25 art. 93 CP RBu[1049], alin. (1) art. 337B CP RMa[1050], în alin. (3) § 5-41-102 din Codul penal al statului Arkansas[1051] și în art. 205.4745 din Codul penal al statului Nevada[1052]). Din analiza acestor definiții rezultă că rețeaua informatică se poate exprima nu doar în 1) ansamblul format din două

[1044] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[1045] *Recommendation No.R.(89)9 of the Committee of the Ministers to Member States on Computer-related Crime*. [citat 07.07.2022] Disponibil: http://www.cm.coe.int/ta/rec/1989/ 89r9.htm
[1046] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[1047] Ibidem.
[1048] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[1049] *Codul penal al Republicii Bulgaria*. [citat 09.07.2022] Disponibil: https://codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[1050] *Codul penal al Republicii Malta*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Malta-RO.html
[1051] *2010 Arkansas Code. Title 5 – Criminal Offenses*. [citat 06.03.2022] Disponibil: https://law.justia.com/codes/arkansas/2010/title-5/subtitle-4/chapter-41/subchapter-1/5-41-102/
[1052] *2009 Nevada Code. Title 15 – Crimes and punishments*. [citat 06.03.2022] Disponibil: https://law.justia.com/codes/nevada/2009/title-15/chapter-205/unlawful-acts-regarding-computers-and-information-services/

sau mai multe calculatoare interconectate care oferă posibilitatea realizării unui schimb de date informatice, ci și în 2) interconexiunea dintre liniile şi circuitele de comunicare cu un calculator, printr-un dispozitiv aflat la distanţă, care oferă posibilitatea realizării unui schimb de date informatice.[1053] Apar semne de întrebare în legătură cu cel de-al doilea tip de rețea informatică. Considerăm că, pentru a înțelege sensul sintagmei „interconexiunea dintre liniile şi circuitele de comunicare cu un calculator, printr-un dispozitiv aflat la distanţă, care oferă posibilitatea realizării unui schimb de date informatice", este util să apelăm la următoarele clarificări de ordin terminologic: „Conectivitatea este asigurată de echipamente de reţea (*hub*-uri, *switch*-uri, routere, puncte de acces *wireless*)"[1054]; „Transmisia datelor se realizează prin medii de transmisie care pot fi: conductoare de cupru – pentru transmisia datelor sub formă de semnale electrice"[1055]; „fibră optică – din fibre de sticlă sau materiale plastice – pentru a transporta datele sub formă de impulsuri luminoase"[1056]; „medii de transmisie a datelor fără fir – transmit datele sub formă de unde radio, microunde, raze infraroşii sau raze laser – în cadrul conexiunilor fără fir *(wireless)*".[1057]

Din acest punct de vedere, definițiile doctrinare, prezentate mai jos, sunt prea înguste. Din ele rezultă că, prin „rețea informatică" trebuie să se înțeleagă doar ansamblul format din două ori mai multe calculatoare interconectate care oferă posibilitatea realizării unui schimb de date informatice. Astfel, T. Anghel folosește nu noțiunea „rețea informatică", ci noțiunea „rețea de calculatoare *(computer network)*", prin care înțelege „ansamblul de calculatoare autonome interconectate, capabile să comunice unele cu altele folosind canale de comunicație (medii de transmisie)".[1058] De asemenea, R.-L. Lupșa vorbește despre „rețeaua de calculatoare", prin care înțelege „un sistem [...] care interconectează niște calculatoare, permițând unor programe ce se execută pe aceste calculatoare să comunice între ele".[1059] Păreri similare exprimă A.N. Popov[1060] și V.V. Strigunov.[1061]

[1053] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale", 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[1054] *Note de curs – Introducere în reţelele de calculator*. [citat 09.07.2022] Disponibil: https://www.afahc.ro/ro/facultate/cursuri/retele_note_curs.pdf
[1055] Ibidem.
[1056] Ibidem.
[1057] Ibidem.
[1058] ANGHEL, Traian. *Dicționar de informatică*. București: Corint Books, 2017, p. 325. 447 p. ISBN 978-606-793-178-5.
[1059] LUPȘA, Radu-Lucian. *Rețele de calculatoare. Principii*. [citat 08.07.2022] Disponibil: https://www.cs.ubbcluj.ro/~rlupsa/works/retele.pdf
[1060] ПОПОВ, А.Н. О предмете преступления, предусмотренного ст. 272 УК РФ. În: *Криминалистъ*, 2008, № 1, с. 5-10. ISSN 2686-7753.
[1061] СТРИГУНОВ, В.В. *Введение в компьютерные сети*. Хабаровск: Изд-во Тихоокеан. гос. ун-та, 2016, с. 7. 103 с. ISBN 978-5-7389-1860-5.

Noțiunea „rețea informatică” nu trebuie limitată la sensul de „rețea de calculatoare”. De exemplu, Internetul lucrurilor (sau, altfel spus, Internetul obiectelor) reprezintă o reţea de dispozitive (televizor inteligent, frigider inteligent, cafetieră inteligentă etc.) ce pot fi conectate între ele şi/sau la Internet, astfel încât să poată procesa date. D. Savu, M. Tomescu și L. Băjenaru menționează: „Internetul lucrurilor (Internet of Things – IoT) este un concept care defineşte o lume în care toate obiectele (maşini, electrocasnice, sisteme de iluminat, dispozitive mobile, portabile etc.)”[1062] „sunt conectate între ele prin intermediul Internetului. Internetul lucrurilor nu se bazează numai pe calculatoare ca să existe”[1063]; „Fiecare obiect, chiar şi corpul uman[1064], poate deveni o parte din Internetul lucrurilor dacă este echipat cu anumite componente electronice”[1065]; „Aceste părţi variază cu siguranţă, în funcţie de ce trebuie să efectueze obiectul, dar se încadrează în două mari categorii”[1066]: „obiectul trebuie să fie capabil să captureze date, de obicei, prin intermediul senzorilor”[1067]; „obiectul trebuie să fie în măsură să transmită aceste date în altă parte prin intermediul Internetului.”[1068]

Continuând ideea, este necesar să menționăm că noțiunea „rețea informatică” se intersectează cu noțiunea „rețea de comunicații electronice”. Conform art. 2 al Legii nr. 241 din 15.11.2007 a comunicaţiilor electronice, prin „reţea de comunicaţii electronice” se înțelege „sistemele de transmisie şi, după caz, echipamentele de comutare sau rutare”[1069], „precum şi alte resurse care permit transmiterea semnalelor prin suport fizic, electromagnetic sau prin orice alte mijloace”[1070], „incluzând reţele de comunicaţii prin satelit, reţele fixe (cu comutare de circuite sau comutare de pachete, inclusiv Internet) şi reţele mobile terestre”[1071], „reţele de transport al energiei electrice, în cazul în care acestea sunt utilizate şi pentru transmiterea semnalelor”[1072], reţele utilizate pentru difuzarea programelor audiovizuale, reţele de televiziune prin cablu, indiferent de tipul informaţiei transmise”.[1073] Definiții aproape identice ale noțiunii „rețea de comunicații electronice” sunt formulate în art. 1 al Directivei 2002/77/CE a Comisiei din

---

[1062] SAVU, Daniel, TOMESCU, Mihaela, BĂJENARU, Lidia. Internetul lucrurilor – o nouă paradigmă a conectării în Internet. În: *Revista Română de Informatică şi Automatică*, 2017, vol. 27, nr. 1, pp. 5-14. ISSN 1841-4303.
[1063] Ibidem.
[1064] În acest sens, putem vorbi despre: stimulatoare cardiace inteligente; implanturi cohleare inteligente; lentile inteligente; pastile inteligente, etc.
[1065] SAVU, Daniel, TOMESCU, Mihaela, BĂJENARU, Lidia. Internetul lucrurilor – o nouă paradigmă a conectării în Internet. În: *Revista Română de Informatică şi Automatică*, 2017, vol. 27, nr. 1, pp. 5-14. ISSN 1841-4303.
[1066] Ibidem.
[1067] Ibidem.
[1068] Ibidem.
[1069] Legea comunicaţiilor electronice: nr. 241 din 15.11.2007. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 51-54, 155.
[1070] Ibidem.
[1071] Ibidem.
[1072] Ibidem.
[1073] Ibidem.

16.09.2002 privind concurența pe piețele de rețele și servicii de comunicații electronice[1074] și în art. 2 al Directivei (UE) 2018/1972 a Parlamentului European și a Consiliului din 11.12.2018 de instituire a Codului european al comunicațiilor electronice.[1075] Observăm că destinația unei rețele de comunicații electronice este transmiterea semnalelor sau difuzarea programelor audiovizuale.

Obiectul material secundar al infracțiunilor prevăzute la art. 259 CP RM îl reprezintă, printre altele, calculatorul.

Noțiunea de calculator (computer) nu este definită în legislația Republicii Moldova. În alte state, o asemenea noțiune este definită chiar în legea penală (spre exemplu, în alin. (1) art. 337B CP RMa[1076], în alin. (2) § 5-41-102 Codul penal al statului Arkansas[1077] și în art. 205.4735 din Codul penal al statului Nevada[1078]). Din aceste definiții legislative, care nu se deosebesc mult una de cealaltă, aflăm că se consideră calculator dispozitivul electronic care: 1) îndeplinește funcții logice, aritmetice sau de memorie; 2) presupune manipularea de impulsuri electronice sau magnetice pentru îndeplinirea oricăreia dintre aceste funcții; 3) include echipamente legate într-un sistem sau o rețea.[1079]

Definițiile doctrinare ale noțiunii de calculator ne ajută să deslușim alte caracteristici ale dispozitivului electronic analizat. Astfel, după T. Anghel, „calculator (computer), denumit și sistem de calcul *(computer sistem)*, este o mașină capabilă să accepte date structurate (ca intrări)”[1080], „să le prelucreze conform unei liste de instrucțiuni numită program și să furnizeze rezultatele (ca ieșiri)”.[1081] L. Vasiu exprimă părerea că „un calculator este compus din partea de echipament (numită şi hardware) şi un set de programe informatice. Majoritatea sistemelor sunt

---

[1074] *Directiva 2002/77/CE a Comisiei din 16.09.2002 privind concurența pe piețele de rețele și servicii de comunicații electronice*. [citat 07.07.2022] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0077&from=RO

[1075] *Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11.12.2018 de instituire a Codului european al comunicațiilor electronice*. [citat 07.07.2022] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32018L1972&from=en

[1076] *Codul penal al Republicii Malta*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Malta-RO.html

[1077] *2010 Arkansas Code. Title 5 – Criminal Offenses*. [citat 06.03.2022] Disponibil: https://law.justia.com/codes/arkansas/2010/title-5/subtitle-4/chapter-41/subchapter-1/5-41-102/

[1078] *2009 Nevada Code. Title 15 – Crimes and punishments*. [citat 06.03.2022] Disponibil: https://law.justia.com/codes/nevada/2009/title-15/chapter-205/unlawful-acts-regarding-computers-and-information-services/

[1079] STRÎMBEANU, Alexandru. Calculatorul – obiect material al infracțiunilor prevăzute la art. 259 din Codul penal. În: *Conferința științifică națională cu participare internațională „Integrare prin cercetare și inovare”, dedicată Zilei internaționale a Științei pentru pace și Dezvoltare (10-11 noiembrie 2022)*. Chișinău: CEP USM, 2022, pp. 69-71. ISBN 978-9975-152-48-8.

[1080] ANGHEL, Traian. *Dicționar de informatică*. București: Corint Books, 2017, p. 59-60. 447 p. ISBN 978-606-793-178-5.

[1081] Ibidem, p. 59-60.

realizate dintr-un număr de subsisteme”[1082]; „Un calculator poate fi văzut, din punct de vedere al echipamentului (hardware), ca un sistem”[1083] „constând din cinci subsisteme funcţionale – intrare (input), control, procesare aritmetică şi logică, memorie şi ieşire (output)”.[1084] Puncte de vedere asemănătoare au N. Niță și V. Dobrin[1085], V.N. Loktiuhin[1086], O.Ia. Baev și V.A. Meșcereakov.[1087]

Calculatorul este nu doar un sistem de calcul, ci și un sistem informatic. G. Zlati afirmă: „Sistemul informatic este: 1. un dispozitiv 2. ce asigură prelucrarea automată a datelor 3. cu ajutorul unui program informatic”[1088]; „Spre exemplu, este evident că un computer corespunde acestei definiţii”.[1089] Această viziune își găsește confirmarea în definiția din art. 2 al Legii nr. 20/2009: „sistem informatic – orice dispozitiv izolat sau ansamblu de dispozitive interconectate”[1090] „ori aflate în legătură care asigură ori dintre care unul sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor”.[1091] Fără doar și poate, calculatorul este un dispozitiv care asigură, prin executarea unui program, prelucrarea automată a datelor.

Aceste considerente ne determină să punem la îndoială oportunitatea prezenței în dispoziția de la alin. (1) art. 259 CP RM a sintagmelor „informaţia din calculatoare” și „dereglarea funcţionării calculatoarelor”, odată ce în aceeași dispoziție sunt prezente sintagmele „informaţia din [...] sistemul informatic” și „dereglarea funcţionării [...] sistemului informatic”. Comparația cu dispozițiile similare din unele legi penale străine face ca această îndoială să devină mai mare: „Cel care, ca urmare a comiterii uneia din infracţiunile prevăzute la § 1, împiedică, integral sau parţial”[1092], „*funcţionarea corectă a sistemului informatic* (evid. ns.) în cauză sau a oricărui alt

---

[1082] VASIU, Lucian. *Informatică juridică şi drept informatic. Suport de curs pentru frecvență redusă*. [citat 06.03.2022] Disponibil: file.ucdc.ro/cursuri/8_4_dt4752_Informatica_juridica_Vasiu_Lucian.pdf
[1083] Ibidem.
[1084] Ibidem.
[1085] NIȚĂ, Nelu, DOBRIN, Vasile. *Principalele forme de manifestare a criminalităţii informatice în contextul actual al dezvoltării tehnologice şi al globalizării*. [citat 04.07.2022] Disponibil: https://www.universuljuridic.ro/principalele-forme-de-manifestare-a-criminalitatii-informatice-in-contextul-actual-al-dezvoltarii-tehnologice-si-al-globalizarii/
[1086] ЛОКТЮХИН, В.Н. *Архитектура компьютера. Кн.1: Структура персонального компьютера*. Рязань: Ряз. гос. ун-т им. С.А. Есенина, 2008, с. 5. 136 с. ISBN 978-5-88006-549-3.
[1087] БАЕВ, О.Я., МЕЩЕРЯКОВ, В.А. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации. În: *Защита информации. Конфидент*, 1998, № 7, с. 8-9. ISSN 2413-3582.
[1088] ZLATI, George. *Art. 35 din Legea 161/2003 – problematica definiţiilor*. [citat 06.03.2022] Disponibil: https://www.penalmente.eu/2011/06/03/art-35-din-legea-1612003-problematica-definitiilor/
[1089] Ibidem.
[1090] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.
[1091] Ibidem.
[1092] *Codul penal al Regatului Belgiei*. [citat 04.07.2022] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html

sistem informatic [...]”[1093] (§ 3 art. 550ter CP RBl); „Împiedicarea sau modificarea funcţionării unui sistem de prelucrare automată de date (evid. ns.) [...]”[1094] (art. 323-2 CP RFr); „Persoana care, prin orice mijloc, fără autorizaţie şi în mod grav, *împiedică sau întrerupe funcţionarea unui sistem informatic* (evid. ns.)”[1095] „care are legătură cu un altul, prin introducerea, transmiterea, distrugerea, ştergerea, deteriorarea, alterarea, eliminarea sau facerea datelor informatice inaccesibile, dacă rezultatul produs este grav [...]”[1096] (alin. 2 art. 264 CP RSp).

2.1.3. Victima infracțiunilor prevăzute la art. 259 CP RM

În doctrina penală română sunt utilizate noțiunile „subiect activ al infracțiunii” și „subiect pasiv al infracțiunii”. O astfel de abordare are la bază următorul înțeles al noțiunii generice de subiect al infracțiunii: „persoană fizică sau juridică care a săvârșit sau a participat la săvârșirea infracțiunii, precum și persoana asupra căreia se răsfrânge urmarea infracțiunii”.[1097] Fundamentul conceptual al unui astfel de înțeles îl constituie noțiunea „raport juridic penal” cu următoarea semnificație: „raport juridic de conflict (de contradicție) izvorât din săvârșirea unei infracțiuni”[1098]; „Părțile acestui raport sunt subiectul (sau subiecții) activ (persoana sau persoanele care au săvârșit infracțiunea în calitate de autori, instigatori sau complici”[1099], „o infracțiune fapt consumat sau o tentativă), pe de o parte, și subiectul pasiv general al infracțiunii, care este statul ca reprezentant al societății”.[1100]

Fără a pune la îndoială temeinicia utilizării noțiunii „raport juridic penal”, atragem atenția asupra faptului că concepția dihotomică a subiectului infracțiunii nu este consacrată în legea penală autohtonă.[1101] Or, în art. 21 CP RM, prin „subiect al infracțiunii” se are în vedere doar persoana care săvârșește infracțiunea. Aceeași idee rezultă implicit din alin. (6) art. 42 CP RM: „Participanţii trebuie să întrunească semnele subiectului infracţiunii”. În aceste condiții,

---

[1093] Ibidem.
[1094] *Codul penal al Republicii Franceze*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Franta-RO.html
[1095] *Codul penal al Regatului Spaniei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Spania-RO.html
[1096] *Codul penal al Regatului Spaniei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Spania-RO.html
[1097] UDROIU, Mihail. *Dicționar de drept penal și de procedură penală*. București: C.H. Beck, 2009, p. 381. 437 p. ISBN 978-973-115-425-1.
[1098] BOROI, Alexandru, GORUNESCU, Mirela, POPESCU, Mihaela. *Dicționar de drept penal*. București: All Beck, 2004, p. 337. 417 p. ISBN 973-655-425-X.
[1099] Ibidem, p. 337.
[1100] Ibidem, p. 337.
[1101] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

considerăm lipsită de suport normativ recurgerea, în procesul de analiză a infracțiunilor prevăzute de Codul penal al Republicii Moldova, a noțiunilor „subiect activ al infracțiunii” și „subiect pasiv al infracțiunii”.[1102] Până la o eventuală modificare/completare a Codului penal al Republicii Moldova, în dreptul penal al Republicii Moldova prin „subiect al infracțiunii” se are în vedere doar persoana care comite infracțiunea, nu și persoana asupra căreia se comite infracțiunea. A înfățișa lucrurile altfel înseamnă a prezenta aspectul *„de lege ferenda”* în calitate de aspect *„de lege lata”* și, în consecință, a genera erori care pot influența calitatea aplicării legii penale.[1103]

Conceptul de victimă a infracțiunii este folosit în mai multe norme din Codul penal al Republicii Moldova (de exemplu: lit. g) alin. (1) art. 76; lit. e) și h) alin. (1) art. 77; lit. d), e) și n) alin. (2) art. 145; art. 146; art. 148, etc.). În toate aceste cazuri, prin „victimă a infracțiunii” se are în vedere persoana fizică sau persoana juridică asupra căreia este săvârșită infracțiunea.[1104]

I. Moscalciuc argumentează de ce victima infracțiunii face parte din sistemul obiectului infracţiunii: „Dauna cauzată victimei, ca subiect al relaţiilor sociale apărate de legea penală, face parte din urmările prejudiciabile ale infracţiunii, dar nu în întregime”[1105]; „Se are în vedere numai componenta socială a daunei respective. Astfel, victimei poate să-i fie cauzată vătămarea integrităţii corporale sau a sănătăţii, să-i fie distruse sau deteriorate bunurile etc.”[1106]; „În acest caz, componenta socială a daunei constă în crearea imposibilităţii pentru victimă de a-şi îndeplini obligaţiile de muncă”[1107], „de a se bucura de posibilitatea de a participa activ la viaţa socială, ori în privarea acesteia de posibilitatea de a-şi exercita deplin drepturile de proprietar sau posesor”[1108]; „Prin intermediul acestei componente sociale a daunei se stabileşte legătura dintre victimă şi obiectul juridic special al infracţiunii.”[1109] Păreri similare au R. Berdilo[1110], A. Păduraru și B. Giurcă.[1111] Din analiza acestor opinii poate fi dedusă concluzia că victima

---

[1102] A se vedea, de exemplu: JENUNCHI, Elena. *Răspunderea penală pentru constrângerea de a face declarații*: tz. de doct. în drept. Chișinău, 2020, p. 28, 59. 182 p.; STRATAN, Andrei. Calitatea victimei în cadrul infracțiunilor prevăzute la art. 238 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale”*, 2020, nr. 3, pp. 198-203. ISSN 1814-3199; DASCĂLU, Beatrice Daiana. Subiecții infracțiunii de violență în familie. În: *Legea și Viața*, 2017, nr. 4, pp. 43-45. ISSN 2587-4373.

[1103] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

[1104] Ibidem.

[1105] MOSCALCIUC, Irina. Consumatorul – victima infracţiunilor săvârşite în sfera consumului de produse şi servicii. În: *Revista Naţională de Drept*, 2007, nr. 5, pp. 47-53. ISSN 1811-0770.

[1106] Ibidem.

[1107] Ibidem.

[1108] Ibidem.

[1109] Ibidem.

[1110] BERDILO, Rodica. Victima omorului săvârșit în stare de afect. În: *Revista Institutului Naţional al Justiţiei*, 2021, nr. 1, pp. 33-38. ISSN 1857-2405.

[1111] GIURCĂ, Bogdan. Elementele constitutive ale infracțiunii în lumina noului Cod penal. În: *Politica legislativă între reglementare europeană, naţională şi internaţională: noi perspective ale dreptului / Conferinţa Internaţională*

infracțiunilor prevăzute la art. 259 CP RM este persoana (fizică sau juridică) care participă la relațiile sociale ocrotite împotriva acestor infracțiuni.[1112] Suntem de acord cu Gh. Gladchi care afirmă: „Trăsăturile caracteristice personalității victimei cuprinse în componența infracțiunii [...], sunt indisolubil legate de caracterul obiectului infracțiunii asupra căruia este îndreptată fapta socialmente periculoasă”.[1113] Rezultă că trebuie să stabilim caracteristicile persoanei (fizice sau juridice) care participă la relațiile sociale apărate împotriva infracțiunilor prevăzute la art. 259 CP RM.

Ab initio, trebuie să precizăm că statul nu poate fi victimă a infracțiunilor prevăzute la art. 259 CP RM, în particular, și a infracțiunilor prevăzute de Codul penal al Republicii Moldova, în general.[1114] I. Selevestru afirmă în mod întemeiat: „Ar fi impropriu ca, din postura de victimă a infracțiunii, statul să-și exercite calitatea de apărător al ordinii de drept”[1115]; „Un stat, care evoluează în această postură, este un stat care se declară incapabil de a-și apăra cetățenii împotriva infracțiunilor. Este un stat ca și cum inexistent”.[1116]

În alin. 4 art. 2 din Carta ONU se menționează: „[...] toţi membrii Organizaţiei se vor abţine, în relaţiile lor internaţionale de a recurge la ameninţarea cu forța”[1117] „sau la folosirea ei fie împotriva integrităţii teritoriale ori independenței politice a vreunui stat fie în orice alt mod incompatibil cu scopurile Naţiunilor Unite”.[1118] În opinia lui A.-N. Popescu, un atac cibernetic (care poate presupune accesul ilegal la informaţia computerizată) poate exprima conținutul noțiunii de folosire a forței în sensul alin. 4 art. 2 din Carta ONU.[1119] În condițiile în care atacul cibernetic (care poate presupune accesul ilegal la informaţia computerizată) corespunde noțiunii de folosire a forței în sensul alin. 4 art. 2 din Carta ONU, statul atacat nu este victimă în sensul dreptului penal al Republicii Moldova. Într-un asemenea caz, victime pot fi persoanele (fizice sau juridice) care participă la relațiile sociale apărate împotriva infracțiunilor prevăzute la art.

---

de Drept, Studii Europene şi Relaţii Internaţionale (Bucureşti, 24-25 mai 2013). Bucureşti: Hamangiu, 2013, pp. 286-296. ISBN 978-606-678-642-3.

[1112] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

[1113] GLADCHI, Gheorghe. Obiectul material al infracțiunii și victima infracțiunii. În: *Reabilitarea victimelor infracțiunii: Conferința științifico-practică națională dedicată aniversării a 75 de ani de la fondarea Universității de Stat din Moldova (Chișinău, 22 octombrie 2021)*. Chişinău: CEP USM, 2022, pp. 70-76. ISBN 978-9975-159-02-9.

[1114] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

[1115] SELEVESTRU, Irina. Victima infracţiunilor prevăzute la art. 191 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale”*, 2015, nr. 3, pp. 194-199. ISSN 1814-3199.

[1116] Ibidem.

[1117] *United Nations Charter*. [citat 11.07.2022] Disponibil: https://www.un.org/en/about-us/un-charter

[1118] Ibidem.

[1119] POPESCU, Adrian-Nicușor. *Atacul cibernetic și principiul interzicerii folosirii forței*. [citat 11.07.2022] Disponibil: https://www.universuljuridic.ro/atacul-cibernetic-si-principiul-interzicerii-folosirii-fortei/

259 CP RM. Statul atacat poate fi considerat victimă numai în sensul dreptului penal internațional.[1120]

După această paranteză, consemnăm că infracțiunile prevăzute la art. 259 CP RM sunt biobiectuale, presupunând prezența obiectului juridic principal și a obiectului juridic secundar. Din perspectiva obiectului juridic principal al infracțiunilor prevăzute la art. 259 CP RM, victimă a acestor infracțiuni este persoana fizică sau persoana juridică care participă la relaţiile sociale cu privire la accesul autorizat sau permis la informaţia computerizată. Urmează să stabilim caracteristicile unor astfel de persoane.[1121]

În opinia lui E. Muradov, „în funcție de modul de circumstanțiere a calității subiectului special în dispoziția incriminatoare, pot fi deosebite următoarele tipuri de infracțiuni economice: 1) infracţiunile economice ai căror subiecţi nu au semne speciale”[1122]; „2) infracţiunile economice ai căror subiecţi au semne speciale direct indicate în textul legii penale”[1123]; „3) infracţiunile economice ai căror subiecţi au semne speciale care nu sunt indicate direct în textul legii penale, dar care decurg din acesta”.[1124] Făcând o paralelă, se poate afirma că există infracţiuni ai căror victime posedă semne speciale care nu sunt indicate direct în textul legii penale, dar care decurg din acesta. Teza dată o demonstrează, de pildă, art. 360 CPR, în care victima infracțiunii nu este descrisă în niciun fel.[1125]

Acțiunea, descrisă în art. 360 CPR, este asemănătoare cu acțiunea principală descrisă în art. 259 CP RM. Datorită acestui fapt, obiectul juridic special al infracțiunii prevăzute la art. 360 din Codul penal al României are un conținut similar cu cel al obiectului juridic principal al infracțiunilor prevăzute la art. 259 CP RM. O asemenea similaritate ne poate ajuta la stabilirea caracteristicilor persoanei (fizice sau juridice) care participă la relaţiile sociale apărate în principal împotriva infracțiunilor prevăzute la art. 259 CP RM.[1126]

Părerile doctrinarilor români cu privire la victima infracțiunii, prevăzute la art. 360 CPR, sunt divizate. De exemplu, P. Tamas-Erno consideră că orice persoană poate fi victimă a acestei infracțiuni.[1127] O altă părere aparține unui grup relativ numeros de autori care consideră că

[1120] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.
[1121] Ibidem.
[1122] МУРАДОВ, Э. Признаки специального субъекта как критерий классификации преступлений в сфере экономической деятельности. În: *Уголовное право*, 2003, № 4, с. 51-52. ISSN 2071-5870.
[1123] Ibidem.
[1124] Ibidem.
[1125] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.
[1126] Ibidem.
[1127] TAMAS-ERNO, Peter. Accesarea ilegală a conturilor de Facebook privit din perspectiva dreptului penal. În*: Revista Facultății de Drept Oradea*, 2019, nr. 1, pp. 151-157. ISSN 1582-7585.

persoana fizică sau juridică, care este deţinătoarea legitimă (de drept) a sistemului informatic, evoluează ca victimă a infracțiunii prevăzute la art. 360 CPR.[1128] Fără doar și poate, toate aceste opinii (mai puțin cea exprimată de P. Tamas-Erno) ne ajută să stabilim caracteristicile persoanei (fizice sau juridice) care participă la relaţiile sociale protejate în principal împotriva infracțiunilor prevăzute la art. 259 CP RM. În replică la cele afirmate de către P. Tamas-Erno, nu oricare persoană poate fi titulara valorii sociale apărate împotriva infracțiunii prevăzute la art. 360 CPR. Sistemul informatic, accesat ilegal în contextul acestei infracțiuni, nu poate aparține oricărei persoane. Așa cum rezultă din majoritatea părerilor doctrinarilor români, pe care le-am consemnat mai sus, victimă a infracțiunii prevăzute la art. 360 CPR trebuie considerată persoana care deține dreptul la protecția sistemului informatic împotriva accesului ilegal la acesta. Anume aceasta trebuie să fie vectorul spre care va fi orientat demersul nostru de stabilire a caracteristicilor persoanei fizice sau ale persoanei juridice care participă la relaţiile sociale apărate în principal împotriva infracțiunilor prevăzute la art. 259 CP RM.[1129]

Desigur, textul dispoziției art. 259 CP RM nu coincide cu textul dispoziției art. 360 CPR. Ca urmare, detaliile privind caracteristicile persoanelor în cauză urmează a fi identificate în corespundere cu legislația Republicii Moldova. Subliniem că, atunci când spunem „legislația Republicii Moldova”, avem în vedere nu doar art. 259 CP RM, ci și normele extrapenale la care face referire acest articol.[1130] Or, în Hotărârea nr. 25 din 13.10.2015 pentru controlul constituţionalităţii unor prevederi ale Hotărârii Guvernului nr. 79 din 23 ianuarie 2006 privind aprobarea Listei substanţelor narcotice, psihotrope şi a plantelor care conţin astfel de substanţe depistate în trafic ilicit, precum şi cantităţile acestora, Curtea Constituțională a Republicii Moldova a reținut: „[...] 63. [...] Existenţa dispoziţiilor de blanchetă în normele penale constituie o expresie a procesului obiectiv de reglementare normativă, fiind o modalitate specială de formulare a reglementărilor juridico-penale”[1131]; „64. Fără a contesta principiul codificării legii

[1128] DUVAC, Constantin. Accesul ilegal la un sistem informatic în reglementarea noului Cod penal. În: *Revista română de dreptul proprietăţii intelectuale*, 2012, nr. 1, pp. 88-109. ISSN 1584-7241; MANEA, Cornelia. Accesul ilegal la un sistem informatic. În: *Revista Pro Lege*, 2009, nr. 1, pp. 40-48. ISSN 1224-2411; MEDEANU, Tiberiu, CRĂCIUNESCU, Adrian. Accesul ilegal la un sistem informatic elemente constitutive şi delimitarea de alte infracțiuni. În: *Sesiunii ştiinţifice internaţionale „Uniunea Europeană – spaţiu de libertate, securitate şi justiţie” (Academia de Poliţie, Bucureşti, 23 mai 2013)*. Bucureşti: Editura Universitară, pp. 28-37. ISBN 978-606-591-723-1; MARIN, Cătălin. Accesul, fără drept, la un sistem informatic. În: *Conferința studențească anuală „Nicolae Titulescu”. Constant 2011 (București, 25-26 martie 2011)*. București: Pro Universitaria, 2011, pp. 430-443. ISSN 2246-9214; PĂVĂLEANU, Vasile. *Drept penal special*. București: Universul Juridic, 2014, p. 517. 620 p. ISBN 978-606-673-287-1.

[1129] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

[1130] Ibidem.

[1131] Hotărârea Curții Constituționale a Republicii Moldova pentru controlul constituţionalităţii unor prevederi ale Hotărârii Guvernului nr. 79 din 23 ianuarie 2006 privind aprobarea Listei substanţelor narcotice, psihotrope şi a

penale, recurgerea la dispoziţiile de blanchetă în Codul penal asigură stabilitatea legii penale”[1132], astfel încât conținutul acesteia să nu fie direct proporțional cu frecventele modificări ale actelor normative subsecvente, precum și legătura sistemică cu alte acte normative aplicabile. [...]”.[1133]

Revenind la analiza noastră, suntem de părerea că, la caracteristicile victimei infracţiunilor prevăzute la art. 259 CP RM, se referă implicit, între altele, următorul pasaj din alineatul (1) al acestui articol: „al unei persoane care nu este autorizată în temeiul legii sau al unui contract, 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”[1134]?

Din acest pasaj rezultă în aparență că despre victima infracţiunilor, prevăzute la art. 259 CP RM, trebuie să vorbim doar în ipoteza de acces ilegal la informaţia computerizată al unei persoane care 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. Considerăm că, în realitate, despre victima infracţiunilor, prevăzute la art. 259 CP RM, trebuie să vorbim și în ipoteza de acces ilegal la informaţia computerizată al unei persoane care fie nu este autorizată în temeiul legii sau al unui contract, fie depăşeşte limitele autorizării. Ajungem la această concluzie după ce analizăm anumite norme extrapenale la care face referire art. 259 CP RM.[1135] În primul rând, interesează prevederea de la alin. (2) art. 4 al Legii nr. 1069/2000: „Persoanele care activează în cadrul sistemelor şi reţelelor informatice sunt obligate să asigure protecţia datelor”.[1136] De asemenea, conform pct. 7) alin. (1) art. 11 al Legii nr. 982 din 11.05.2000 privind accesul la informaţie (în continuare – Legii nr. 982/2000), „furnizorul de informaţii [...] este obligat [...] să asigure protejarea informaţiilor ce se află la dispoziţia sa de accesul, distrugerea sau modificarea nesancţionate”.[1137]

---

plantelor care conţin astfel de substanţe depistate în trafic ilicit, precum şi cantităţile acestora: nr. 25 din 13.10.2015. În: *Monitorul Oficial al Republicii Moldova*, 2016, nr. 13-19, 01.

[1132] Ibidem.

[1133] Ibidem.

[1134] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.

[1135] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

[1136] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

[1137] Legea privind accesul la informaţie: nr. 982 din 11.05.2000. În: *Monitorul Oficial al Republicii Moldova*, 2000, nr. 88-90, 664.

În alt context, G. Zlati exclude posibilitatea prezenței victimei secundare (subiectului pasiv secundar) în cazul infracțiunii prevăzute la art. 360 CPR.[1138] Totodată, acest autor menționează: „Subiecții pasivi secundari sunt identificați fie în cazul infracțiunilor complexe, fie în cazul infracțiunilor pluriofensive”[1139], unde se poate realiza o ierarhizare a valorilor sociale protejate prin textul de incriminare”.[1140] Amintim cu această ocazie că infracțiunile prevăzute la art. 259 CP RM sunt biobiectuale. Din perspectiva obiectului juridic secundar al infracțiunilor prevăzute la art. 259 CP RM, victimă a acestor infracțiuni este persoana fizică sau persoana juridică care participă la relaţiile sociale cu privire la integritatea, autenticitatea, disponibilitatea sau ireproductibilitatea informației computerizate ori funcționalitatea calculatoarelor, a sistemului sau a reţelei informatice, apărate împotriva cauzării de: 1) daune în proporții mari (în cazul infracțiunii prevăzute la alin. (1)); 2) daune în proporții deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2)).[1141]

În doctrina penală autohtonă găsim opinii variate cu privire la participantul la asemenea relații sociale.

Astfel, fără a preciza dacă se referă la victima infracțiuni sau nu, A. Barbăneagră și Gh. Alecu menționează: „Proprietar al resurselor și sistemelor informaționale, al tehnologiilor și mijloacelor de asigurare a acestora se consideră persoana fizică, persoana juridică sau statul”[1142] „care exercită integral dreptul la posesiune, folosință și dispoziție asupra resurselor și sistemelor informaționale, tehnologiilor și mijloacelor de asigurare a acestora.”[1143] Referitor la victima infracțiunilor prevăzute la art. 259 CP RM, o părere similară a fost exprimată de către V. Stati[1144], L. Gîrla și Iu. Tabarcea.[1145]

Asemenea păreri corespund doar în parte cu interpretarea art. 259 CP RM în coroborare cu art. 3 al Legii nr. 467/2003. Astfel, în acest articol sunt definite noțiunile „posesor de resurse şi

---

[1138] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 160. 658 p. ISBN 978-606-8892-62-7.
[1139] Ibidem, p. 160.
[1140] Ibidem, p. 160.
[1141] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.
[1142] BARBĂNEAGRĂ, Alexei et al. *Codul penal comentat şi adnotat*. Chişinău: Cartier, 2005, p. 434. 656 p. ISBN 9975-29-338-X; BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 567. 860 p. ISBN 978-9975-105-20-0.
[1143] BARBĂNEAGRĂ, Alexei et al. *Codul penal comentat şi adnotat*. Chişinău: Cartier, 2005, p. 434. 656 p. ISBN 9975-29-338-X; BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 567. 860 p. ISBN 978-9975-105-20-0.
[1144] BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005, p. 496. 804 p. ISBN 9975-79-324-X; STATI, Vitalie. Răspunderea penală pentru infracţiunile în domeniul informaticii şi telecomunicaţiilor. În: *Analele ştiinţifice ale Universităţii de Stat din Moldova, Seria „Ştiinţe socioumanistice”*, 2005, Vol. I, pp. 387-394. ISSN 1811-2668.
[1145] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 15. 592 с. ISBN 978-9975-4158-2-8.

sisteme informaţionale, de tehnologii şi mijloace de asigurare a acestora” și „proprietar al resurselor şi sistemelor informaţionale, al tehnologiilor şi mijloacelor de asigurare a acestora”. Prima dintre aceste noțiuni este definită în modul următor: „posesor de resurse şi sisteme informaţionale, de tehnologii şi mijloace de asigurare a acestora – persoana fizică, persoana juridică sau statul”[1146], „având drept de posesiune şi folosinţă asupra resurselor şi sistemelor informaţionale, tehnologiilor şi mijloacelor de asigurare a acestora, în condiţiile stabilite de titularul drepturilor respective”.[1147] Cea de-a doua dintre aceste noțiuni este definită astfel: „proprietar al resurselor şi sistemelor informaţionale, al tehnologiilor şi mijloacelor de asigurare a acestora – persoana fizică, persoana juridică sau statul”[1148] „care exercită integral dreptul de posesiune, folosinţă şi dispoziţie asupra resurselor şi sistemelor informaţionale, tehnologiilor şi mijloacelor de asigurare a acestora”.[1149] În cazul ambelor noțiuni este important să înțelegem ce înseamnă „resurse şi sisteme informaţionale, tehnologii şi mijloace de asigurare a acestora”.

În art. 3 al Legii nr. 467/2003 pot fi identificate următoarele trei definiții: „resursă informaţională – totalitatea de informaţii documentate în sistemele informaţionale automatizate, organizată în conformitate cu cerinţele stabilite şi cu legislaţia în vigoare”[1150]; „sistem informaţional – totalitatea de resurse şi tehnologii informaţionale interdependente, de metode şi de personal, destinată păstrării, prelucrării şi furnizării de informaţie”[1151]; „tehnologie informaţională – totalitatea de metode, procedee şi mijloace de prelucrare şi transmitere a informaţiei şi regulile de aplicare a acesteia”.[1152] În acest articol lipsește definiția noțiunii „mijloace de asigurare a resurselor informaționale, a sistemelor informaţionale sau a tehnologiilor informaționale”. Totuși, nu aceste noțiuni sunt utilizate în art. 259 CP RM. În acest articol se menționează despre „distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”. Doar noțiunea „resursă informaţională” în accepțiunea art. 3 al Legii nr. 467/2003 este parțial relevantă, întrucât se intersectează cu noțiunea „informație (distrusă, deteriorată, modificată, blocată sau copiată)” din art. 259 CP RM.[1153]

[1146] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.
[1147] Ibidem.
[1148] Ibidem.
[1149] Ibidem.
[1150] Ibidem.
[1151] Ibidem.
[1152] Ibidem.
[1153] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

După această clarificare vom continua demersul nostru investigativ. Astfel, conform alin. (2) art. 7 al Legii nr. 467/2003, „subiecți ai raporturilor juridice în domeniul creării, administrării, mentenanței, dezvoltării și utilizării sistemelor informaționale de stat sunt: a) proprietarul sistemului informațional”[1154]; b) posesorul sistemului informațional; c) deținătorul sistemului informațional; d) administratorul tehnic al sistemului informațional; e) utilizatorii sistemului informațional”.[1155] Noțiunea de proprietar al sistemelor informaționale de stat este definită în art. 7^1 din aceeași lege. Potrivit alin. (1) art. 30 al Legii nr. 1069/2000, „dreptul de proprietate asupra produsului informatic îl obţin: a) creatorul – în urma creării produsului informatic cu forţe proprii şi pe cont propriu”[1156]; „b) persoana care a făcut comandă de creare a produsului informatic şi a finanţat toate lucrările aferente creării acestuia – în baza contractului încheiat cu creatorul produsului informatic”[1157]; „c) persoana juridică sau fizică ce intenţionează să folosească programul sau baza de date – în baza contractului încheiat cu proprietarul produsului informatic; d) moştenitorii şi alţi succesori de drepturi ai proprietarului – conform legislaţiei”.[1158] Noțiunile „posesorii sistemelor informaționale de stat”, „deținătorii sistemelor informaționale de stat” și „administratorii tehnici ai sistemelor informaționale de stat” sunt definite în art. 7^2-7^4 ale Legii nr. 467/2003.

Toate aceste definiții pot facilita într-o măsură redusă stabilirea caracteristicilor victimei infracțiunilor prevăzute la art. 259 CP RM, întrucât nu noțiunile „sistem informațional” și „produs informatic” sunt utilizate în acest articol. Reiterăm că în art. 259 CP RM se menționează despre „distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”.[1159] În acest context, menționăm că, în comparație cu prevederile Legii nr. 467/2003, mai relevante sunt unele prevederi ale Legii nr. 1069/2000. Astfel, alin. (2) art. 3 al acestei legi prevede: „Sistemele şi reţelele informatice, precum şi resursele informaţionale pot aparţine persoanelor juridice şi fizice cu titlu de proprietate privată sau publică”.[1160] Conform alin. (1) art. 16 al Legii nr. 1069/2000, „orice persoană este în drept să deţină date, programe şi echipamente, precum şi să prelucreze

---

[1154] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.
[1155] Ibidem.
[1156] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[1157] Ibidem.
[1158] Ibidem.
[1159] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.
[1160] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

date şi programe”[1161], „cu obţinerea unor produse informatice pentru uz propriu, dacă aceasta nu contravine prevederilor prezentei legi”.[1162] De asemenea, prezintă interes art. 29 al Legii nr. 1069/2000: „(1) Obiecte ale dreptului de proprietate în domeniul informaticii pot fi: a) resursele informaţionale şi datele [...]”[1163]; b) sistemele informatice. (2) Subiecte ale dreptului de proprietate în domeniul informaticii pot fi statul – prin autorităţile administraţiei publice, precum şi persoanele juridice şi fizice”.[1164] Din analiza acestor norme rezultă că persoanele fizice și persoanele juridice pot fi proprietari sau altfel de posesori / deținători ai informaţiilor computerizate, ai calculatorului, ai sistemului informatic sau ai rețelei informatice.

În concordanță cu dispozițiile Legii nr. 1069/2000, reproduse mai sus, S. Brînza, V.Stati și Iu. Diaconu afirmă că victimă a infracţiunilor prevăzute la art. 259 CP RM este „proprietarul sau alt posesor al informaţiei computerizate, al calculatorului, al sistemului informatic sau al reţelei informatice accesate ilegal”.[1165] În privința victimei aceloraşi infracțiuni, L. Dumneanu și D. Gurev au o poziție care se deosebește printr-un singur detaliu: „proprietarul sau *deținătorul* (evid. ns.) informaţiei computerizate, calculatorului, sistemului informatic sau al reţelei informatice accesate ilegal”.[1166] În continuare, este necesar să analizăm care dintre sintagme – „alt posesor al informaţiei computerizate, al calculatorului, al sistemului informatic sau al reţelei informatice accesate ilegal”[1167] (utilizată de către S. Brînza, V.Stati și Iu. Diaconu) sau „deținătorul informaţiei computerizate, calculatorului, sistemului informatic sau al reţelei informatice accesate ilegal”[1168] (folosită de către L. Dumneanu și D. Gurev) – este mai potrivită pentru a caracteriza victima infracțiunilor prevăzute la art. 259 CP RM.

Noțiunea de deținător este folosită, de exemplu, în art. 4 din Codul funciar: „Prin deţinători de terenuri se înţeleg titularii dreptului de proprietate, de posesiune, de beneficiere funciară”.[1169]

[1161] Ibidem.
[1162] Ibidem.
[1163] Ibidem.
[1164] Ibidem.
[1165] BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011, p. 263. 1324 p. ISBN 978-9975-53-028-7; POALELUNGI, Mihai et al. *Manualul judecătorului pentru cauze penale*. Chișinău: Tipografia Centrală, 2013, p. 703. 1192 p. ISBN 978-9975-53-231-0; BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 350. 1300 p. ISBN 978-9975-53-470-3.
[1166] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM, p. 92. 261 p. ISBN 978-9975-158-29-9.
[1167] BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011, p. 263. 1324 p. ISBN 978-9975-53-028-7; POALELUNGI, Mihai et al. *Manualul judecătorului pentru cauze penale*. Chișinău: Tipografia Centrală, 2013, p. 703. 1192 p. ISBN 978-9975-53-231-0; BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 350. 1300 p. ISBN 978-9975-53-470-3.
[1168] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM, p. 92. 261 p. ISBN 978-9975-158-29-9.
[1169] Codul funciar al Republicii Moldova: nr. 828 din 25.12.1991. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 107, 817.

Referitor la noțiunea de deținător utilizată într-un context similar în legislația română, R.N. Popescu susține: „Noțiunea de „deținător“ este [...] definită prin art. 3 din Legea nr. 18/1991 (se are în vedere Legea României nr. 18 din 19.02.1991 a fondului funciar – *n.a.*)”[1170]: „În sensul prezentei legi, prin deţinători de terenuri se înţelege titularii dreptului de proprietate”[1171], „ai altor drepturi reale asupra acestora sau cei care, potrivit legii civile, au calitatea de posesori ori deţinători precari”.[1172] După cum se poate observa definiția noțiunii de deținător este extrem de largă, acoperind practic toate ipotezele care pot apărea în practică. [...] Cu alte cuvinte, în sensul Legii nr. 18/1991, *noțiunea de deținător este cel care stăpânește bunul, indiferent cu ce titlu (ex. proprietate, moștenire, închiriere etc.)* (evid. ns.)”.[1173]

Mai multă claritate noțiunii de deținător îi aduce punctul de vedere exprimat de către I.R. Urs: „Alături de posesie şi proprietate ca modalităţi de stăpânire a unui bun, art. 918 din noul Cod civil, printr-o formulare negativă, este reglementată a treia modalitate de stăpânire a unui bun, anume detenţia precară”[1174]; „Actualul legiuitor, pentru a evita confuziile din Codul civil încă în vigoare, precizează în art. 918 expres „cazurile care nu constituie posesie”, evidenţiind astfel că precaritatea nu este un viciu al posesiei”[1175], „ci o situaţie juridică distinctă cu regim juridic special având „efectele recunoscute posesiei în cazurile şi limitele prevăzute de lege”.”[1176]; „Aşadar, nu constituie posesie stăpânirea unui bun de către un detentor precar, precum: a) locatarul, comodatarul, depozitarul, creditorul gajist”[1177]; „b) titularul dreptului de superficie, usufruct, uz, abitaţie sau servitute, faţă de nuda proprietate; c) fiecare coproprietar, în proporţie cu cotele-părţi ce revin celorlalţi coproprietari”[1178]; „d) orice altă persoană care, deţinând temporar un bun al altuia, este obligată să îl restituie sau care îl stăpâneşte cu îngăduinţa acestuia”.[1179] Același autor evocă: „Detenţia precară şi posesia sunt două situaţii juridice diferite şi ca urmare detentorul precar se deosebeşte de posesor”[1180]; „Deşi îi apropie până la confuzie un element comun, respectiv stăpânirea materială, fizică a bunului *(corpus)*, ceea ce îi aşează în

---

[1170] POPESCU, Răzvan Nicolae. *Legea nr. 87/2020 „Mi se aplică”? Persoanele îndreptățite la constituirea dreptului de proprietate asupra terenului*. [citat 11.07.2022] Disponibil: https://www.juridice.ro/758030/legea-nr-87-2020-mi-se-aplica-persoanele-indreptatite-la-constituirea-dreptului-de-proprietate-asupra-terenului.html
[1171] Ibidem.
[1172] Legea României a fondului funciar: nr. 18 din 19.02.1991. În: *Monitorul Oficial al României*, 1991, nr. 31.
[1173] POPESCU, Răzvan Nicolae. *Legea nr. 87/2020 „Mi se aplică”? Persoanele îndreptățite la constituirea dreptului de proprietate asupra terenului*. [citat 11.07.2022] Disponibil: https://www.juridice.ro/758030/legea-nr-87-2020-mi-se-aplica-persoanele-indreptatite-la-constituirea-dreptului-de-proprietate-asupra-terenului.html
[1174] URS, Iosif Robi. Consideraţii asupra reglementării posesiei şi detenţiei precare în noul Cod civil român. În: *Analele Universităţii Titu Maiorescu. Drept, Serie Nouă*, 2008, pp. 9-19. ISSN 1584-4781.
[1175] Ibidem.
[1176] Ibidem.
[1177] Ibidem.
[1178] Ibidem.
[1179] Ibidem.
[1180] Ibidem.

categorii juridice distincte este elementul psihologic al stăpânirii materiale – *animus*”[1181]; „Detentorul precar deţine bunul pentru altul căruia îi recunoaşte dreptul asupra bunului, iar după cum am aflat mai sus, posesorul îl stăpâneşte prin putere proprie, pentru sine”[1182]; „După cum observăm, detentorii precari deţin bunul fie ca titulari ai unor drepturi de creanţă, fie ca titulari ai unor drepturi reale, fie ca simpli deţinători prin bunăvoinţa proprietarului”.[1183]

Însă, în Codul civil al Republicii Moldova nu sunt folosite noțiunile „detentor precar” și „detenție precară”. În acest sens, I. Selevestru argumentează: „Nu considerăm necesară utilizarea sintagmei „detentor precar” în raport cu victima infracţiunilor prevăzute la art. 191 CP RM”[1184]; „Or, în corespundere cu alin. (6) art. 335 din Codul civil, „posesiunea este precară când nu se exercită sub nume de proprietar””[1185] „(în varianta în vigoare a Codului civil al Republicii Moldova, această prevedere se află la alin. (6) art. 532 – *n.a.*)”[1186]; „Aşadar, indiferent dacă posesiunea este exercitată în nume propriu sau în numele unei alte persoane, ea rămâne a fi posesiune şi nu se transformă în detenţie”; „Codului civil al Republicii Moldova nu-i este cunoscută expresia „detenţie precară”. Aceasta este folosită în Codul civil român din 17.07.2009”.[1187]

În concluzie, din perspectiva Codului civil al Republicii Moldova, sintagma „alt posesor al informaţiei computerizate, al calculatorului, al sistemului informatic sau al reţelei informatice accesate ilegal” (utilizată de către S. Brînza, V.Stati și Iu. Diaconu) este mai potrivită decât sintagma „deținătorul informaţiei computerizate, calculatorului, sistemului informatic sau al reţelei informatice accesate ilegal” (folosită de către L. Dumneanu și D. Gurev). Nu trebuie să uităm că posesia (în sensul Codului civil al Republicii Moldova) este o stare de fapt, nu neapărat o stare de drept. Or, conform alin. (1) art. 482 din acest cod, „posesiunea se dobândeşte prin exercitarea voită a stăpânirii de fapt a bunului”[1188].[1189]

Un alt aspect, la care dorim să ne referim, ține de posibilitatea evoluării utilizatorului informației computerizate în calitate de victimă a infracțiunilor prevăzute la art. 259 CP RM.

[1181] Ibidem.
[1182] Ibidem.
[1183] Ibidem.
[1184] SELEVESTRU, Irina. Victima infracţiunilor prevăzute la art. 191 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale”*, 2015, nr. 3, pp. 194-199. ISSN 1814-3199.
[1185] Ibidem.
[1186] Ibidem.
[1187] Ibidem.
[1188] Codul civil al Republicii Moldova: nr. 1107 din 06.06.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 82-86, 661.
[1189] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

O astfel de posibilitate este admisă de către V. Stati, L. Gîrla și Iu. Tabarcea.[1190] În doctrina penală română, o opinie asemănătoare este exprimată de către Z. Sadâc.[1191] De asemenea, G. Zlati evocă în legătură cu victima (subiectul pasiv) infracțiunii prevăzute la art. 360 CPR: „Acesta nu se identifică în mod obligatoriu cu proprietarul ori deținătorul sistemului informatic. Așadar, subiectul pasiv poate să fie inclusiv o persoană ce are un drept de utilizare consolidat (chiar limitat) în raport cu acesta”.[1192]

Conform art. 3 al Legii nr. 467/2003, prin „utilizator de informaţie” se înțelege „persoana fizică sau persoană juridică ce efectuează acţiuni de prezentare, primire, păstrare şi alte acţiuni de utilizare a informaţiei documentate în sistem informaţional automatizat”.[1193] Potrivit art. 7^5 al aceleiași legi, „utilizatori ai sistemelor informaționale de stat sunt persoanele fizice și/sau persoanele juridice de drept public sau privat”.[1194]

Este oare posibil ca utilizatorul de informații computerizate să fie altcineva decât proprietarul sau alt posesor al unor asemenea informaţii? Răspunsul la această întrebare este afirmativ. La o asemenea ipoteză se referă D.S. Azarov: „Infracțiunea poate împiedica exercitarea dreptului unei persoane, care este un utilizator autorizat al anumitor informații ce nu-i aparțin cu titlu de proprietate”[1195] „(bunăoară, persoana a achitat pentru a accesa anumite informații care au fost distruse, blocate, modificate etc.)”.[1196] La o ipoteză asemănătoare se referă G. Zlati: victima achită „un abonament lunar pentru a putea folosi platforma Netflix”.[1197] În ambele aceste ipoteze, victimă este utilizatorul care nu este nici proprietarul informațiilor computerizate distruse, deteriorate, modificate, blocate sau copiate, nici alt posesor al acestora. Bineînțeles, vorbim despre utilizatorul care beneficiază de dreptul la protecția informaţiilor computerizate împotriva distrugerii, deteriorării, modificării, blocării sau copierii.[1198]

[1190] BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005, p. 496. 804 p. ISBN 9975-79-324-X; STATI, Vitalie. Răspunderea penală pentru infracţiunile în domeniul informaticii şi telecomunicaţiilor. În: *Analele ştiinţifice ale Universităţii de Stat din Moldova, Seria „Ştiinţe socioumanistice”*, 2005, Vol. I, pp. 387-394. ISSN 1811-2668; ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 15. 592 с. ISBN 978-9975-4158-2-8.

[1191] SADÂC, Zafer. Theoretical and Practical Considerations regarding the Illegal Access to a Computer System in the Romanian Criminal Law. În: *Technium Social Sciences Journal*, 2021, nr. 26, pp. 944-949. ISSN 2668-7798.

[1192] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 160. 658 p. ISBN 978-606-8892-62-7.

[1193] Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.

[1194] Ibidem.

[1195] АЗАРОВ, Д.С. *Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)*. Київ: Атіка, 2007, с. 54. 304 с. ISBN 966-326-230-3.

[1196] Ibidem, c. 54.

[1197] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 160. 658 p. ISBN 978-606-8892-62-7.

[1198] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

În alt context, N.A. Rozenfeld menționează: „Noțiunea de posesor de informații computerizate și cea de posesor de sistem informatic pot să nu coincidă”.[1199] Totodată, L. Dumneanu și D. Gurev afirmă: „Nu se exclude identificarea unei sau mai multor victime (cu calități diferite) într-o singură infracțiune”.[1200] Suntem de acord cu ambele păreri. Or, infracțiunea are o singură victimă în cazul în care aceeași persoană este atât proprietarul, alt posesor sau utilizatorul informaţiilor computerizate accesate ilegal, cât și proprietarul sau alt posesor al informației distruse, deteriorate, modificate, blocate sau copiate, ori al calculatorului, al sistemului informatic sau al reţelei informatice, ale căror funcționare a fost dereglată. În alte cazuri, proprietarul, alt posesor sau utilizatorul informaţiilor computerizate accesate ilegal poate fi altcineva decât proprietarul sau alt posesor al calculatorului, al sistemului informatic sau al reţelei informatice, ale căror funcționare a fost dereglată. Doar în aceste din urmă cazuri, putem vorbi despre prezența victimei principale și a victimei secundare.[1201]

În aceste din urmă cazuri, intenția unică a făptuitorului cuprinde pluralitatea și varietatea de victime. Deci, nu putem vorbi despre un concurs de infracțiuni, întrucât art. 259 CP RM se aplică o singură dată. De aceea, avem rezerve față de următoarea idee promovată de G. Zlati: „În măsura în care este accesată o pluralitate de sisteme informatice, fiecare având un alt titular, se va reține un concurs de infracțiuni”.[1202] Considerăm că această idee contravine spiritului Deciziei Curții Constituționale a României nr. 368 din 30.05.2017 referitoare la excepția de neconstituționalitate a dispozițiilor art. 35 alin. (1) și ale art. 39 alin. (1) lit. b) din Codul penal[1203], prin care sintagma „și împotriva aceluiași subiect pasiv” din cuprinsul dispoziției de la alin. (1) art. 35 CPR a fost declarată neconstituțională. Numărul de victime, ca și numărul și/sau varietatea de obiecte materiale, nu reprezintă factori care pot avea un impact asupra unității infracțiunii. Singurul factor relevant este unitatea intenției/rezoluției infracționale.[1204]

[1199] РОЗЕНФЕЛЬД, Н.А. *Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж*: дис. на здоб. наук. ступ. канд. юрид. наук. Київ, 2003, с. 55. 222 с.

[1200] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM, p. 92-93. 261 p. ISBN 978-9975-158-29-9.

[1201] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

[1202] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 157. 658 p. ISBN 978-606-8892-62-7.

[1203] Decizia Curții Constituționale a României referitoare la excepția de neconstituționalitate a dispozițiilor art. 35 alin. (1) și ale art. 39 alin. (1) lit. b) din Codul penal: nr. 368 din 30.05.2017. În: *Monitorul Oficial al României*, 2017, nr. 566.

[1204] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

2.2. Latura obiectivă a infracțiunilor prevăzute la art. 259 CP RM

Din art. 15 și 52 CP RM reiese că latura obiectivă reprezintă unul din elementele constitutive ale faptei infracționale. Indiferent dacă infracțiunea este formală sau materială, latura ei obiectivă include ca semn constitutiv fapta prejudiciabilă (elementul material). Acest semn se referă la manifestarea exterioară a infracțiunii, la comportamentul făptuitorului, care se concretizează în acțiune sau inacțiune.

2.2.1. Fapta prejudiciabilă în cazul infracțiunilor prevăzute la art. 259 CP RM

După cum deducem din denumirea art. 259 CP RM și din dispoziția de la alin. (1) art. 259 CP RM, fapta prejudiciabilă, prevăzută de acest articol, cuprinde acțiunea de acces ilegal la informaţia computerizată. La această etapă a analizei folosim cu prudență cuvântul „cuprinde", deoarece *infra* urmează să soluționăm următoarea dilemă: 1) epuizează oare acțiunea de acces ilegal la informaţia computerizată întreg conținutul faptei prejudiciabile care este prevăzută de art. 259 CP RM *sau* 2) această acțiune este doar una din componentele faptei prejudiciabile care este prevăzută în art. 259 CP RM?

În Raportul explicativ la Convenția de la Budapesta, în pct. 46, este definită noțiunea de accesare, utilizată în art. 2 „Accesarea ilegală" din Convenția respectivă[1205]: „Noțiunea „accesare" presupune pătrunderea în întregime într-un sistem informatic sau în oricare parte a acestuia [...]"[1206]; „[...] Noțiunea „accesare" presupune intrarea într-un alt sistem informatic, în cazul în care acesta este conectat prin rețele publice de telecomunicații, sau la un sistem informatic din aceeași rețea [...]"[1207]; „Nu este relevantă metoda de conectare (de exemplu, de la distanță, inclusiv prin legături fără fir sau la o distanță apropiată)".[1208] Această definiție nu are un caracter normativ, deși constituie o interpretare oficială a unei noțiuni normative.

În legislația Republicii Moldova lipsește definiția normativă a noțiunii de acces. Un exemplu de definiție normativă de acest gen îl găsim în legislația României. Astfel, la lit. b) alin. (1) art.

[1205] Acest articol prevede: „Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune"*, „potrivit dreptului său intern, accesarea intenţionată şi fără drept a ansamblului ori a unei părţi a unui sistem informatic"*; „O parte poate condiţiona o astfel de incriminare de comiterea încălcării respective prin violarea măsurilor de securitate"*, „cu intenţia de a obţine date informatice ori cu altă intenţie delictuală, sau de legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic".*

* *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561

[1206] *Explanatory Report to the Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/16800cce5b

[1207] Ibidem.

[1208] Ibidem.

138 din Codul de procedură penală al României, este folosită noțiunea „accesul la un sistem informatic”, care se referă la una dintre metodele speciale de supraveghere sau cercetare. Alineatul (3) din același articol conține următoarea definiție: „Prin acces la un sistem informatic se înțelege pătrunderea într-un sistem informatic sau mijloc de stocare a datelor informatice fie direct, fie de la distanță”[1209], „prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe”.[1210] Dacă abstragem ultima parte – „în scopul de a identifica probe” – atunci putem afirma că definiția dată concentrează esența explicației din pct. 46 al Raportului explicativ la Convenția de la Budapesta.

Totuși, nici explicația din pct. 46 al Raportului explicativ la Convenția de la Budapesta, nici definiția din alin. (3) art. 138 din Codul de procedură penală al României, nu posedă suficient potențial pentru a reda semnificația noțiunii „accesul ilegal la informaţia computerizată”, utilizate în art. 259 CP RM. Or, obiectul accesului ilegal în accepțiunea acestui articol este informaţia computerizată, nu sistemul informatic. Din aceste considerente, nu putem beneficia la justa valoare de randamentul definițiilor propuse de către unii doctrinari autohtoni. De exemplu, S. Brînza și V. Stati menționează: „„Acces” înseamnă uzitarea de resursele unui sistem informatic, adică darea de instrucţiuni unui sistem informatic, comunicarea cu/printr-un sistem informatic”[1211], „stocarea informaţiei sau regăsirea acesteia într-un sistem informatic. Accesul include intrarea într-un alt sistem informatic, conectat prin reţele de telecomunicaţii publice sau într-un alt sistem informatic din aceeaşi reţea informatică”[1212], „indiferent de metoda de comunicare. Metoda de comunicare – la distanţă, inclusiv graţie legăturii prin satelit sau nu, ori de aproape – nu prezintă relevanţă la calificare”.[1213] La rândul lor, L. Dumneanu și D. Gurev afirmă: „Prin acces se înţelege folosirea de componentele unui sistem informatic, cum ar fi accesarea elementelor unui sistem informatic”[1214], „comunicarea cu/printr-un sistem informatic, depozitarea informaţiei sau regăsirea acesteia într-un sistem informatic”[1215]; „Accesul presupune penetrarea unui alt sistem informatic, conectat prin reţele de telecomunicaţii publice sau într-un alt sistem informatic din aceeaşi reţea, indiferent prin ce metoda de comunicare”.[1216] Într-o măsură mai pronunțată, exigențelor dispoziției art. 259 CP RM îi corespunde definiția formulată

[1209] Codul de procedură penală al României: nr. 135 din 01.07.2010. În: *Monitorul Oficial al României*, 2010, nr. 486.
[1210] Ibidem.
[1211] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 351. 1300 p. ISBN 978-9975-53-470-3.
[1212] Ibidem, p. 351.
[1213] Ibidem, p. 351.
[1214] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM, p. 93. 261 p. ISBN 978-9975-158-29-9.
[1215] Ibidem, p. 93.
[1216] Ibidem, p. 93.

de către C. Moțoc și L. Gîrla: „Accesul reprezintă un proces de asigurare a posibilității de a implementa un act de familiarizare și (sau) manipulare a informațiilor [...]”.[1217]

Pentru a defini noțiunea de acces la informația computerizată, care să corespundă exigențelor dispoziției art. 259 CP RM, este necesar, în primul rând, să luăm în calcul înțelesul noțiunii de informație computerizată: informația destinată prelucrării pe un calculator, fixată pe un suport care poate fi citit de un calculator sau transmis într-un mediu care face posibilă interacționarea în cadrul unui sistem informatic sau al unei rețele informatice. Însă, aceasta nu este suficient. Pentru a accesa informația computerizată, este necesar mai întâi să fie accesat calculatorul, suportul material de informaţie, sistemul informatic sau reţeaua informatică, în care sau pe care se află respectiva informație. Ținând cont de acest aspect și de înțelesul noțiunii de informație computerizată, precum și având ca puncte de reper definițiile propuse de către C. Moțoc, L. Gîrla, S. Brînza, V. Stati, L. Dumneanu și D. Gurev, considerăm că, prin „acces la informația computerizată” în accepțiunea art. 259 CP RM trebuie de înțeles: obținerea posibilității de a recurge la informația computerizată, în vederea beneficierii de calitățile utile ale acesteia.

În alt context, în art. 2 al Convenției de la Budapesta, se vorbește despre „accesarea [...] ansamblului ori a unei părţi a unui sistem informatic”.[1218] În art. 3 „Accesarea ilegală a sistemelor informatice” din Directiva 2013/40/UE este menționată „accesarea [...] unui sistem informatic sau a unei părți a acestuia”.[1219] Făcând analogie cu art. 259 CP RM, observăm că legiuitorul trece cu tăcerea acest detaliu. Aceasta înseamnă că, în cazul infracțiunilor prevăzute de acest articol, accesul la informația computerizată este fie integral, fie parțial. Amploarea accesării informației computerizate nu are vreun impact asupra calificării faptei în conformitate cu art. 259 CP RM, însă poate fi luată în calcul în procesul de individualizare a pedepsei.

Mai important este însă să stabilim nu atât amploarea accesării informației computerizate în accepția art. 259 CP RM, cât mai ales caracterul accesării acesteia.

În context, atrage atenția următoarea opinie a lui G.S.O. Kurbanov, care vizează infracțiunile prevăzute de un articol din Codul penal al Republicii Azerbaidjan, ce corespunde art. 259 CP RM: „Accesul ilegal este un concept [...] care include [...]: intruziunea „fizică”, care oferă posibilitatea de a prelua informații dintr-un calculator; operarea neautorizată cu informațiile

---

[1217] MOȚOC, Costică, GÎRLA, Lilia. Protecția juridico-penală a secretului profesional prin prisma incriminărilor prevăzute la art. 178, 259, 260[1], 260[2] CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale”*, 2020, nr. 3, pp. 139-151. ISSN 1814-3199.

[1218] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561

[1219] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en

dintr-un calculator”.[1220] În aceeași ordine de idei se înscriu punctele de vedere exprimate de către unii autori români. De exemplu, Gh.Iu. Ioniță afirmă: „Accesul la un sistem informatic poate să fie la un nivel fizic și/sau la un nivel logic: 1) la nivel fizic, accesul presupune interacțiunea cu *hardware*-ul (partea fizică) sistemului informatic (componentele)”[1221]; „2) la nivel logic, accesul presupune interacțiunea cu *software*-ul (partea logică) sistemului informatic (programe/aplicații)”[1222]; „Cu alte cuvinte, în momentul în care retragem o sumă de bani de la un ATM sau plătim un produs/serviciu prin intermediul ATM-ului/POS-ului, accesul se face atât la nivel fizic”[1223], „pentru că interacționăm cu *hardware*-ul (componentele fizice) acelui sistem informatic (fantă de acces pentru card, tastatură, ecran), cât și la nivel logic”[1224], „pentru că interacționăm cu *software*-ul (partea logică) sistemului informatic (programele / aplicațiile / sistemul de operare)”.[1225] De asemenea, R.A. Nestor susține: „În forma sa cea mai simplă, accesul la un sistem informatic presupune o interacțiune a făptuitorului cu tehnica de calcul vizată prin intermediul echipamentelor”[1226]; „sau diverselor componente ale sistemului vizat (sursă de alimentare, butoane de pornire, tastatură, mouse, joystick)”[1227]; „Manipularea acestor dispozitive se transformă în solicitări către Unitatea Centrală de Prelucrare [...], care va procesa date ori va rula programe de aplicații în beneficiul intrusului.”[1228]

Aceste păreri se deosebesc de cele exprimate de alți autori români. Astfel, I. Kuglay relevă: „Accesarea sistemului constituie, în principiu, acea operaţiune prin care se realizează o interacţiune funcţională cu sistemul informatic”[1229]; „O primă delimitare pe care practica neunitară a reclamat-o a fost aceea între interacţiunea de ordin material, fizic şi cea de ordin logic”[1230]; „numai aceasta din urmă are semnificaţia accesării sistemului informatic, respectiv numai aceea care conferă făptuitorului posibilitatea „de a da comenzi, de a cauza introducerea, obţinerea”[1231], „afişarea, stocarea ori diseminarea de date informatice sau folosirea în orice alt

---

[1220] КУРБАНОВ, Г.С.О. Объективная сторона преступления, связанного с неправомерным доступом к компьютерной информации. În: *Правовая информатика*, 2013, nr. 4, с. 17-20. ISSN 1994-1404.
[1221] IONIȚĂ, Gheorghe Iulian. Accesul la un sistem informatic și recursul în interesul legii formulat în această materie. În: *Revista de Drept Penal*, 2013, vol. 20, nr. 4, pp. 111-125. ISSN 1223-0790.
[1222] Ibidem.
[1223] Ibidem.
[1224] Ibidem.
[1225] Ibidem.
[1226] NESTOR, Raul Alexandru. *Incriminarea accesului ilegal la un sistem informatic sau riscul de a transforma un mijloc esențial de obținere a informației în mod de încălcare a legii penale*. [citat 06.03.2022] Disponibil: https://www.juridice.ro/753151/incriminarea-accesului-ilegal-la-un-sistem-informatic-sau-riscul-de-a-transforma-un-mijloc-esential-de-obtinere-a-informatiei-in-mod-de-incalcare-a-legii-penale.html
[1227] Ibidem.
[1228] Ibidem.
[1229] BODORONCEA, Georgina et al. *Codul penal: comentariu pe articole*. București: C.H. Beck, 2014, p. 778. 902 p. ISBN 978-606-18-0408-5.
[1230] Ibidem, p. 778.
[1231] Ibidem, p. 779.

mod a resurselor unui calculator, sistem”[1232] „ori reţea informatică sau comunicarea cu unităţile sale aritmetice, logice ori de memorie”[1233].”[1234] De asemenea, G. Zlati menționează: „Accesul trebuie să fie unul propriu-zis, înțelegând prin aceasta posibilitatea ca agentul, prin interacţiunea logică”[1235] „pe care o are cu sistemul informatic să poată beneficia (ori să existe cel puţin potenţial această posibilitate) de funcţiile ori resursele sistemului informatic”[1236]; „Această abordare ar fi din punctul nostru de vedere suficient de restrictivă pentru a nu extinde câmpul de aplicabilitate a normei de incriminare”[1237] „dincolo de ceea ce s-a dorit şi suficient de abstractă încât să poată suferi anumite interpretări evolutive”.[1238] Susținem opinia lui I. Kuglay și G. Zlati.

Accesul ilegal la informația computerizată (în accepția art. 259 CP RM) trebuie deosebit de interceptarea ilegală a unei transmisii de date informatice (în sensul art. 260^1 CP RM). În ultimul caz, interacțiunea este, de asemenea, de ordin logic. La concret, are loc interceptarea ilegală a unei transmisii de date informatice (inclusiv a unei emisii electronice) care nu sunt publice și care sunt, după caz: 1) destinate unui sistem informatic; 2) provin dintr-un asemenea sistem; 3) se efectuează în cadrul unui sistem informatic. În ultimul caz, atunci când se interceptează ilegal transmisia de date informatice (inclusiv a unei emisii electronice) care nu sunt publice, se aplică doar art. 260^1 CP RM. Pentru a deosebi cele două infracțiuni, se poate apela, cu ajustările de rigoare la următoarea explicație din jurisprudența română, dată de Înalta Curte de Casație și Justiție a României: „Infracțiunea prevăzută de art. 361 C. pen. (se are în vedere infracțiunea de interceptare ilegală a unei transmisii de date informatice – *n.a.*) se diferențiază de infracțiunea de acces, fără drept, la un sistem informatic”[1239], „prin faptul că acțiunea de interceptare se realizează în procesul de transmitere a acestor date de la un sistem informatic la altul”[1240]; „Ambele infracțiuni sunt săvârșite cu scopul de a obține ilegal date informatice (de regulă, folosite ulterior pentru comiterea infracțiunii contra patrimoniului)”[1241], „interceptarea

---

[1232] Ibidem, p. 779.
[1233] VASIU, Ioana, VASIU, Lucian, Contaminanţii informatici ca vector ai accesului ilegal. În: *Revista de Drept Penal*, 2006, nr. 2, pp. 37-40. ISSN 1223-0790.
[1234] BODORONCEA, Georgina et al. *Codul penal: comentariu pe articole*. Bucureşti: C.H. Beck, 2014, p. 778-779. 902 p. ISBN 978-606-18-0408-5.
[1235] ZLATI, George. *Greşita interpretare a accesului la un sistem informatic. Consecinţe practice*. [citat 06.03.2022] Disponibil: https://www.juridice.ro/259331/gresita-interpretare-a-accesului-la-un-sistem-informatic-consecinte-practice.html
[1236] Ibidem.
[1237] Ibidem.
[1238] Ibidem.
[1239] *Înalta Curte de Casație și Justiție a României. Secția penală. Decizia nr. 416/A/2016*. [citat 06.03.2022] Disponibil: www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=133689
[1240] Ibidem.
[1241] Ibidem.

comportând, însă, un caracter dinamic, în timp ce accesul ilegal la un sistem informatic are un caracter static."[1242]

După această divagație, este necesar de menționat că exemplele de acces ilegal la un sistem informatic ne ajută să percepem înțelesul noțiunii „accesul la informația computerizată".

În Decizia Înaltei Curți de Casaţie și Justiţie a României nr. 15 din 14.10.2013 privind interpretarea şi aplicarea unitară a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noţiunii de acces fără drept la un sistem informatic, s-a reținut că acces ilegal la un sistem informatic se consideră, printre altele: folosirea la bancomat a unui card bancar autentic, fără acordul titularului său, în scopul efectuării unor retrageri de numerar; folosirea la bancomat a unui card bancar falsificat, pentru retrageri de numerar.[1243] De exemplu, într-o speță care se conține în practica judiciară română, art. 360 CPR a fost aplicat deoarece „inculpata M.M. a introdus cardul [autentic pierdut de către victimă] în bancomat de două ori"[1244], „a retras de fiecare dată câte 400 lei fără a avea consimţământul persoanei vătămate".[1245]

În speța următoare s-a omis nejustificat aplicarea art. 259 CP RM: F.S. a fost condamnat în conformitate cu alin. (1) art. 237 și lit. a), b) alin. (2) art. 260^4 CP RM. În perioada anilor 2015-2016, acţionând prin înţelegere prealabilă cu persoane neidentificate, urmărind scopul fabricării şi punerii în circulaţie a cardurilor false, făptuitorii au produs, prin intermediul unui program informatic, coduri pentru a accesa un sistem informatic, pentru a obține informaţia de pe banda magnetică a unor carduri bancare. Ulterior, după modificarea informației de pe banda magnetică a acelor carduri bancare, făptuitorii au efectuat plăţi în mărime totală de 118512,62 lei prin intermediul terminalelor care aparțineau unor bănci comerciale din Republica Moldova.[1246] Printre scopurile infracțiunii prevăzute la art. 260^4 CP RM se numără cel de săvârşire a uneia din faptele infracţionale ce sunt specificate în art. 259 CP RM. În ultima din spețele analizate, acest scop a fost prezent și, mai mult, a fost realizat. Or, după cum rezultă din speță, făptuitorii au efectuat plăţi prin intermediul terminalelor care aparțineau unor bănci comerciale. O astfel de acțiune ar fi posibilă doar pe calea accesării serverelor (care sunt sisteme informatice) care

[1242] Ibidem.
[1243] Decizia Înaltei Curți de Casaţie și Justiţie a României privind interpretarea şi aplicarea unitară a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noţiunii de acces fără drept la un sistem informatic: nr. 15 din 14.10.2013. În: *Monitorul Oficial al României*, 2013, nr. 760.
[1244] *Tribunalul Covasna. Sentință penală nr. 11 din 05.03.2019*. [citat 06.03.2022] Disponibil: https://www.jurisprudenta.com/jurisprudenta/speta-150kzrwm/
[1245] Ibidem.
[1246] *Sentinţa Judecătoriei Chişinău (sediul Buiucani) din 14.02.2019. Dosarul nr. 1-601/2018*. [citat 06.03.2022] Disponibil: https://jc.instante.justice.md/ro/pigd_integration/pdf/c8678a6c-f738-e911-80d5-0050568b021b; *Decizia Colegiului penal al Curții de Apel Chișinău din 20.05.2020. Dosarul nr. 1a-631/2020*. [citat 06.03.2022] Disponibil: https://cac.instante.justice.md/ro/pigd_integration/pdf/45946398-403f-4820-8c4e-0ed11ad86fc1

aparțineau băncilor ce deserveau deținătorii acelor carduri. Ca urmare, soluția de calificare a celor comise de către F.S. și persoanele neidentificate ar fi trebuit să includă art. 259 CP RM.

Prezentând exemple de acces la un sistem informatic, G. Zlati specifică: „accesarea unui cont bancar online”[1247]; „autentificarea (accesul) fără drept la interfața de administrare a unei pagini web”[1248]; „utilizarea clandestină a puterii de calcul a unui sistem informatic prin intermediul unui program informatic în vederea generării de noi monede electronice”[1249]; „folosirea de la distanță *(remote access)* a unui sistem informatic prin intermediul programului Team Viewer.”[1250]

P. Tamas-Erno prezintă ca exemplu de acces la un sistem informatic accesarea conturilor de Facebook cu ajutorul unor programe sau softuri, cum ar fi Keylogger, Stealer, Scampage, Session Hijacking etc.[1251] De asemenea, în opinia lui V. Coman, accesarea unui cont de e-mail sau de Facebook se înscrie în lista de exemple de acces la un sistem informatic.[1252] Despre astfel de cazuri, în care s-a aplicat art. 360 CPR, aflăm din practica judiciară. Astfel, într-un caz, „la data de 17.09.2015, inculpata Ţ.A., care a fost prietenă cu A.D.C., a accesat fără drept contul de messenger şi e-mail al acestuia”[1253]; „Pentru a putea sparge conturile, inculpata cunoştea răspunsul la una din întrebările de securitate şi, după mai multe încercări, a aflat răspunsul şi la a doua întrebare de securitate”[1254]; „După accesarea ilegală a acestor conturi, inculpata a schimbat parola de acces şi întrebările de securitate, restricţionând accesarea conturilor de messenger şi e-mail de titular”[1255]; „Ulterior, inculpata Ţ.A. a accesat pagina de Facebook a persoanei vătămate A.D.C., a schimbat parola de acces şi a copiat toate conversaţiile din pagina de mesaje ale acestui cont”[1256]; „Pentru a avea control asupra paginii de Facebook, inculpata a modificat parola de acces”.[1257] Despre un alt caz de acest gen relatează într-un articol de-al său A.V. Iugan: „Martorul B, care corespondase pe Yahoo Messenger anterior cu soția inculpatului, i-a spus inculpatului că user name-ul și parola de la adresa de mail a soției sale ar putea să fie

---

[1247] ZLATI, George. *Utilizarea clandestină a puterii de calcul a sistemelor informatice aparţinând utilizatorilor unor platforme online. Incidenţa dreptului penal*. https://www.penalmente.eu/2017/09/30/utilizarea-clandestina-a-puterii-de-calcul-a-sistemelor-informatice-apartinand-utilizatorilor-unor-platforme-online-incidenta-dreptului-penal/
[1248] Ibidem.
[1249] Ibidem.
[1250] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Editura Solomon, 2020, p. 195. 658 p. ISBN 978-606-8892-62-7.
[1251] TAMAS-ERNO, Peter. Accesarea ilegală a conturilor de Facebook privit din perspectiva dreptului penal. În*: Revista Facultății de Drept Oradea*, 2019, nr. 1, pp. 151-157. ISSN 1582-7585.
[1252] COMAN, Vasile. *Accesarea contului de e-mail şi de Facebook. Noţiunea de date informatice. Forma agravată prevăzută de art. 360 alin. (3) CP*. [citat 06.03.2022] Disponibil: https://www.universuljuridic.ro/accesarea-contului-de-e-mail-si-de-facebook-notiunea-de-date-informatice-forma-agravata-prevazuta-de-art-360-alin-3-cp/
[1253] *Tribunalul Neamț. Sentință penală 56/P din 31.08.2016*. [citat 06.03.2022] Disponibil: https://www.jurisprudenta.com/jurisprudenta/speta-109d7k31/
[1254] Ibidem.
[1255] Ibidem.
[1256] Ibidem.
[1257] Ibidem.

salvate”[1258], „astfel că acesta din urmă a accesat aplicația Yahoo Messenger și a observat că era afișat Yahoo! ID: I@yahoo.com, parola (Password)”[1259] „fiind memorată, iar prin intermediul butonului „Sign in” a deschis aplicația. În acest mod, inculpatul C, ajutat de martorul B, a accesat, fără a avea acordul soției sale”[1260], „G, adresa de poștă electronică a acesteia, având denumirea: I@yahoo.com, comportându-se din punct de vedere informatic”[1261], „ca și cum ar fi fost utilizatorul autorizat G.”[1262] O speță asemănătoare găsim în jurisprudența autohtonă. Astfel, V.A. a fost condamnat în baza lit. c) alin. (2) art. 259 CP RM. La mijlocul lunii septembrie 2005, aflându-se într-o cafenea din mun. Chișinău, acesta a accesat ilegal adresa de poștă electronică ce aparținea lui D.M. și a modificat parola de acces la această adresă. Apoi, V.A., aflând informația necesară din poșta electronică accesată ilegal, a putut intra într-un joc electronic, substituindu-se lui D.M. și modificând parametrii acelui joc și parola de acces la acel joc. Astfel, lui D.M. i-au fost cauzate daune în mărime de 502,80 lei.[1263]

Observăm că, în ultima speță, făptuitorul nu doar a accesat un sistem informatic (și anume – serverul prin intermediul căruia era prestat serviciul de poștă electronică), ci și a obținut posibilitatea de a recurge la informația computerizată din contul de poștă electronică al victimei, în vederea beneficierii de calitățile utile ale acestei informații. În general, indiferent de modalitatea faptică sub care se înfățișează accesul la un sistem informatic, trebuie să stabilim dacă acest acces a avut o continuitate, astfel încât să putem vorbi despre accesul la informația computerizată din acel sistem. Doar într-un asemenea caz putem vorbi despre accesul la informația computerizată în accepția art. 259 CP RM.

În mod similar – indiferent de modalitatea faptică sub care se înfățișează accesul la un calculator, la un suport material de informaţie ori la o rețea informatică – trebuie să stabilim dacă acest acces a avut o continuitate, astfel încât să putem vorbi despre accesul la informația computerizată din acel calculator, din acel suport material de informaţie ori din acea rețea informatică. În lipsa unei astfel de continuități, nu putem vorbi despre accesul la informația computerizată în accepția art. 259 CP RM.

[1258] IUGAN, Andrei Viorel. *Acces fără drept la sisteme informatice și alterarea integrității datelor informatice*. [citat 06.03.2022] Disponibil: https://www.universuljuridic.ro/acces-fara-drept-la-sisteme-informatice-si-alterarea-integritatii-datelor-informatice/
[1259] Ibidem.
[1260] Ibidem.
[1261] Ibidem.
[1262] Ibidem.
[1263] *Decizia Colegiului penal lărgit al CSJ din 13.03.2006. Dosarul nr. 1ra-208/2007*. [citat 06.03.2022] Disponibil: http://jurisprudenta.csj.md/archive_courts/cauta/; *Hotărârea Plenului CSJ din 30.06.2008. Dosarul nr. 4-1re-209/2008*. [citat 06.03.2022] Disponibil: http://jurisprudenta.csj.md/archive_courts/cauta/

Încheiem examinarea noțiunii de acces la informația computerizată cu analiza unui alt aspect nelipsit de interes. Astfel, unele norme corespondente cu art. 259 CP RM, prevăzute de anumite legi penale străine, conțin formulări pe care nu le atestăm în art. 259 CP RM. Spre exemplu, § 1 art. 550bis CP RBl prevede: „Cel care, ştiind că nu este autorizat, accesează un sistem informatic *sau se menţine în acesta* (evid. ns.)”[1264], „este pedepsit cu [închisoarea de la șase luni la doi ani] şi cu o amendă de la douăzeci şi şase [de euro] la douăzeci şi cinci de mii [de euro]”[1265] „sau doar la una din aceste pedepse”.[1266] Prevederi similare conțin art. 615-ter CP RI[1267] și art. 509-1 CP MDL.[1268] La fel ca în art. 259 CP RM, în art. 360 CPR nu sunt utilizate formulări de genul celor din art. 550bis CP RBl, din art. 615-ter CP RI și din art. 509-1 CP MDL. Ca urmare, G. Zlati consideră nereglementată în art. 360 CPR ipoteza menținerii accesului după retragerea ori expirarea autorizării: „În măsura în care după un acces intenționat autorizat sau un acces obținut în mod fortuit (de exemplu, o redirecționare automată a utilizatorului) ori din eroare”[1269] „(de exemplu, agentul crede că interacționează cu propriul sistem informatic), agentul păstrează accesul, rămânând în pasivitate, nu se va putea reține art. 360 C. pen.”[1270]; „În schimb, dacă agentul iese din pasivitate și are o conduită comisivă, s-ar putea considera că discutăm despre un acces prin depășirea limitelor autorizării”.[1271] În concluzie, nu este necesar ca art. 259 CP RM să fie completat după modelul § 1 art. 550bis CP RBl, al art. 615-ter CP RI și al art. 509-1 CP MDL.

În altă ordine de idei, după cum rezultă din dispoziția de la alin. (1) art. 259 CP RM, nu orice acces la informația computerizată intră sub incidența articolului respectiv. Condiția obligatorie este ca accesul la informația computerizată să fie ilegal.

A.S. Amiraslanov, F.M. Abubakirov, A.G. Djafarov sunt de părerea că în partea specială a legii penale sunt descrise fapte cu caracter ilegal; pe cale de consecință, ar fi de prisos să vorbim despre ilegalitate atunci când caracterizăm o infracțiune concretă specificată în partea specială a legii penale.[1272] R. Berdilo pune la îndoială temeinicia unor astfel de păreri.[1273]

[1264] *Codul penal al Regatului Belgiei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html
[1265] Ibidem.
[1266] Ibidem.
[1267] *Codul penal al Republicii Italia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Italia-RO.html
[1268] *Codul penal al Marelui Ducat de Luxemburg*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Luxemburg-RO.html
[1269] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Editura Solomon, 2020, p. 192. 658 p. ISBN 978-606-8892-62-7.
[1270] Ibidem, p. 192.
[1271] Ibidem, p. 192.
[1272] АМИРАСЛАНОВ. А.С. Эволюция понятия убийства в уголовном праве России. În: *Актуальные мировые тренды развития социально-гуманитарного знания. Сборник научных трудов по материалам*

Conform alin. (1) art. 14 CP RM, „infracţiunea este o faptă (acţiune sau inacţiune) prejudiciabilă, prevăzută de legea penală, săvârşită cu vinovăţie şi pasibilă de pedeapsă penală”.[1274] Odată ce o faptă prejudiciabilă este prevăzută de legea penală, rezultă că ea este ilegală. Totuși, așa cum se va putea vedea *infra*, acțiunea de acces la informația computerizată nu epuizează conținutul faptei prejudiciabile prevăzute la art. 259 CP RM. În general, ilegalitatea unei fapte prejudiciabile este reprezentată la nivelul fie al tuturor componentelor acesteia, fie doar al uneia sau al unora dintre componentele faptei prejudiciabile. De exemplu, în cazul infracțiunii de viol (art. 171 CP RM), acțiunea principală de raport sexual nu este ilegală *per se*. Violul este o faptă ilegală deoarece acțiunea principală de raport sexual este însoțită de acțiunea adiacentă concretizată fie în constrângerea fizică sau psihică a persoanei, fie în profitarea de imposibilitatea acesteia de a se apăra ori de a-şi exprima voinţa. Astfel, în cazul violului, ilegalitatea faptei prejudiciabile este reprezentată doar la nivelul acțiunii adiacente.

Este necesar să ne concentrăm pe semantismul termenului „ilegal” în contextul particular al infracțiunilor prevăzute de art. 259 CP RM.

Conform alin. (3) art. 34 din Constituția Republicii Moldova, „dreptul la informaţie nu trebuie să prejudicieze măsurile de protecţie a cetăţenilor sau siguranţa naţională”.[1275] Interpretarea *per a contrario* a acestei prevederi ne determină să afirmăm că, în cazul infracțiunilor prevăzute la art. 259 CP RM, făptuitorul exercită abuziv dreptul la informaţie, prejudiciind măsurile de protecţie a cetăţenilor sau siguranţa naţională. În asemenea împrejurări, legiuitorul apreciază ca prejudiciabil un asemenea comportament, având ca reper prevederea din alin. (2) art. 54 din Constituția Republicii Moldova: „Exerciţiul drepturilor şi libertăţilor nu poate fi supus altor restrângeri decât celor prevăzute de lege, care corespund normelor unanim recunoscute ale dreptului internaţional”[1276] „şi sunt necesare în interesele securităţii naţionale, integrităţii teritoriale, bunăstării economice a ţării, ordinii publice”[1277], „în scopul prevenirii tulburărilor în masă şi infracţiunilor, protejării drepturilor, libertăţilor şi demnităţii altor persoane”[1278], „împiedicării divulgării informaţiilor confidenţiale sau garantării autorităţii şi

---

Международной научно-практической конференции, 2017, с. 110-113. ISBN 978-5-9500429-6-6; АБУБАКИРОВ, Ф.М., ДЖАФАРОВ, А.Г. Достаточно ли признаков, характеризующих убийство по УК РФ? În: *Законность и правопорядок в современном обществе*, 2016, № 31, с. 115-119. ISBN 978-5-907088-23-8.

[1273] BERDILO, Rodica. *Răspunderea penală pentru omorul săvârșit în stare de afect*. Chișinău: Tipografia Centrală, 2021, p. 56. 399 p. ISBN 978-9975-104-94-4.

[1274] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

[1275] Constituția Republicii Moldova. În: *Monitorul Oficial al Republicii Moldova*, 1994, nr. 1, 140.

[1276] Ibidem.

[1277] Ibidem.

[1278] Ibidem.

imparţialităţii justiţiei”.[1279] În acest plan, este utilă următoarea aserțiune din Hotărârea Curții Constituționale a Republicii Moldova nr. 19 din 22.06.2015 pentru interpretarea articolului 34 alin. (3) din Constituția Republicii Moldova: „În sensul articolului 34 alin. (3) din Constituție: restrângerea dreptului la informație poate avea loc doar atunci când are la bază un scop real și justificat”[1280] „de protecție a unui interes legitim privind protecția cetățenilor sau siguranța națională, iar interesul public pentru aflarea informației nu prevalează”[1281]; „orice restrângere a accesului la informație, inclusiv categoriile de informații, specifice și limitate”[1282], „care nu pot fi dezvăluite în vederea protecției cetățenilor sau siguranței naționale, trebuie să fie prevăzută de lege”[1283] „și necesară într-o societate democratică pentru protecția unui interes legitim; justificarea interesului legitim se fundamentează pe gravitatea prejudicierii acestuia în cazul publicării unor informații”[1284], „autoritățile publice urmând să demonstreze că divulgarea informației ar amenința în mod grav protecția cetățenilor sau siguranța națională”.[1285] Reieșind din această aserțiune, este prezumabil că interdicția de exercitare abuzivă a dreptului la informaţie, stabilită în art. 259 CP RM, îndeplinește următoarele condiții: 1) are la bază un scop real și justificat de protecție a unui interes legitim privind protecția cetățenilor sau siguranța națională; 2) interesul public pentru aflarea informației computerizate nu prevalează; 3) orice restrângere a accesului la informația computerizată, inclusiv categoriile de informații, specifice și limitate, care nu pot fi dezvăluite în vederea protecției cetățenilor sau siguranței naționale, este prevăzută de lege și necesară într-o societate democratică pentru protecția unui interes legitim. Ca urmare, se poate susține că interdicția de exercitare abuzivă a dreptului la informaţie, stabilită în art. 259 CP RM, respectă exigența stabilită în alin. (3) art. 1 CP RM: „Prezentul cod se aplică în conformitate cu prevederile Constituţiei Republicii Moldova [...]”.

Mai sus am afirmat că termenul „ilegal”, utilizat în art. 259 CP RM în raport cu acțiunea de acces la informația computerizată, își găsește concretizarea în sintagma „al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depășește limitele autorizării ori nu are permisiunea persoanei competente să folosească”[1286] „să administreze sau să controleze un

[1279] Ibidem.
[1280] Hotărârea Curții Constituționale a Republicii Moldova pentru interpretarea articolului 34 alin. (3) din Constituția Republicii Moldova: nr. 19 din 22.06.2015. În: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 330-331, 33.
[1281] Ibidem.
[1282] Ibidem.
[1283] Ibidem.
[1284] Ibidem.
[1285] Ibidem.
[1286] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

sistem informatic ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic”[1287], folosită în dispoziția de la alin. (1) art. 259 CP RM.

Ca paradigmă pentru sintagma sus-menționată din alin. (1) art. 259 CP RM a servit formularea din alin. (2) art. 35 al Legii României nr. 161/2003: „În sensul prezentului titlu (se are în vedere Titlul III „Prevenirea și combaterea criminalității informatice” – *n.a.*), acționează fără drept”[1288] „persoana care se află în una dintre următoarele situații: a) nu este autorizată, în temeiul legii sau al unui contract; b) depășește limitele autorizării”[1289]; „c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra”[1290] „sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic”.[1291] Până la intrarea în vigoare la 01.02.2014 a Legii României nr. 187 din 24.10.2012 pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal[1292], art. 42 al Legii României nr. 161/2003 (care a fost abrogat) avea următorul conținut: „Accesul, fără drept, la un sistem informatic constituie infracţiune şi se pedepseşte cu închisoare de la 3 luni la 3 ani sau cu amendă”[1293]; „(2) Fapta prevăzută la alin. (1), săvârşită în scopul obţinerii de date informatice, se pedepseşte cu închisoare de la 6 luni la 5 ani”[1294]; „(3) Dacă fapta prevăzută la alin. (1) sau (2) este săvârşită prin încălcarea măsurilor de securitate, pedeapsa este închisoarea de la 3 la 12 ani”.[1295]

Cele trei ipoteze de ilegalitate, specificate în alin. (1) art. 259 CP RM și în alin. (2) art. 35 al Legii României nr. 161/2003, decurg din următoarea definiție formulată la lit. d) art. 2 al Directivei 2013/40/UE: „„fără a avea dreptul” înseamnă un comportament menționat de prezenta directivă, inclusiv accesarea [...]”[1296] „fără autorizare din partea proprietarului sau a unui alt titular de drepturi, a sistemului sau a unei părți a acestuia, sau care nu este permis în temeiul legislației naționale”.[1297] De asemenea, în pct. 38 din Raportul explicativ la Convenția de la

---

[1287] Ibidem.
[1288] Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.
[1289] Ibidem.
[1290] Ibidem.
[1291] Ibidem.
[1292] Legea României pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal: nr. 187 din 24.10.2012. În: *Monitorul Oficial al României*, 2012, nr. 757.
[1293] Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.
[1294] Ibidem.
[1295] Ibidem.
[1296] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en
[1297] Ibidem.

Budapesta, se menționează: „Expresia „fără drept” își trage sensul din contextul în care este folosită”[1298]; „Astfel, fără a restricționa modul în care părțile pot implementa conceptul în dreptul lor intern, acesta se poate referi la comportamente întreprinse fără autorizare”[1299] „(legislativă, executivă, administrativă, judiciară, contractuală sau consensuală) sau comportamente care altfel nu sunt acoperite de justificările”[1300] „stabilite prin lege sau de principiile relevante în temeiul dreptului intern”.[1301]

Considerăm că cele trei ipoteze de ilegalitate, specificate în alin. (1) art. 259 CP RM, sunt suficiente pentru a asigura atât condiția de claritate și previzibilitate a legii penale, cât și condiția de prevenire eficientă a eludării legii penale. Ultimei dintre aceste condiții nu-i corespunde, spre exemplu, definiția de la lit. г) art. 1 al Acordului de cooperare între statele membre ale Comunității Statelor Independente în lupta împotriva infracțiunilor din domeniul informației informatice: „acces ilegal – acces neautorizat la informația computerizată”.[1302] În mod similar, accesul ilegal la informaţia computerizată era înțeles în art. 176[1] CP RM din 1961: „Accesul ilegal *(nesancţionat)* (evid. ns.) la informaţia ce se păstrează în sistemul computerizat, cu încălcarea sistemului de protecţie”.[1303]

Cu regret, la lit. b) alin. (2) art. 28 al Legii nr. 1069/2000, se menționează despre: „pătrunderea *neautorizată* (evid. ns.) în sistemele şi reţelele informatice publice sau private [...]”.[1304] În alin. (3) art. 4 din aceeași lege, se menționează: „Se interzice accesul şi conectarea *neautorizate* (evid. ns.) la sistemele şi reţelele informatice.”[1305] Asemenea formulări, care se deosebesc de termenii folosiți pentru caracterizarea acțiunii principale în art. 259 CP RM, pot induce în eroare în procesul de calificare a infracțiunilor. O abordare asemănătoare cu cea din Legea nr. 1069/2000 o întâlnim în legile penale ale altor state (de exemplu, în alin. (1) art. 266 CP RCr[1306] și în alin. (1) art. 337C CP RMa[1307]). În toate aceste cazuri exemplificate, nu este clar dacă este sancționabil accesul la informația computerizată care se realizează fie cu depășirea

---

[1298] *Explanatory Report to the Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/16800cce5b
[1299] Ibidem.
[1300] Ibidem.
[1301] Ibidem.
[1302] *Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации*. [citat 06.03.2022] Disponibil: https://docs.cntd.ru/document/902140948
[1303] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
[1304] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[1305] Ibidem.
[1306] *Codul penal al Republicii Croaţia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Croatia-RO.html
[1307] *Codul penal al Republicii Malta*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Malta-RO.html

limitelor autorizării, fie „fără permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic”[1308] „ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic.”[1309] Ceea ce denotă că reglementările penale exemplificate nu asigură ocrotirea eficientă a ordinii de drept.

Pentru a percepe mai bine ce presupun cele trei ipoteze de ilegalitate, specificate în alin. (1) art. 259 CP RM, îl vom cita pe Gh. Alecu: „Accesul fără drept la un sistem informatic înseamnă, în sensul legii, că persoana respectivă se află în una din următoarele situaţii”[1310]: „a) nu este autorizată, în temeiul legii sau al unui contract. Persoanele care operează în bazele de date cu personalul unei instituţii o fac în baza autorizării primite de la conducerea instituţiei”[1311], „deoarece ele respectă legislaţia muncii şi pe cea privitoare la datele personale; b) depăşeşte limitele autorizării”[1312]; „Depăşirea limitelor autorizării poate însemna accesul la resurse din Intranetul companiei/instituţiei aflate la nivele de acces superioare cele permise utilizatorului”[1313]; „c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic”[1314] „ori de a desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic.”[1315]

Anumite indicii în ceea ce privește *prima dintre aceste ipoteze* – lipsa autorizării de a accesa informația computerizată – găsim în opinia exprimată de către L. Gîrla și Iu. Tabarcea: „Accesul va fi neautorizat atunci când subiectul nu are un temei legal pentru utilizarea resurselor informatice”[1316] „sau pentru deținerea acestora, precum și în cazurile în care o persoană, deși accesează informația computerizată legal”[1317], „o face fără a respecta procedura stabilită de proprietarul informației sau de lege”.[1318] În termeni asemănători se exprimă M. Dobrinoiu.[1319]

În textul Legii nr. 1069/2000 pot fi identificate anumite indicii care ne ajută să pătrundem mai bine în esența noțiunii „lipsa autorizării de a accesa informația computerizată”: „Orice persoană este în drept să deţină date, programe şi echipamente, precum şi să prelucreze date şi

---

[1308] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1309] Ibidem.
[1310] ALECU, Gheorghe. *Instituţii de drept penal: partea generală şi partea specială*. Constanţa: Ovidius University Press, 2010, p. 512. 635 p. ISBN 978-973-614-579-7.
[1311] Ibidem, p. 512.
[1312] Ibidem, p. 512.
[1313] Ibidem, p. 513.
[1314] Ibidem, p. 513.
[1315] Ibidem, p. 513.
[1316] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 16. 592 с. ISBN 978-9975-4158-2-8.
[1317] Ibidem, с. 16.
[1318] Ibidem, с. 16.
[1319] DOBRINOIU, Maxim. Considerații tehnice și juridice privind reținerea infracțiunii de acces ilegal la un sistem informatic în situația interogării unei baze de date prin depășirea limitelor autorizării. În: *Penalmente Relevant*, 2021, nr. 1, 2021, pp. 70-78. ISSN 2501-1367.

programe”[1320], „cu obţinerea unor produse informatice pentru uz propriu, dacă aceasta nu contravine prevederilor prezentei legi”[1321] (alin. (1) art. 16); „Proprietarul produselor informatice are dreptul de a autoriza persoane care să posede”[1322], „utilizeze şi/sau să administreze aceste produse, fiind în drept să efectueze orice operaţiune legală cu acestea şi în privinţa acestora”[1323] (alin. (4) art. 29).

La cea de-*a doua ipoteză a ilegalității* – depășirea limitelor autorizării de a accesa informația computerizată – se referă următoarea explicație din Decizia Înaltei Curți de Casaţie și Justiţie a României nr. 68 din 29.09.2021 privind dispoziţiile art. 360 alin. (1) din Codul penal: „Analiza depăşirii limitelor autorizării implică, pe de o parte, stabilirea existenţei autorizării legale sau contractuale, iar, pe de altă parte, determinarea conţinutului acesteia”[1324], „singurul în măsură să furnizeze criteriile obiective în raport cu care se poate concluziona asupra caracterului legal sau ilegal al accesului la sistemul informatic”[1325]; „În acest sens, în cadrul examenului realizat, organul judiciar verifică, în temeiul actelor normative care reglementează competenţele şi atribuţiile de serviciu într-un anumit domeniu de activitate”[1326], „al regulamentelor de ordin intern sau al clauzelor specifice din contractele de muncă şi al prevederilor din fişele postului, limitele autorizării”[1327], „dar şi conduita materială efectivă a agentului pe durata accesului la sistemul informatic, toate acestea constituind aspecte de natură strict factuală, ce diferă de la caz la caz”[1328], „în funcţie de particularităţile speţei deduse judecăţii, şi care urmează a fi stabilite de instanţa învestită pe baza materialului probator administrat în cauză”[1329], „care va fundamenta concluzia depăşirii sau a nedepăşirii respectivelor limite şi, implicit,a caracterului legal ori ilegal al accesului”.[1330]

Așadar, depășirea limitelor autorizării de a accesa informația computerizată presupune că făptuitorul deține autorizarea de a accesa informația computerizată, însă acesta nu se conformează autorizării respective, arogându-și împuterniciri care nu i-au fost acordate. Analiza unor prevederi relevante dintr-un act normativ ne permite să înțelegem care pot fi împrejurările în care se depășesc limitele autorizării de a accesa informația computerizată. Astfel, Hotărârea

[1320] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[1321] Ibidem.
[1322] Ibidem.
[1323] Ibidem.
[1324] Decizia Înaltei Curți de Casație și Justiție a României referitoare la interpretarea dispozițiilor art. 360 alin. (1) din Codul penal: nr. 68 din 29.09.2021. În: *Monitorul Oficial al României*, 2022, nr. 56.
[1325] Ibidem.
[1326] Ibidem.
[1327] Ibidem.
[1328] Ibidem.
[1329] Ibidem.
[1330] Ibidem.

Guvernului nr. 153 din 25.08.2021 pentru aprobarea Conceptului Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat" și a Regulamentului privind modul de ținere a Registrului resurselor și sistemelor informaționale de stat prevede, printre altele: „Utilizatorii SI RRSIS (adică ai Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat" – *n.a.*)"[1331] „vor fi autorizați să acceseze *doar blocurile funcționale și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia* (evid. ns.)"[1332] (pct. 46 din Anexa nr. 1); „Utilizatorii RRSIS (adică ai Registrului resurselor și sistemelor informaționale de stat – *n.a.*) sunt autorizați să acceseze"[1333] „*doar funcționalitățile și datele pentru care au permisiunile necesare, conform rolurilor fiecăruia* (evid. ns.)"[1334] (pct. 43 din Anexa nr. 2). De asemenea, Hotărârea Guvernului nr. 1123 din 14.12.2010 privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal prevede, printre altele: „Drepturile de acces ale utilizatorilor la sistemele informaţionale de date cu caracter personal sunt revizuite cu regularitate"[1335] „pentru asigurarea faptului că nu au fost acordate drepturi de acces neautorizate (maximum peste fiecare şase luni)"[1336] „şi *după oricare schimbare de statut al utilizatorului* (evid. ns.)"[1337] (pct. 48); „Fiecare metodă de acces de la distanţă la sistemele informaţionale de date cu caracter personal se autorizează de persoanele responsabile ale deţinătorilor de date cu caracter personal şi permisă *doar utilizatorilor, cărora aceasta le este necesar pentru îndeplinirea obiectivelor stabilite* (evid. ns.)"[1338] (pct. 55). Dispoziții asemănătoare găsim în alte acte normative: Hotărârea Guvernului nr. 601 din 12.08.2020 cu privire la aprobarea Conceptului Sistemului informațional de management în educație[1339]; Hotărârea Guvernului nr. 169 din 08.09.2021 cu privire la Registrul de stat al serviciilor publice[1340], etc.

Ultima, *a treia ipoteză a ilegalității* presupune realizarea accesului la informația computerizată fără permisiunea persoanei competente să folosească, să administreze sau să

[1331] Hotărârea Guvernului pentru aprobarea Conceptului Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat" și a Regulamentului privind modul de ținere a Registrului resurselor și sistemelor informaționale de stat: nr. 153 din 25.08.2021. În: *Monitorul Oficial al Republicii Moldova*, 2021, nr. 226-229, 415.
[1332] Ibidem.
[1333] Ibidem.
[1334] Ibidem.
[1335] Hotărârea Guvernului privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal: nr. 1123 din 14.12.2010. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 254-256, 1282.
[1336] Ibidem.
[1337] Ibidem.
[1338] Ibidem.
[1339] Hotărârea Guvernului cu privire la aprobarea Conceptului Sistemului informațional de management în educație: nr. 601 din 12.08.2020. În: *Monitorul Oficial al Republicii Moldova*, 2020, nr. 212-220, 746.
[1340] Hotărârea Guvernului cu privire la Registrul de stat al serviciilor publice: nr. 169 din 08.09.2021. În: *Monitorul Oficial al Republicii Moldova*, 2021, nr. 230-237, 436.

controleze un sistem informatic ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic. Această ipoteză implică îndeplinirea următoarelor două condiții: 1) făptuitorul nu are permisiunea de a accesa informația computerizată; 2) o asemenea permisiune o acordă persoana competentă „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."[1341]

Până acum am analizat ilegalitatea accesului la informația computerizată, privită drept condiție de aplicare a art. 259 CP RM. În cele ce urmează vom examina contrateza – legalitatea accesului la informația computerizată – privită drept condiție de neaplicare a art. 259 CP RM. În acest context, M. Dobrinoiu susține: „Fiind o trăsătură caracteristică comună a tuturor infracţiunilor informatice, cerinţa expresă ca fapta să fie comisă „fără drept" reflectă, în mod logic"[1342], „posibilitatea ca o faptă în legătură cu un sistem informatic să nu fie întotdeauna considerată o infracţiune *per se*"[1343], „ci şi un act legitim sau justificat chiar dacă nu ne aflăm în una din cauzele care înlătură caracterul penal al faptei".[1344]

Interpretarea în sens invers *(per a contrario)* a sintagmei „al unei persoane care nu este autorizată în temeiul legii sau al unui contract, 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"[1345], utilizată în dispoziția de la alin. (1) art. 259 CP RM, ne determină să afirmăm că persoana, care realizează accesul la informația computerizată, nu este pasibilă de răspundere în baza acestui articol în oricare din următoarele cazuri: 1) „este autorizată în temeiul legii sau al unui contract"[1346]; 2) „nu depășește limitele autorizării"[1347]; 3) „are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic." [1348]

[1341] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1342] DOBRINOIU, Maxim. Accesul ilegal la poşta electronică. În: *Revista de Drept Penal*, 2008, nr. 3, pp. 122-125. ISSN 1223-0790.
[1343] Ibidem.
[1344] Ibidem.
[1345] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1346] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1347] Ibidem.
[1348] Ibidem.

Fiind pe poziții apropiate, S. Brînza și V. Stati dezvăluie conținutul noțiunii „acces legal la informația computerizată”: „De exemplu, nu poate avea un caracter ilegal accesul care a fost autorizat de către proprietarul sau alt posesor al sistemului informatic vizat”[1349]; „[...] La fel, nu poate fi considerată infracţiune nici interacţionarea cu un sistem informatic care permite accesul liber şi gratuit al publicului”[1350] „(de exemplu, reţelele Wi-Fi neprotejate sau care oferă servicii de comunicaţii electronice „la liber”.”[1351] L. Gîrla și Iu. Tabarcea prezintă exemple din aceeași categorie: „Accesul se consideră autorizat în următoarele cazuri: 1) accesul a fost autorizat de către proprietarul sau posesorul resurselor informaționale sau al sistemelor informatice”[1352], „al tehnologiilor și mijloacelor de asigurare a acestora în vederea verificării sau protejării sistemelor informatice”[1353]; „2) accesul la resursele informaționale ale sistemelor informatice publice și private este realizat de către organele statului abilitate de lege în vederea asigurării securității naționale”[1354], „în cursul urmăririi penale sau în procesul de desfășurare a activităților speciale de investigaţii; 3) accesul în legătură cu activitățile uzuale și legale de proiectare a sistemelor informatice”[1355], „cu activitățile de funcționare curentă a sistemelor informatice sau cu activitățile comerciale licite; 4) accesul pentru a obține informații despre propria persoană”.[1356]

În legătură cu ultimele trei exemple prezentate de către L. Gîrla și Iu. Tabarcea, trebuie să precizăm că prezența unor scopuri legitime nu este suficientă, fiind necesare toate celelalte condiții care asigură respectarea legalității. Or, de exemplu, în conformitate cu alin. (3) art. 28 al Legii nr. 1069/2000, „în scopul asigurării securităţii naţionale, organele abilitate au drept de acces la resursele informaţionale din sistemele informatice publice sau private. În procesele penale”[1357], „organele menţionate pot, în baza mandatului emis de procuror, intercepta reţelele informatice, utilizând aparatajul tehnic al proprietarului sistemului informatic.”[1358] Pentru a fi interpretată la justa valoare, această dispoziție trebuie coroborată cu alin. (1) art. 7 din Codul de procedură penală al Republicii Moldova: „Procesul penal se desfăşoară în strictă conformitate cu principiile şi normele unanim recunoscute ale dreptului internaţional, cu tratatele internaţionale

[1349] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 351. 1300 p. ISBN 978-9975-53-470-3.
[1350] Ibidem, p. 351.
[1351] Ibidem, p. 351.
[1352] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 16. 592 с. ISBN 978-9975-4158-2-8.
[1353] Ibidem, с. 16.
[1354] Ibidem, с. 16.
[1355] Ibidem, с. 16.
[1356] Ibidem, с. 16.
[1357] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[1358] Ibidem.

la care Republica Moldova este parte”[1359], „cu prevederile Constituţiei Republicii Moldova şi ale prezentului cod”.[1360] De asemenea, conform lit. a) art. 3 al Legii nr. 59 din 29.03.2012 privind activitatea specială de investigaţii, „activitatea specială de investigaţii se bazează pe [principiul] legalităţii”.[1361]

Prin prisma principiului legalității trebuie privite și alte reglementări care vizează accesul la informația computerizată. Este posibil ca prevederile, care reglementează accesul la informația computerizată să aibă chiar un caracter local, fiind emise/adoptate în cadrul unei instituții, întreprinderi sau organizații. La un asemenea exemplu se referă T. Medeanu și A. Crăciunescu: „Accesarea unor date informatice stocate sau vehiculate de altă persoană care are acces la acelaşi computer, nu reprezintă infracţiunea de acces ilegal la un sistem informatic, în accepţiunea legii penale, ci o încălcare”[1362] „a reglementărilor din instituţia respectivă, pe linia protejării informaţiilor”.[1363] Nu agreăm o asemenea poziție. Așa cum am relevat anterior, prevederile din actele normative subordonate legii, dacă dezvoltă prevederile unor legi, corespund condiției „este autorizată în temeiul legii”[1364] din alin. (1) art. 259 CP RM. Formularea „este autorizată în temeiul legii”[1365] este mai largă decât formularea „este autorizată prin lege”. Dacă ultima dintre aceste formulări ar fi folosită în alin. (1) art. 259 CP RM, atunci am fi de acord că prevederile, care reglementează accesul la informația computerizată, ar trebui să fie cuprinse exclusiv în textul unei legi.

Persoana, care realizează accesul la informația computerizată, se află în câmpul legalității nu doar atunci când este autorizată în temeiul legii sau al unui contract ori atunci când nu depășește limitele autorizării, ci și atunci când are permisiunea – expresă sau tacită – din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic. La baza unei astfel de interpretări care rezultă din alin. (1) art. 259 CP RM, este pusă dispoziția cu valoare de principiu din art. 55 al Constituției Republicii Moldova: „Orice

---

[1359] Codul de procedură penală al Republicii Moldova: nr. 122 din 14.03.2003. În: *Monitorul Oficial al Republicii Moldova*, 2003, nr. 104-110, 447.
[1360] Ibidem.
[1361] Legea privind activitatea specială de investigaţii: nr. 59 din 29.03.2012. În: *Monitorul Oficial al Republicii Moldova*, 2012, nr. 113-118, 373.
[1362] MEDEANU, Tiberiu, CRĂCIUNESCU, Adrian. Accesul ilegal la un sistem informatic elemente constitutive şi delimitarea de alte infracţiuni. În: *Sesiunii ştiinţifice internaţionale „Uniunea Europeană – spaţiu de libertate, securitate şi justiţie” (Academia de Poliţie, Bucureşti, 23 mai 2013)*. Bucureşti: Editura Universitară, pp. 28-37. ISBN 978-606-591-723-1.
[1363] Ibidem.
[1364] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1365] Ibidem.

persoană îşi exercită drepturile şi libertăţile constituţionale cu bună-credinţă, fără să încalce drepturile şi libertăţile altora”.[1366]

Atunci când este vorba despre persoane între care există un anumit climat de încredere, poate fi suficientă permisiunea tacită de a accesa informația computerizată. În context, S. Brînza și V. Stati menționează: „Accesul la informaţia computerizată aparţinând ambilor soţi de către unul dintre aceştia nu poate fi considerat ilegal atât timp cât calculatorul, suportul material de informaţie”[1367], „sistemul sau reţeaua informatică este în mod uzual folosită de către fiecare dintre aceştia, iar informaţia computerizată stocată nu este personalizată”[1368] „sau semnalizată prin criptare sau protejare împotriva deschiderii. [...] Dacă ne aflăm în cazul unui computer la care lucrează în mod curent două sau mai multe persoane”[1369], „se admite faptul că acestea accesează respectivul sistem informatic legal, fiind beneficiarele unei aprobări prealabile sau ale unei înţelegeri”[1370]; „În aceste condiţii, fapta uneia dintre persoane de a accesa informaţia computerizată, stocată sau vehiculată de o alta”[1371], „în interiorul aceluiaşi computer, nu mai poate fi calificată în baza [...] art. 259 CP RM”.[1372]

În altă privință, după părerea lui V. Stati, în cazul infracţiunilor prevăzute la art. 259 CP RM, fapta prejudiciabilă „constă în acţiunea principală de acces ilegal la informaţia computerizată, însoţită de acţiunea adiacentă de distrugere”[1373], „deteriorare, modificare, blocare sau copiere a informaţiei, de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice”.[1374] În opinia lui S. Brînza și V. Stati, „doar accesul ilegal la informaţia computerizată este insuficient pentru a întregi fapta prejudiciabilă prevăzută la [...] art. 259 CP RM”[1375]; „[...] Acţiunea principală se poate afla în legătură cauzală cu urmările prejudiciabile numai dacă este însoţită de acţiunea adiacentă”.[1376] Păreri similare au L. Gîrla și Iu. Tabarcea[1377], L. Dumneanu și

---

[1366] Constituția Republicii Moldova. În: *Monitorul Oficial al Republicii Moldova*, 1994, nr. 1, 140.
[1367] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 351. 1300 p. ISBN 978-9975-53-470-3.
[1368] Ibidem, p. 351.
[1369] Ibidem, p. 351.
[1370] Ibidem, p. 351.
[1371] Ibidem, p. 351.
[1372] Ibidem, p. 351.
[1373] BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005, p. 496. 804 p. ISBN 9975-79-324-X. STATI, Vitalie. Răspunderea penală pentru infracţiunile în domeniul informaticii şi telecomunicaţiilor. În: *Analele ştiinţifice ale Universităţii de Stat din Moldova, Seria „Ştiinţe socioumanistice”*, 2005, Vol. I, pp. 387-394. ISSN 1811-2668.
[1374] Ibidem.
[1375] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 354. 1300 p. ISBN 978-9975-53-470-3.
[1376] Ibidem, p. 354.
[1377] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 16. 592 с. ISBN 978-9975-4158-2-8.

D. Gurev.[1378] Astfel de puncte de vedere își găsesc implicit confirmarea în dispoziția de la lit. b) alin. (2) art. 28 al Legii nr. 1069/2000: „În scopul asigurării protecţiei datelor şi evitării infracţiunilor ce ţin de domeniul informaticii, se interzice: [...] pătrunderea neautorizată”[1379] „în sistemele şi reţelele informatice publice sau private *pentru a* [...] *modifica, deteriora, distruge date, programe şi echipamente* (evid. ns.)”.[1380]

S. Brînza și V. Stati prezintă un exemplu care ilustrează efectele pe care insuficiența acțiunii de acces ilegal la informaţia computerizată le are asupra procesului de calificare a infracțiunilor: „Dacă făptuitorul accesează aplicaţia de poştă electronică, distrugând, deteriorând, modificând, blocând sau copiind informaţia computerizată ori dereglând funcţionarea calculatoarelor”[1381], „a sistemului informatic sau a reţelei informatice, cauzând prin aceasta daune în proporţii mari, atunci fapta poate fi calificată în baza [...] art. 259 CP RM”[1382]; „Însă, dacă făptuitorul accesează aplicaţia de poştă electronică, doar luând cunoştinţă de conţinutul informaţiei primite”[1383], „transmise ori stocate de victimă, atunci va lipsi temeiul aplicării [...] art. 259 CP RM”.[1384] O viziune apropiată are S. Copețchi.[1385] Într-adevăr, dacă intenția făptuitorului se limitează la săvârșirea accesului ilegal la informaţia computerizată, iar această intenție se realizează, atunci lipsește temeiul aplicării art. 259 CP RM. În cazul dat, este lipsă latura obiectivă a infracțiunii în deplinătatea sa, motiv pentru care vorbim despre lipsa componenței de infracțiune.

În doctrina autohtonă sunt exprimate păreri care diferă de cele ale lui S. Brînza, V. Stati, L. Gîrla, Iu. Tabarcea, L. Dumneanu și D. Gurev, specificate mai sus. Astfel, A. Barbăneagră și Gh. Alecu afirmă în legătură cu infracțiunile prevăzute la art. 259 CP RM: „Latura obiectivă a infracţiunii se realizează printr-o activitate de acces nesancţionat, fără drept, la un sistem informatic”[1386]; „[...] Modalităţile de realizare a accesului ilegal la informaţiile computerizate sunt: distrugerea, deteriorarea, modificarea, blocarea, copierea informaţiei; degradarea funcţionării calculatoarelor”[1387]; „degradarea funcţionării sistemului; degradarea funcţionării

---

[1378] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM, p. 96. 261 p. ISBN 978-9975-158-29-9.
[1379] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[1380] Ibidem.
[1381] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 354. 1300 p. ISBN 978-9975-53-470-3.
[1382] Ibidem, p. 354.
[1383] Ibidem, p. 355.
[1384] Ibidem, p. 355.
[1385] COPEȚCHI, Stanislav. Corespondenţa electronică: obiect imaterial al infracţiunii prevăzute la art. 178 CP RM? În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2017, nr. 8, pp. 116-122. ISSN 1814-3199.
[1386] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 567. 860 p. ISBN 978-9975-105-20-0.
[1387] Ibidem, p. 568.

reţelei informatice”.[1388] O astfel de poziție ar trebui susținută dacă ar fi exprimată, spre exemplu, cu privire la infracțiunea prevăzută la alin. (1) art. 237 CP RSlo: „Persoana care, în desfăşurarea operaţiunilor comerciale, fără autorizaţie, *introduce, modifică, ascunde, şterge sau distruge orice date sau programe de calculator”*[1389] *„sau în orice alt fel accesează* (evid. ns.) un sistem informatic în mod ilegal pentru a obţine beneficii materiale ilegale pentru sine sau pentru o terţă persoană”[1390] „sau pentru a provoca daune bunurilor altei persoane, se sancţionează cu pedeapsa închisorii de până la trei ani”.[1391] Sintagma „sau în orice alt fel accesează” din această normă demonstrează că introducerea, modificarea, ascunderea, ştergerea sau distrugerea oricăror date sau programe de calculator nu are un caracter de sine stătător, ci reprezintă o listă de exemple de modalități de manifestare a accesului ilegal la datele sau programele de calculator.

În dispoziția de la alin. (1) art. 259 CP RM nu este utilizată sintagma „sau în orice alt fel accesează” ori sintagme similare. În această normă este folosită sintagma „dacă este însoţit de”, care denotă că acțiunea principală este însoțită de acțiunea adiacentă. O concepție apropiată este promovată în alin. (3) art. 216 CP RBu[1392] și în alin. (1) § 247 CP RSl.[1393]

Dacă legiuitorul ar fi dorit să prezinte în alin. (1) art. 259 CP RM metodele acțiunii principale, atunci ar fi recurs la altfel de formulări. În partea specială a Codului penal al Republicii Moldova pot fi identificate asemenea formulări: „Aceleaşi acţiuni [...] *săvârşite prin* (evid. ns.) incendiere, explozie sau prin o altă modalitate periculoasă”[1394] (alin. (2) art. 197); „Introducerea pe sau scoaterea de pe teritoriul Republicii Moldova a mărfurilor, prin locuri stabilite pentru control vamal, *prin* (evid. ns.) tăinuire de controlul vamal”[1395], „prin ascundere în locuri special pregătite sau adaptate în acest scop, ori cu folosirea frauduloasă a documentelor sau a mijloacelor de identificare vamală”[1396], „ori prin nedeclarare sau declarare neautentică în documentele vamale sau în alte documente de trecere a frontierei, dacă valoarea mărfurilor este mai mare de 8000 de unități convenționale”[1397] (alin. (1) art. 248); „Instigarea la ură sau violență, *manifestată prin* (evid. ns.) îndemnuri publice, diseminare a informației sau alte forme de

---

[1388] Ibidem, p. 568.
[1389] *Codul penal al Republicii Slovenia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovenia-RO.html
[1390] Ibidem.
[1391] Ibidem.
[1392] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[1393] *Codul penal al Republicii Slovace*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovacia-RO.html
[1394] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1395] Ibidem.
[1396] Ibidem.
[1397] Ibidem.

informare a publicului”[1398], „inclusiv prin intermediul mass-mediei, în formă scrisă, desen sau imagine, sau prin intermediul unui sistem informatic, împotriva unei categorii de persoane pe motive de prejudecată”[1399] (art. 346).

Astfel, se poate susține că în art. 259 CP RM s-a renunțat la concepția privitoare la compunerea monomembră a faptei prejudiciabile care era consacrată în art. 176[1] CP RM din 1961: „1. Accesul ilegal (nesancţionat) la informaţia ce se păstrează în sistemul computerizat, cu încălcarea sistemului de protecţie [...]”[1400]; „2. Aceeaşi acţiune săvârşită din imprudenţă, care a cauzat nimicirea sau blocarea informaţiei, precum şi scoaterea din funcţiune a utilajului computerizat ori alte urmări grave”.[1401] Observăm că, în această concepție, nimicirea sau blocarea informaţiei, precum şi scoaterea din funcţiune a utilajului computerizat, apar ca manifestări ale variantei agravate a infracțiunii, nu ca manifestări ale variantei-tip ale infracțiunii. Astfel, în art. 176[1] CP RM din 1961, nimicirea sau blocarea informaţiei, precum şi scoaterea din funcţiune a utilajului computerizat, erau privite ca elemente circumstanțiale, nu ca elemente obligatorii în structura infracțiunii. În anumite privințe această concepție se regăsește în art. 323-1 CP RFr[1402] și în art. 509-1 CP MDL.[1403]

Totuși, trebuie să subliniem că o asemenea concepție nu este sugerată de actele cu vocație internațională în materie. Conform acestor acte, „distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”[1404] este menționată nu în contextul infracțiunilor cu denumirea marginală de acces ilegal la informația computerizată/la sistemul informatic, ci în contextul altor infracțiuni.

De exemplu, în Convenția de la Budapesta, alin. 1 art. 4 „Afectarea integrităţii datelor” prevede: „Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern”[1405], „fapta comisă intenţionat şi fără drept *de a distruge, şterge, deteriora, modifica sau elimina date informatice* (evid. ns.)”.[1406] Art. 5 „Afectarea integrităţii sistemului” din aceeași convenție prevede: „Fiecare parte va adopta măsurile legislative şi alte măsuri care sunt necesare pentru a incrimina ca infracţiune, în

---

[1398] Ibidem.
[1399] Ibidem.
[1400] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
[1401] Ibidem.
[1402] *Codul penal al Republicii Franceze*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Franta-RO.html
[1403] *Codul penal al Marelui Ducat de Luxemburg*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Luxemburg-RO.html
[1404] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1405] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[1406] Ibidem.

conformitate cu dreptul intern”[1407], „afectarea gravă, intenţionată şi fără drept a funcţionării unui sistem informatic, prin *introducerea, transmiterea, periclitarea, ştergerea, deteriorarea, alterarea sau suprimarea datelor informatice* (evid. ns.)”.[1408] În Directiva 2013/40/UE, art. 4 „Afectarea ilegală a integrității sistemului” prevede: „Statele membre adoptă măsurile necesare pentru a asigura că perturbarea gravă sau întreruperea funcționării unui sistem informatic”[1409] „prin *introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea, eliminarea datelor informatice sau prin a le face inaccesibile* (evid. ns.)”[1410], „cu intenție și fără drept, este incriminată, cel puțin atunci când nu reprezintă un caz minor”.[1411] Potrivit art. 5 „Afectarea ilegală a integrității datelor” din aceeași directivă, „statele membre adoptă măsurile necesare pentru a asigura că fapta”[1412] „care constă în *ștergerea, periclitarea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau în a le face inaccesibile* (evid. ns.)”[1413], „cu intenție și fără drept, este incriminată, cel puțin atunci când nu reprezintă un caz minor”.[1414]

În Codul penal al Republicii Moldova, prevederilor din cele două acte cu vocație internațională, reproduse mai sus, le corespund prevederile art. 260^2 „Alterarea integrităţii datelor informatice ţinute într-un sistem informatic” și, respectiv, art. 260^3 „Perturbarea funcţionării sistemului informatic”. Astfel, art. 260^2 CP RM prevede: „Modificarea, ştergerea sau deteriorarea intenţionată a datelor informatice ţinute într-un sistem informatic ori restricţionarea ilegală a accesului la aceste date”[1415], „transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, comercializarea sau punerea la dispoziţie, sub orice formă”[1416], „a datelor informatice cu acces limitat, dacă aceste acţiuni au cauzat daune în proporţii mari [...]”.[1417] Alin. (1) art. 260^3 CP RM prevede: „Perturbarea funcţionării unui sistem informatic prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor

[1407] Ibidem.
[1408] Ibidem.
[1409] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en
[1410] Ibidem.
[1411] Ibidem.
[1412] Ibidem.
[1413] Ibidem.
[1414] Ibidem.
[1415] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1416] Ibidem.
[1417] Ibidem.

informatice”[1418] „sau prin restricţionarea accesului la aceste date, dacă aceste acţiuni au cauzat daune în proporţii mari [...]”.[1419]

În context, nu putem ignora părerea lui I. Kuglay: „Infracţiunea prevăzută de art. 360 C.pen. este în principiu o infracţiune-mijloc”[1420]; „scopul accesării unui sistem informatic este, în cele mai multe situaţii, comiterea unei alte infracţiuni”[1421]; „De aceea, în multe situaţii infracţiunea va intra în concurs cu o altă infracţiune dintre cele contra siguranţei şi integrităţii sistemelor şi datelor informatice sau cu una contra patrimoniului”.[1422] Accentuăm că această opinie este valabilă în raport cu art. 360 CPR, în care este incriminat „accesul, fără drept, la un sistem informatic”.[1423] În art. 259 CP RM este incriminat nu pur și simplu accesul ilegal la informaţia computerizată, ci accesul ilegal la informaţia computerizată însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, dacă, în rezultat, s-au produs daune în proporţii mari / deosebit de mari. Nu trebuie să uităm despre această diferență când încercăm că preluăm opinii ale doctrinarilor din România (sau din alte state). Asemenea opinii trebuie analizate atent prin prisma art. 259 CP RM. De aceea, accentuăm: nu este întemeiat să reținem concursul ideal dintre una din infracțiunile, care sunt specificate în art. 259 CP RM, și una din infracțiunile ce sunt prevăzute de art. 260^2 sau 260^2 CP RM. Aceeași distrugere, deteriorare, modificare, blocare sau copiere a informaţiei ori dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice nu trebuie calificată în baza a două articole.

După aceste precizări cu caracter clarificator, ne vom concentra pe analiza modalităților normative ale acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM.

Cât privește modalitatea normativă de *distrugere a informaţiei computerizate*, în doctrina penală sunt prezentate diverse opinii privitoare la conținutul noțiunii corespunzătoare.

De pildă, S. Brînza și V. Stati înțeleg prin „distrugere a informaţiei computerizate” „ștergerea ireversibilă şi completă a informaţiei computerizate”.[1424] După A. Barbăneagră și Gh. Alecu, „prin distrugere se înţelege fapta persoanei orientată spre nimicirea informaţiei, care nu mai

---

[1418] Ibidem.
[1419] Ibidem.
[1420] BODORONCEA, Georgina et al. *Codul penal: comentariu pe articole*. Bucureşti: C.H. Beck, 2014, p. 780. 902 p. ISBN 978-606-18-0408-5.
[1421] Ibidem, p. 780.
[1422] Ibidem, p. 780.
[1423] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[1424] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 354. 1300 p. ISBN 978-9975-53-470-3.

poate fi restabilită”.[1425] Opinii asemănătoare au M. Gheorghiță[1426], V. Soltan[1427], A. Borodac[1428], C. Moțoc, L. Gîrla[1429] și N. Lazareva.[1430]

Din alin. 1 art. 4 al Convenției de la Budapesta ar rezulta că distrugerea datelor informatice nu trebuie echivalată cu ștergerea sau eliminarea acestora: „Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune”[1431], „potrivit dreptului său intern, fapta comisă intenţionat şi fără drept de a distruge, şterge, deteriora, modifica sau elimina date informatice”.[1432] Folosirea distinctă a cuvintelor „distruge”, „șterge” și „elimina” demonstrează că aceste cuvinte au semnificații care diferă.

Nu același lucru rezultă din art. 260^3 CP RM care are menirea să transpună pe plan intern prevederile alin. 1 art. 4 al Convenției de la Budapesta: „Modificarea, ştergerea sau deteriorarea intenţionată a datelor informatice ţinute într-un sistem informatic ori restricţionarea ilegală a accesului la aceste date”[1433], „transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, comercializarea sau punerea la dispoziţie”[1434], „sub orice formă, a datelor informatice cu acces limitat, dacă aceste acţiuni au cauzat daune în proporţii mari [...]”.[1435] Dintr-o asemenea formulare, care cu foarte multă aproximație reproduce prevederile alin. 1 art. 4 al Convenției de la Budapesta, s-ar putea deduce că ştergerea intenţionată a datelor informatice este una dintre manifestările distrugerii informației computerizate.

Acest tablou al ambiguității este completat de explicația din pct. 61 al Raportului explicativ la Convenția de la Budapesta, referitoare la alin. 1 art. 4 al Convenției de la Budapesta: „La alineatul 1, „distrugerea” [...] se referă în special la o modificare negativă a integrității sau a

---

[1425] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0.
[1426] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 570. 836 p. ISBN 9975-61-291-1.
[1427] SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261^1 Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf
[1428] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chișinău: Tipografia Centrală, 2004, p. 365. 622 p. ISBN 9975-9788-7-8.
[1429] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 17. 592 с. ISBN 978-9975-4158-2-8.
[1430] ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista ştiinţifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.
[1431] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[1432] Ibidem.
[1433] Ibidem.
[1434] Ibidem.
[1435] Ibidem.

conținutului informațional al datelor și programelor”[1436]; „„Ștergerea” datelor este echivalentul distrugerii unui lucru corporal. Le distruge și le face de nerecunoscut”[1437]; „Eliminarea datelor computerizate înseamnă orice acțiune care împiedică sau încetează disponibilitatea datelor pentru persoana care are acces la computer sau suportul de date pe care au fost stocate”.[1438]

Toate aceste neclarități contribuie la lipsa de previzibilitate a noțiunii „distrugerea informaţiei computerizate”. Considerăm că această carență a art. 259 CP RM nu-i poate fi imputată făptuitorului. Întrucât (după cum reiese din alin. (2) art. 3 CP RM) legea penală necesită o interpretare restrictivă, suntem de părerea că ștergerea sau eliminarea informaţiei computerizate nu pot să reprezinte exemple care decurg din noțiunea „distrugerea informaţiei computerizate”, folosite în art. 259 CP RM. Această noțiune poate fi reprezentată numai de distrugerea sau deteriorarea calculatorului, a suportului material de informaţie, a sistemului informatic sau a reţelei informatice, care are ca efect distrugerea informației computerizate ce se afla în acel calculator, pe acel suport material de informaţie, în acel sistem informatic sau în acea reţea informatică. În aceste condiții, art. 259 CP RM trebuie aplicat împreună cu art. 197 CP RM sau cu art. 104 din Codul contravențional[1439] (în continuare – CC RM).

Următoarea modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM este *deteriorarea informaţiei computerizate*.

S. Brînza și V. Stati înțeleg prin „deteriorarea informaţiei computerizate” „aducerea informaţiei computerizate într-o stare care o face inutilizabilă temporar sau în parte”.[1440] După părerea lui A. Borodac, „deteriorarea constă în distrugerea parțială a informației, ea neputând fi utilizată conform destinației sale inițiale, dar putând fi restabilită prin intermediul unor programe speciale”.[1441] L. Gîrla și Iu. Tabarcea consideră că „deteriorarea informaţiei computerizate se exprimă în aducerea ei în stare de inutilitate parțială, atunci când o parte a informației este distorsionată sau alterată”.[1442]

Ca și distrugerea informaţiei computerizate, deteriorarea informaţiei computerizate nu poate presupune ștergerea sau eliminarea acestei informații. Argumentele, prezentate mai sus în

---

[1436] *Explanatory Report to the Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/16800cce5b
[1437] Ibidem.
[1438] Ibidem.
[1439] Codul contravențional al Republicii Moldova: nr. 218 din 24.10.2008. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 3-6, 15.
[1440] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 354. 1300 p. ISBN 978-9975-53-470-3.
[1441] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 365. 622 p. ISBN 9975-9788-7-8.
[1442] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 17. 592 с. ISBN 978-9975-4158-2-8.

legătură cu noțiunea „distrugerea informaţiei computerizate” își păstrează valabilitatea în raport cu noțiunea „deteriorarea informaţiei computerizate”. De aceea, noțiunea „deteriorarea informaţiei computerizate” poate fi reprezentată numai de deteriorarea calculatorului, a suportului material de informaţie, a sistemului informatic sau a reţelei informatice, care are ca efect deteriorarea informației computerizate ce se afla în acel calculator, pe acel suport material de informaţie, în acel sistem informatic sau în acea reţea informatică. În asemenea împrejurări, art. 259 CP RM trebuie aplicat împreună cu art. 197 CP RM sau cu art. 104 CC RM.

O altă modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM este *modificarea informaţiei computerizate*.

În viziunea lui S. Brînza și V. Stati, prin „modificarea informaţiei computerizate” trebuie de înțeles „alterarea informaţiei computerizate iniţiale”.[1443] Din punctul de vedere al lui A. Barbăneagră și Gh. Alecu, „modificarea desemnează schimbarea aspectului, formei şi a conţinutului informaţiei, adică făptuitorul introduce sau şterge date informatice din calculator, sistemul sau reţeaua informatică”.[1444] Opinii apropiate exprimă M. Gheorghiță[1445], V. Soltan[1446], A. Borodac[1447], C. Moțoc, L. Gîrla, Iu. Tabarcea[1448] și N. Lazareva.[1449]

În contextul analizei modalității normative de modificare a informației computerizate, prezintă interes exemplul adus de către G. Zlati: „Agentul lansează un atac informatic împotriva sistemelor informatice deținute de un spital în vederea comiterii unui omor”[1450]; „Spre exemplu, agentul accesează fără drept baza de date a spitalului [...] și modifică [...] tratamentul unui pacient cu intenția de a-i provoca decesul [...]”.[1451] Precizăm că, în această ipoteză, concursul dintre infracțiunile prevăzute la art. 145 (cu sau fără a se face referire la art. 27 CP RM) și 259

[1443] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 354. 1300 p. ISBN 978-9975-53-470-3.

[1444] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0.

[1445] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chișinău: Arc, 2003, p. 570. 836 p. ISBN 9975-61-291-1.

[1446] SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261[1] Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf

[1447] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chișinău: Tipografia Centrală, 2004, p. 365-366. 622 p. ISBN 9975-9788-7-8.

[1448] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 17-18. 592 с. ISBN 978-9975-4158-2-8; MOȚOC, Costică, GÎRLA, Lilia. Protecția juridico-penală a secretului profesional prin prisma incriminărilor prevăzute la art. 178, 259, 260[1], 260[2] CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale”*, 2020, nr. 3, pp. 139-151. ISSN 1814-3199.

[1449] ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista științifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.

[1450] ZLATI, George. Legitima apărare și starea de necesitate în domeniul criminalității informatice (I). În: *Dreptul*, 2015, nr. 4, pp. 145-172. ISSN 1811-0770.

[1451] Ibidem.

CP RM este posibil numai dacă accesul ilegal la baza de date a spitalului, însoțit de modificarea acestor date, produce daune în proporții mari sau deosebit de mari. În lipsa unor asemenea daune, se va aplica doar art. 145 CP RM (cu sau fără a se face referire la art. 27 CP RM).

Următoarea modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM este *blocarea informaţiei computerizate*.

S. Brînza și V. Stati sunt de părerea că, în această situație, vorbim despre „crearea de inaccesibilitate a informaţiei computerizate, deşi informaţia dată se păstrează”.[1452] A. Barbăneagră și Gh. Alecu afirmă că „blocarea se realizează prin împiedicarea recepţionării sau transmiterii informaţiei computerizate”.[1453] În termeni similari își formulează opinia M. Gheorghiță[1454], V. Soltan[1455], A. Borodac[1456], C. Moțoc, L. Gîrla, Iu. Tabarcea[1457] și N. Lazareva.[1458]

În context, este interesant să analizăm anumite spețe din practica judiciară, pentru a stabili dacă trebuia aplicat art. 259 CP RM.

Spre exemplu, într-o speță, J.A. a fost condamnat în conformitate cu alin. (1) art. 177, alin. (1) art. 178 și art. 260^5 CP RM. La 26.07.2015, în intervalul de timp 15.42 - 18.53, de la domiciliul său, acesta a accesat ilegal şi fără consimţământul lui P.P. două conturi de poștă electronică ale acestuia, care conţineau informaţii ce constituiau secretul personal al lui P.P. După aceasta, J.A. a modificat parola de acces la conturile respective, astfel restricționând accesul lui P.P. la acestea, precum şi a modificat datele informatice păstrate de către ultimul, rezultând date necorespunzătoare adevărului Aceste acţiuni au fost comise în scopul de a-l avantaja pe J.A. în litigiul civil dintre acesta și P.P.[1459] În acest caz, lipsește temeiul aplicării alin. (1) art. 178 CP RM. J.A. nu a violat „dreptul la secretul scrisorilor, telegramelor, coletelor şi

---

[1452] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 354. 1300 p. ISBN 978-9975-53-470-3.

[1453] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0.

[1454] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 570. 836 p. ISBN 9975-61-291-1.

[1455] SOLTAN, Veaceslav. Infracțiunile informatice (art. $259\text{-}261^1$ Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf

[1456] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 365. 622 p. ISBN 9975-9788-7-8.

[1457] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 17. 592 с. ISBN 978-9975-4158-2-8; MOȚOC, Costică, GÎRLA, Lilia. Protecția juridico-penală a secretului profesional prin prisma incriminărilor prevăzute la art. 178, 259, 260^1, 260^2 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale”*, 2020, nr. 3, pp. 139-151. ISSN 1814-3199.

[1458] ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista științifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.

[1459] *Decizia Colegiului penal lărgit al CSJ din 11.06.2019. Dosarul nr. 1ra-445/2019*. [citat 11.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=13789

altor trimiteri poştale, al convorbirilor telefonice şi înştiinţărilor telegrafice, cu încălcarea legislaţiei."[1460] Aplicarea față de J.A. a alin. (1) art. 178 CP RM constituie un exemplu de aplicare a legii penale prin analogie. Violarea dreptului la secretul poștei electronice nu este incriminată în art. 178 CP RM. Invocarea acestui articol pentru violarea dreptului la secretul poștei electronice reprezintă aplicarea art. 178 CP RM dincolo de limitele stabilite de către legiuitor, ceea ce, în mod evident, este ilegal. Accesarea ilegală a conturilor de poștă electronică ale victimei corespunde noțiunii de acces ilegal la informația computerizată, folosite în art. 259 CP RM. Însă, lipsesc celelalte condiții – prezența acțiunii adiacente și a urmărilor prejudiciabile – care ar permite aplicarea art. 259 CP RM. Or, „modificarea ilegală a datelor informatice, precum și restricţionarea ilegală a accesului la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice"[1461], au fost săvârșite în contextul infracțiunii de fals informatic (art. 260^5 CP RM). În concluzie, lui J.A. urma să-i fie aplicată răspunderea doar în baza alin. (1) art. 177 și art. 260^5 CP RM. Modificarea și blocarea informaţiei computerizate, care aparținea victimei, nu a fost săvârșită în contextul uneia dintre infracțiunile prevăzute la art. 259 CP RM.

În altă speță, Ţ.A. a fost condamnată în baza art. 260^5 CP RM. La 16.12.2011, în temeiul încheierii executorului judecătoresc, lui A.I. i-a fost transmis în proprietate privată un bun imobil amplasat în or. Ialoveni. La 03.01.2012, Ţ.A., specialist în evidenţa documentelor al unui Oficiu Cadastral Teritorial, nefiind autorizată să acceseze datele din Registrul Bunurilor Imobile, a accesat ilegal aceste date și a introdus date informatice cu privire la punerea interdicţiei pe imobilul transmis în proprietatea lui A.I. După aceasta, Ţ.A. a restricţionat ilegal accesul la aceste date, în scopul de a limita dreptul de dispoziţie a proprietarului A.I. asupra bunului imobil menţionat. Această interdicţie s-a menţinut până la 13.01.2012.[1462] În acest caz, „introducerea ilegală a datelor informatice, precum și restricţionarea ilegală a accesului la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice"[1463], au fost comise în contextul infracțiunii de fals informatic (art. 260^5 CP RM). Deci, aplicarea acestui articol este întemeiată. Modificarea și blocarea informaţiei computerizate din Registrul Bunurilor Imobile nu a fost săvârșită în contextul uneia dintre infracțiunile prevăzute la art. 259 CP RM. Atestăm accesarea ilegală a informației computerizate,

[1460] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1461] Ibidem.
[1462] *Decizia Colegiului penal al CSJ din 25.06.2014. Dosarul nr. 1ra-1113/2014*. [citat 11.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=2653
[1463] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

și anume – a datelor din Registrul Bunurilor Imobile. Însă, în lipsa acțiunii adiacente și a urmărilor prejudiciabile, această accesare ilegală a informației computerizate nu este suficientă pentru aplicarea art. 259 CP RM. Întrucât Ț.A., ca persoană publică, a săvârşit o acţiune care ţinea de competenţa unei alte persoane publice (și anume – a accesat datele din Registrul Bunurilor Imobile, nefiind autorizată pentru aceasta), urma să-i fie aplicat suplimentar art. 313 CC RM, care prevede răspunderea pentru excesul de putere sau depăşirea atribuţiilor de serviciu (adică pentru „săvârşirea unei acţiuni care depăşeşte în mod vădit limitele drepturilor şi atribuţiilor acordate prin lege”[1464] „și care contravine intereselor publice sau drepturilor şi intereselor ocrotite de lege ale persoanelor fizice sau juridice, dacă fapta nu întruneşte elementele constitutive ale infracţiunii”[1465]).

În altă speță, G.A. și G.T. au fost condamnați în baza alin. (1) art. 260^6 și lit. b), d) alin. (2) art. 261^1 CP RM. În perioada 06.03.2018 - 14.03.2018, în scopul prestării serviciilor de „Call Centru”, cei doi făptuitori au fondat întreprinderea „G.A.L.” S.R.L., al cărei administrator era G.T.[1466]; utilizând fraudulos un număr din numerotația de telefonie fixă, atribuită de către compania „Moldtelecom” S.A., G.A. și G.T. au închiriat o cameră într-un imobil[1467], unde au instalat un sistem informatic, interconectat cu alte două sisteme informatice[1468]; în aceste împrejurări, făptuitorii au accesat neautorizat rețelele şi serviciile de telecomunicații ale companiei „Moldtelecom” S.A., au restricționat accesul la datele informatice[1469] şi au efectuat terminații neautorizate ale traficului voce, generând ilegal 40687,9 minute, cauzând astfel companiei „Moldtelecom” S.A. daune în mărime de 183.790,25 lei.[1470] În acest caz, restricționarea accesului la datele informatice a fost săvârșită în contextul infracțiunii prevăzute la alin. (1) art. 260^6 CP RM. Or, restricţionarea accesului la astfel de date a fost comisă pentru a se obţine un beneficiu material, fiind cauzate daune în proporţii mari. Restricționarea accesului la datele informatice a fost precedată nu de accesul ilegal la informația computerizată în accepția art. 259 CP RM, ci de accesul neautorizat la reţelele şi serviciile de telecomunicaţii. Pune în gardă că daunele în proporții mari au fost reținute la calificare de două ori, deși au fost cauzate o singură dată. Considerăm că daunele în proporții mari au fost cauzate în contextul fraudei informatice (alin. (1) art. 260^6 CP RM), nu al accesului neautorizat la reţelele şi serviciile de

[1464] Codul contravențional al Republicii Moldova: nr. 218 din 24.10.2008. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 3-6, 15.
[1465] Ibidem.
[1466] *Decizia Colegiului penal al CSJ din 05.08.2020. Dosarul nr. 1ra-1508/2020*. [citat 11.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=16547
[1467] Ibidem.
[1468] Ibidem.
[1469] Ibidem.
[1470] Ibidem.

telecomunicaţii (lit. b) și d) alin. (2) art. 261^1 CP RM). Accesul neautorizat la reţelele şi serviciile de telecomunicaţii a constituit nu un scop în sine, ci etapa de pregătire de infracțiunea prevăzută la alin. (1) art. 260^6 CP RM. În concluzie, G.A. și G.T. ar fi urmat să răspundă doar în conformitate cu alin. (1) art. 260^6 CP RM.

După examinarea acestor exemple din practica judiciară, revenim la analiza modalităților normative ale acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM. Următoarea modalitate de acest gen este *copierea informaţiei computerizate*.

S. Brînza și V. Stati afirmă că, prin „copierea informaţiei computerizate" se înțelege „reproducerea informaţiei computerizate originale, deşi această informaţie se păstrează intactă şi în stare de utilizare".[1471] După A. Barbăneagră și Gh. Alecu, „acţiunea de copiere presupune transferul ilegal al informaţiei computerizate de pe un suport material pe altul".[1472] Puncte de vedere asemănătoare sunt exprimate de către M. Gheorghiță[1473], V. Soltan[1474], A. Borodac[1475], C. Moțoc, L. Gîrla, Iu. Tabarcea[1476] și N. Lazareva.[1477]

În art. 259 CP RM se are în vedere copierea logică a informației computerizate (care presupune folosirea unui program de calculator), nu copierea fizică a acesteia (de exemplu: reproducerea manuală; reproducerea prin fotografierea textului sau a imaginii de pe ecranul calculatorului etc.). În caz contrar, își pierde sensul noțiunea de informație computerizată, care presupune circulația într-un mediu informatic.

Cu atât mai puțin, reproducerea în creierul uman prin memorare a unei informații văzute, auzite sau altfel percepute nu formează conținutul noțiunii „copierea informației computerizate", folosite în art. 259 CP RM. O astfel de reproducere este inerentă din momentul accesării oricărei informații computerizate și nu poate fi privită în contextul acțiunii adiacente prevăzute la art. 259 CP RM.

[1471] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 354. 1300 p. ISBN 978-9975-53-470-3.

[1472] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0.

[1473] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 570. 836 p. ISBN 9975-61-291-1.

[1474] SOLTAN, Veaceslav. Infracțiunile informatice (art. $259\text{-}261^1$ Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf

[1475] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 365. 622 p. ISBN 9975-9788-7-8.

[1476] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 18. 592 с. ISBN 978-9975-4158-2-8; MOȚOC, Costică, GÎRLA, Lilia. Protecția juridico-penală a secretului profesional prin prisma incriminărilor prevăzute la art. 178, 259, 260^1, 260^2 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale"*, 2020, nr. 3, pp. 139-151. ISSN 1814-3199.

[1477] ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista ştiinţifică a USM „Studia Universitatis". Seria „Ştiinţe sociale"*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.

Suntem de acord cu G.S.O. Kurbanov, în opinia căruia copierea informației computerizate trebuie deosebită de multiplicarea acesteia: „În acest ultim caz, informația este reprodusă nu pe un suport de informație diferit de cel original”[1478] „ci pe suportul de informație original (de exemplu, mai multe fișiere cu același conținut sunt stocate în memoria calculatorului)”.[1479] Așadar, condiția esențială pentru atestarea copierii informației computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, este ca informația computerizată copiată să fie stocată într-un alt calculator, pe un alt suport material de informaţie, într-un alt sistem informatic sau într-o altă reţea informatică, decât cel/cea pe care se păstra informația computerizată originală.

Este posibil ca: 1) la același calculator, la același suport material de informaţie, la același sistem informatic sau la aceeași reţea informatică să aibă acces două sau mai multe persoane; 2) totodată, să fie restricționat accesul pentru una sau unele dintre aceste persoane la o parte a unui astfel de calculator, suport material de informaţie sau sistem informatic ori a unei astfel de reţele informatice. Într-o asemenea situație, pentru a aplica art. 259 CP RM, informația computerizată copiată trebuie să fie stocată în acea parte din calculator, din suportul material de informaţie, din sistemul informatic sau din reţeaua informatică, la care nu are acces victima.

În contextul examinării modalității de copiere a informației computerizate, menționăm o opinie exprimată de S. Brînza și V. Stati. Conform acesteia, pornografia neconsimțită în varianta „revenge porn” poate fi calificată în baza art. 177 și 259 CP RM, „dacă imaginile sau alte reprezentări pornografice sunt obținute în rezultatul accesului ilegal la informaţia computerizată”.[1480] În această ipoteză, aplicarea art. 259 CP RM este posibilă numai dacă se produc daune în proporții mari sau deosebit de mari. În afară de aceasta, pentru ca art. 259 CP RM să poată fi aplicat, accesul ilegal la imaginile sau la alte reprezentări pornografice în formă computerizată trebuie să fie însoțit, de exemplu, de copierea acestor informaţii. Dacă însă accesul ilegal la imaginile sau la alte reprezentări pornografice în formă computerizată este însoțit de diseminarea acestor informații, fără ca ele să fie copiate, atunci lipsește temeiul aplicării art. 259 CP RM.

În opinia lui M.Iu. Dvorețki, „copierea ilegală a informației computerizate poate constitui pregătirea sau tentativa de a comite o altă infracțiune (de exemplu, încălcarea dreptului de

---

[1478] КУРБАНОВ, Г.С.О. Объективная сторона преступления, связанного с неправомерным доступом к компьютерной информации. În: *Правовая информатика*, 2013, nr. 4, c. 17-20. ISSN 1994-1404.
[1479] Ibidem.
[1480] BRÎNZA, Serghei, STATI, Vitalie. „Sexting”, „sextorsion”, „revenge porn”: fenomene reflectate în Codul penal al Republicii Moldova? În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 3, pp. 3-17. ISSN 1814-3199.

autor)”.[1481] Considerăm că această poziție necesită o precizare. Copierea informației computerizate, dacă nu produce daune în proporții mari sau deosebit de mari și dacă nu este precedată de accesul ilegal la acea informație, poate să reprezinte pregătirea de infracțiunile care presupun divulgarea anumitor informații (de exemplu, pregătirea de infracțiunile prevăzute la art. 204, alin. (1) art. 315, art. 316, 337, 344 etc. din Codul penal). În astfel de situații, nu este necesară aplicarea art. 259 CP RM, întrucât copierea informației computerizate nu reprezintă un scop în sine și întrucât nu sunt întrunite toate condițiile care ar permite aplicarea art. 259 CP RM.

În alt context, dar cu referire la aceeași modalitate normativă de copiere a informației computerizate, trebuie de menționat că alin. (2) art. 360 CPR prevede răspunderea pentru „accesul fără drept la un sistem informatic, săvârșit în scopul obținerii de date informatice”.[1482] În legătură cu această circumstanță agravantă, I. Kuglay menționează: „„Obţinerea” de date informatice are semnificaţia preluării, a transferului lor, nu se limitează la simpla „vizualizare” a informaţiei”.[1483] Același autor afirmă: „În forma agravată prin scop, dacă transferul de date are loc, această operaţiune este exterioară infracţiunii prevăzute de art. 360 alin. (2) C.pen.”[1484] „şi va constitui infracţiunea distinctă, de transfer neautorizat de date informatice prevăzută de art. 364 C.pen.”[1485]

Din această opinie rezultă că noțiunea „obținerea de date informatice” din art. 360 CPR are același înțeles ca noțiunea „copierea informației computerizate” din art. 259 CP RM. Totuși, copierea informației computerizate reprezintă nu scopul cu efect agravant al uneia dintre infracțiunile ce sunt specificate în art. 259 CP RM. Așa cum deja am specificat, copierea informației computerizate constituie modalitatea normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM. Accesul ilegal la informația computerizată, urmat de copierea acestei informații, dacă produce daune în proporții mari sau deosebit de mari, atrage aplicarea exclusiv a art. 259 CP RM. Nu va fi necesară invocarea suplimentară a unei alte norme.

În același timp, la lit. f) alin. (2) art. 259 CP RM, este specificată circumstanța agravantă „cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice, în scopul săvârşirii uneia dintre infracţiunile prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6”.[1486] Astfel că există

[1481] ДВОРЕЦКИЙ, М.Ю. Проблемы толкования терминов при квалификации преступлений по ст. 272 Уголовного кодекса РФ. În: *Вестник Тамбовского университета. Серия: Гуманитарные науки*, 2013, № 12, с. 527-532. ISSN 1810-0201.
[1482] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[1483] BODORONCEA, Georgina et al. *Codul penal: comentariu pe articole*. Bucureşti: C.H. Beck, 2014, p. 779. 902 p. ISBN 978-606-18-0408-5.
[1484] Ibidem, p. 780.
[1485] Ibidem, p. 780.
[1486] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

posibilitatea ca – după săvârșirea accesului ilegal la informația computerizată, urmat de copierea acestei informații, dacă se produc daune în proporții mari – să fie comis transferul neautorizat de date informatice dintr-un sistem informatic, care, la rândul său, produce daune în proporţii mari. În acest caz, vom fi în prezența concursului real de infracțiuni prevăzute la lit. f) alin. (2) art. 259 și art. 260^2 CP RM. În mod firesc, informația computerizată, copiată în contextul infracțiunii prevăzute la lit. f) alin. (2) art. 259 CP RM, trebuie să fie alta decât datele informatice transferate neautorizat în contextul infracțiunii prevăzute la art. 260^2 CP RM. Doar în acest fel daunele în proporţii mari, produse în contextul infracțiunii prevăzute la lit. f) alin. (2) art. 259 CP RM, nu vor coincide cu daunele în proporţii mari, produse în contextul infracțiunii care este prevăzută de art. 260^2 CP RM.

Ultima modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM este *dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice*.

După părerea lui S. Brînza și V. Stati, această modalitate presupune „disfuncţionalizarea calculatoarelor, a sistemului sau a reţelei informatice, având ca efect oferirea unei informaţii incorecte, refuzul oferirii informaţiei, scoaterea din funcţiune sau întreruperea funcţionării, etc.”[1487] A. Barbăneagră și Gh. Alecu consideră că „prin dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice se înţeleg acţiunile de defectare a tehnicii menţionate”[1488]; „Drept consecinţe ale dereglării pot fi: deconectarea tehnicii, recepţionarea informaţiei denaturate etc.”[1489] Păreri similare au M. Gheorghiță[1490], V. Soltan[1491], A. Borodac[1492], L. Gîrla, Iu. Tabarcea[1493] și N. Lazareva.[1494]

Nu intră sub incidența art. 259 CP RM „împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul”[1495], „dacă

[1487] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 354. 1300 p. ISBN 978-9975-53-470-3.
[1488] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0.
[1489] Ibidem, p. 568.
[1490] Ibidem, p. 570.
[1491] SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261^1 Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf
[1492] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 365. 622 p. ISBN 9975-9788-7-8.
[1493] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 18. 592 с. ISBN 978-9975-4158-2-8.
[1494] ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista ştiinţifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.
[1495] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

aceste acţiuni au cauzat daune în proporţii mari sau deosebit de mari."[1496] În acest caz se aplică răspunderea pentru frauda informatică (art. 260^6 CP RM). În contextul evocat vom prezenta o speță: C.O. a fost condamnat în baza alin. (5) art. 42 și alin. (1) art. 260^6 CP RM. În perioada 01.01.2017 - 21.02.2017, C.O. a contribuit în calitate de complice la acordarea de mijloace şi de instrumente autorilor infracţiunii şi anume – lui P.V., D.I. şi I.I. Persoanele în cauză au deschis mai multe conturi de card de plată pe numele lor, la unele bănci din Republica Moldova. Ulterior, P.V., D.I. şi I.I. i-au transmis lui C.O. respectivele carduri. În perioada 17.01.2017 - 21.02.2017, persoane neidentificate, prin intermediul cardurilor bancare menţionate, care le-au fost transmise de către C.O., au efectuat mai multe tranzacţii de retragere frauduloasă a numerarului prin metoda „Transaction Reversal Fraud" de la bancomatele din Marea Britanie, restricţionând accesul la datele informatice şi împiedicând funcţionarea sistemelor informatice ale bancomatelor. În rezultat, au fost cauzate daune în proporţii mari.[1497] Observăm că, în acest caz, împiedicarea funcţionării unor sisteme informatice (și anume – a unor bancomate din Marea Britanie) este precedată de accesarea ilegală a acestor sisteme informatice. Mai mult, această împiedicare a funcţionării unor sisteme informatice a cauzat daune în proporţii mari. Cu toate acestea, lipsește temeiul aplicării art. 259 CP RM. Prezența scopului special (și anume – a scopului de a obţine un beneficiu material) face ca art. 260^6 CP RM să fie privit în atare condiții ca normă specială față de art. 259 CP RM. În virtutea regulii stabilite la art. 116 CP RM, într-o astfel de situație, aplicarea art. 260^6 CP RM exclude aplicarea art. 259 CP RM.

2.2.2. Momentul de consumare și urmările prejudiciabile în cazul infracțiunilor prevăzute la art. 259 CP RM

M.-K. Guiu afirmă: „În concepția naturalistică, noțiunea de rezultat al infracțiunii este înțeleasă ca o modificare cauzată de făptuitor în realitatea naturală, sensibilă"[1498]; „Deși, în privința configurației acestei modificări, părerile sunt împărțite: într-o opinie (susținută, la noi, de majoritatea penaliștilor mai vechi)"[1499], „se consideră că această modificare se poate înfățișa atât într-o formă materială, cât și sub forma unei stări noi – ceea ce înseamnă, în fond, că toate

[1496] Ibidem.
[1497] *Decizia Colegiului penal al CSJ din 07.11.2018. Dosarul nr. 1ra-1891/2018*. [citat 11.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=12288
[1498] GUIU, Mioara-Ketty. Clasificarea infracțiunilor în raport cu rezultatul lor. În: *Dreptul*, 2017, nr. 12, pp. 137-149. ISSN 1811-0770.
[1499] Ibidem.

infracțiunile au un rezultat, material sau nematerial”[1500]; „într-o altă opinie (Francesco Antolisei, Giuseppe Bettiol ș.a.), se consideră că această modificare se poate înfățișa numai într-o formă materială (substanțială)”[1501] – „ceea ce înseamnă că numai infracțiunile de rezultat (materiale) pot avea un rezultat, iar nu și cele formale, care sunt lipsite de rezultat. [...]”[1502]; „Ținând seama că nu se poate concepe o infracțiune lipsită de obiect juridic, de scopul de protecție a unei valori sociale, adepții concepției juridice au conchis că orice infracțiune are, în mod necesar, un rezultat juridic”[1503], „ce se poate înfățișa sub două forme: fie sub forma unei leziuni (vătămări), fie sub forma punerii în pericol a valorii sociale protejate”.[1504]

Considerăm că M.-K. Guiu confundă atingerea, care i se aduce obiectului juridic al infracțiunii, cu urmarea prejudiciabilă din cadrul unei infracțiuni. Dacă toate infracțiunile ar avea urmări prejudiciabile, iar rezultatul infracțional ar consta inclusiv în periclitarea valorii sociale protejate, atunci cum infracțiunea consumată ar putea fi deosebită de tentativa de infracțiune? Or, infracțiunea consumată presupune atingerea efectivă ce i se aduce obiectului juridic al infracțiunii, în timp ce tentativa de infracțiune presupune atingerea potențială adusă obiectului juridic al infracțiunii, adică periclitarea acestuia.

În opinia noastră, nu toate infracțiunile au urmări prejudiciabile. Doar infracțiunile materiale le pot avea. În acest sens, suntem de acord cu S. Copețchi și I. Hadîrcă care menționează: „Divizarea componențelor de infracțiune în materiale (cu urmări prejudiciabile) și formale (fără urmări prejudiciabile) decurge din confruntarea componenței de infracțiune cu dispoziția normei juridico-penale”[1505]; „La o analiză atentă a normelor din partea specială a Codului penal conchidem că nu toate normele incriminatoare conțin prevederi ce indică asupra urmărilor prejudiciabile”.[1506] Puncte de vedere asemănătoare exprimă S. Botnaru[1507], V. Bujor[1508] și C. Gurschi.[1509]

O astfel de concepție se promovează nu numai în doctrina penală, ci și în jurisprudența Curții Constituționale a Republicii Moldova. De exemplu, în pct. 68 din Hotărârea nr. 22 din

---

[1500] Ibidem.
[1501] Ibidem.
[1502] Ibidem.
[1503] Ibidem.
[1504] Ibidem.
[1505] COPEȚCHI, Stanislav, HADÎRCĂ, Igor. *Calificarea infracțiunilor: Note de curs*. Chișinău: Tipografia Centrală, 2015, p. 133. 352 p. ISBN 978-9975-53-547-2.
[1506] Ibidem, p. 133-134.
[1507] BOTNARU, Stela, ȘAVGA, Alina, GRAMA, Mariana, GROSU, Vladimir. *Drept penal. Partea generală*. Chișinău: Cartier, 2005, p. 143, 145. 624 p. ISBN 9975-79-318-5.
[1508] BUJOR, Valeriu. Unele aspecte vizând elaborarea normelor de drept penal. În: *Legea și Viața*, 2009, nr. 8, pp. 8-10. ISSN 1810-309X.
[1509] BARBĂNEAGRĂ, Alexei et al. *Codul penal comentat şi adnotat*. Chişinău: Cartier, 2005, p. 48. 656 p. ISBN 9975-29-338-X.

27.06.2017 privind excepţia de neconstituţionalitate a unor prevederi ale articolului 28 alin. (1) din Codul penal, Curtea Constituțională a Republicii Moldova statuează: „Excesul de putere sau depăşirea atribuţiilor de serviciu *este o infracţiune de rezultat (materială), astfel încât consumarea ei este legată”*[1510], *„în mod obligatoriu, de producerea unor consecințe prejudiciabile* (evid. ns.), şi anume: „cauzarea daunelor în proporţii considerabile intereselor publice”[1511] „sau drepturilor şi intereselor ocrotite de lege ale persoanelor fizice sau juridice”.”[1512] O constatare similară se face în pct. 72 din Hotărârea nr. 33 din 07.12.2017 privind excepţia de neconstituţionalitate a unor prevederi din articolele 327 alin. (1) și 361 alin. (2) lit. d) din Codul penal.[1513]

După această notă introductivă, este necesar să stabilim dacă infracțiunile, prevăzute la art. 259 CP RM, sunt formale sau materiale.

În raport cu versiunea în vigoare a art. 259 CP RM, S. Brînza și V. Stati expun următoarea opinie: „Infracţiunea specificată la alin. (1) art. 259 CP RM este o infracţiune materială. Ea se consideră consumată din momentul producerii daunelor în proporţii mari”[1514]; „Mărimea daunelor cauzate prin infracțiunea prevăzută la la alin. (1) art. 259 CP RM nu poate să depăşească”[1515] „[20 de salarii medii lunare pe economie prognozate, stabilite prin hotărârea de Guvern în vigoare la momentul săvârșirii faptei]”[1516]; „Altfel, răspunderea se va aplica în conformitate cu lit. h) alin. (2) art. 259 CP RM”.[1517] O părere similară o exprimă L. Dumneanu și D. Gurev.[1518]

Trebuie de precizat că, până a intra în vigoare la 20.02.2009 Legea nr. 278 din 18.12.2008 pentru modificarea şi completarea Codului penal al Republicii Moldova[1519] (în continuare – Legea nr. 278/2009), alin. (1) art. 259 CP RM avea următoarea dispoziție: „Accesul ilegal la informaţia computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de

---

[1510] Hotărârea Curții Constituționale a Republicii Moldova privind excepţia de neconstituţionalitate a unor prevederi ale articolului 328 alin. (1) din Codul penal: nr. 22 din 27.06.2017. În: *Monitorul Oficial al Republicii Moldova*, 2017, nr. 352-355, 92.
[1511] Ibidem.
[1512] Ibidem.
[1513] Ibidem.
[1514] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 355. 1300 p. ISBN 978-9975-53-470-3.
[1515] Ibidem, p. 355.
[1516] Ibidem, p. 355.
[1517] Ibidem, p. 355.
[1518] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM, p. 97-98. 261 p. ISBN 978-9975-158-29-9.
[1519] Legea 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, 98.

informaţie”[1520], „din sistemul sau reţeaua informatică, dacă acest acces este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei”[1521], „de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”.[1522] Daunele în proporții mari și daunele în proporții deosebit de mari nu erau menționate în acest articol nici măcar în alineatul (2).

La varianta inițială a art. 259 CP RM (și anume – cea dinaintea intrării în vigoare a Legii nr. 278/2008), se referă următoarea părere a lui L. Gîrla și Iu. Tabarcea: „Componența infracțiunii, prevăzute la art. 259 CP RM, este materială”[1523]; „Ea trebuie considerată consumată din momentul în care survin urmările sub forma distrugerii, deteriorării, modificării, blocării sau copierii informaţiei”[1524], „ori a dereglării funcţionării calculatoarelor, a sistemului sau a reţelei informatice”.[1525] În raport cu aceeași variantă a art. 259 CP RM, M. Gheorghiță a avut un punct de vedere apropiat.[1526] De asemenea, în raport cu varianta art. 259 CP RM de până la intrarea în vigoare a Legii nr. 278/2008, A. Borodac a folosit sintagma „componență de infracțiune materială”[1527] în raport cu infracțiunile prevăzute la art. 259 CP RM, menționând: „Infracțiunea se consideră consumată dacă accesul ilegal la informația computerizată este însoțit de distrugerea”[1528], „deteriorarea, modificarea, blocarea, copierea informației sau de dereglarea funcționării calculatoarelor, a sistemului sau a rețelei informatice”.[1529]

În raport cu varianta inițială a art. 259 CP RM (și anume – cea de până la intrarea în vigoare a Legii nr. 278/2008), alți doctrinari au avut o opinie diferită. De exemplu, N. Lazareva a menționat: „Componența infracțiunii, descrisă în art. 259 CP RM este formulată ca fiind formală, iar infracțiunea se consideră consumată din momentul săvârșirii cel puțin a uneia dintre acțiunile menționate în dispoziția art. 259 CP RM”.[1530] Pe poziții similare s-au situat A. Barbăneagră și

---

[1520] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1521] Ibidem.
[1522] Ibidem.
[1523] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 19. 592 с. ISBN 978-9975-4158-2-8.
[1524] Ibidem, с. 19.
[1525] Ibidem, с. 19.
[1526] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 569. 836 p. ISBN 9975-61-291-1.
[1527] BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 364. 622 p. ISBN 9975-9788-7-8.
[1528] Ibidem, p. 364.
[1529] Ibidem, p. 364.
[1530] ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista științifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.

Gh. Alecu.[1531] Astfel de opinii sugerează că latura obiectivă a infracțiunilor, prevăzute la art. 259 CP RM (în varianta dinaintea intrării în vigoare a Legii nr. 278/2008), includea un singur semn constitutiv, și anume – fapta prejudiciabilă.

Avem rezerve față de punctele de vedere de acest gen. Ele s-ar potrivi pentru a caracteriza nu infracțiunile prevăzute la art. 259 CP RM (în varianta dinaintea intrării în vigoare a Legii nr. 278/2008), ci infracțiunea prevăzută la art. 176^1 CP RM din 1961. Amintim că alineatul 1 al acestui articol prevedea răspunderea pentru „accesul ilegal (nesancţionat) la informaţia ce se păstrează în sistemul computerizat, cu încălcarea sistemului de protecţie”.[1532] În alin. 2 art. 176^1 CP RM din 1961 era descrisă varianta agravată a infracțiunii respective: „Aceeaşi acţiune săvârşită din imprudenţă, care a cauzat nimicirea sau blocarea informaţiei, precum şi scoaterea din funcţiune a utilajului computerizat ori alte urmări grave”.[1533]

Considerăm că formularea „distrugerea, deteriorarea modificarea [...] informaţiei, [...] dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”[1534] (care este folosită în dispoziția de la alin. (1) art. 259 CP RM din momentul adoptării Codului penal în vigoare și care nu a fost afectată de adoptarea Legii nr. 278/2008) are un caracter eliptic. La o ipoteză similară se referă S. Brînza: „La alin. (1) art. 145 CP RM nu sunt descrise semnele concrete ale laturii obiective a infracţiunii examinate, legiuitorul preferând o formulare eliptică „omorul unei persoane””[1535]; „În această exprimare, legiuitorul nu a considerat necesară o descriere mai amplă, deoarece s-a folosit de însuşirea obiectivă a substantivului („omorul”), provenit dintr-un verb, de a concentra în el descrierea”[1536]: „1) faptei prejudiciabile constând în acţiunea sau inacţiunea de lipsire ilegală de viaţă a unei alte persoane; 2) urmărilor prejudiciabile, şi anume moartea cerebrală a victimei”[1537]; „3) legăturii de cauzalitate dintre fapta prejudiciabilă şi urmările prejudiciabile”.[1538] Extrapolând ideea de descriere eliptică a unei infracțiuni în textul legii penale, M.-K. Guiu menționează: „Așa-numitele „infracțiuni cu rezultat comprimat” (omorul, uciderea din culpă etc.), în care *verbum regens* descrie atât acțiunea, cât și

---

[1531] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chișinău: Sarmis, 2009, p. 567, 568. 860 p. ISBN 978-9975-105-20-0.
[1532] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
[1533] Ibidem.
[1534] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1535] BRÎNZA, Serghei. Infracțiunea de omor simplu în legea penală a Republicii Moldova. În: *Jurnalul de Studii Juridice*, 2010, număr special, pp. 15-29. ISSN 1841-6195.
[1536] Ibidem.
[1537] Ibidem.
[1538] Ibidem.

rezultatul ei material”[1539] „(moartea, *distrugerea* (evid. ns.)), infracțiunile de vătămare corporală, precum și eventualele infracțiuni complexe care absorb un asemenea rezultat”.[1540] O părere apropiată are I. Soroceanu.[1541]

În legătură cu varianta în vigoare a art. 259 CP RM, S. Brînza și V. Stati vorbesc despre următoarea structură a laturii obiective: „1) fapta prejudiciabilă care constă în acţiunea principală de acces ilegal la informaţia computerizată, însoţită de acţiunea adiacentă de distrugere, deteriorare, modificare”[1542], „blocare sau copiere a informaţiei, de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice”[1543]; „2) urmările prejudiciabile, și anume – daunele în proporţii mari; 3) legătura cauzală dintre fapta prejudiciabilă şi urmările prejudiciabile”.[1544] Păreri asemănătoare au L. Gîrla și Iu. Tabarcea[1545], L. Dumneanu și D. Gurev.[1546]

În ce ne privește, considerăm că înfățișarea urmărilor prejudiciabile ale infracțiunilor ce sunt specificate în art. 259 CP RM trebuie să ia în calcul caracterul eliptic al formulării „distrugerea, deteriorarea, modificarea [...] informaţiei, [...] dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”.[1547] Ca model apropiat poate fi prezentată structura laturii obiective a infracțiunii prevăzute la art. 197 CP RM, propusă în 2005 de către S. Brînza: „1) fapta prejudiciabilă care constă în *acţiunea sau inacţiunea de cauzare a distrugerii ori deteriorării* (evid. ns.)”[1548]; 2) *urmările prejudiciabile sub forma distrugerii sau deteriorării în proporţii mari* (evid. ns.); 3) legătura de cauzalitate dintre fapta prejudiciabilă și urmările prejudiciabile”.[1549] Ulterior, S. Brînza a renunțat la această manieră de prezentare a structurii laturii obiective a infracțiunii prevăzute la art. 197 CP RM: „Latura obiectivă a infracțiunii prevăzute la alin. (1) art. 197 CP RM are următoarea structură: 1) fapta prejudiciabilă care constă

[1539] GUIU, Mioara-Ketty. Clasificarea infracțiunilor în raport cu rezultatul lor. În: *Dreptul*, 2017, nr. 12, pp. 137-149. ISSN 1811-0770.
[1540] Ibidem.
[1541] SOROCEANU, Igor. Caracteristica generală și definirea conceptului de „omor simplu”. În: *Intellectus*, 2021, nr. 3-4, pp. 161-166. ISSN 1810-7079.
[1542] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 351. 1300 p. ISBN 978-9975-53-470-3.
[1543] Ibidem, p. 351.
[1544] Ibidem, p. 351.
[1545] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 15-16. 592 с. ISBN 978-9975-4158-2-8.
[1546] DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM, p. 93. 261 p. ISBN 978-9975-158-29-9.
[1547] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1548] BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005, p. 305. 804 p. ISBN 9975-79-324-X.
[1549] Ibidem, p. 305.

în acţiunea sau inacţiunea de distrugere ori deteriorare”[1550]; „2) urmările prejudiciabile sub formă de daune în proporţii mari; 3) legătura de cauzalitate dintre fapta prejudiciabilă şi urmările prejudiciabile”.[1551] Nu considerăm justificată această schimbare de poziție. Or, formularea „distrugerea sau deteriorarea [...] bunurilor” are în continuare un caracter eliptic.

Cu privire la ipoteza similară prevăzută de Codul penal al Republicii Azerbaidjan, I.B. Agaev menționează: „Potrivit art. 271 din Codul penal [al Republicii Azerbaidjan], existența doar a uneia dintre urmările prejudiciabile este necesară pentru consumarea infracțiunii”[1552]; „O listă a acestor urmări este dată în alineatul unu al articolului”[1553]; „Acestea includ distrugerea, blocarea, modificarea, copierea informației [...]”.[1554] O opinie apropiată cu privire la ipoteza asemănătoare prevăzută de Codul penal al Federației Ruse este exprimată de V. Krâlov.[1555] Dacă am lua în considerare aceste opinii, ar trebui să afirmăm că formularea „distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice” din art. 259 CP RM vizează nu numai fapta prejudiciabilă, ci și la urmările prejudiciabile.

Considerăm că poziția față de structura laturii obiective a infracțiunilor, prevăzute la art. 259 CP RM, trebuie diferențiată în funcție de modalitățile normative ale acțiunii adiacente din cadrul faptei prejudiciabile. Or, dacă recurgem la formularea folosită de către M.-K. Guiu, atunci doar în cazul unora dintre aceste modalități, „*verbum regens* descrie atât acțiunea, cât și rezultatul material”.[1556] În cazul altor modalități normative ale acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, *verbum regens* descrie doar acțiunea.

Diferențierea structurii laturii obiective a infracțiunii, făcută în funcție de modalitățile normative ale acțiunii adiacente din cadrul faptei prejudiciabile, este propusă într-o ipoteză asemănătoare de către V. Stati: „Latura obiectivă a infracţiunii specificate la alin. (2) art. 245^9 CP RM [...] are următoarea structură: 1) fapta prejudiciabilă care se exprimă în acțiunea sau inacțiunea”[1557] „de încălcare a legislaţiei privind convocarea şi desfăşurarea adunării generale a

---

[1550] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. I*. Chișinău: Tipografia Centrală, 2015, p. 981. 1328 p. ISBN 978-9975-53-469-7.
[1551] Ibidem, p. 981.
[1552] АГАЕВ, И.Б.О. *Уголовное право Азербайджанской Республики*. Москва: Юристъ, 2009, с. 567. 684 с. ISBN 978-5-7975-0975-2.
[1553] Ibidem, с. 567.
[1554] Ibidem, с. 567.
[1555] КРЫЛОВ, В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации. În: *Уголовное право*, 1998, № 3, с. 81-89. ISSN 2071-5870.
[1556] GUIU, Mioara-Ketty. Clasificarea infracțiunilor în raport cu rezultatul lor. În: *Dreptul*, 2017, nr. 12, pp. 137-149. ISSN 1811-0770.
[1557] STATI, Vitalie. *Infracțiuni economice: Note de curs*. Chişinău: Tipografia centrală, 2019, p. 403. 600 p. ISBN 978-9975-146-73-9.

asociaţilor (acţionarilor) societăţii comerciale”[1558]; „2) urmările prejudiciabile constând în daune în proporţii deosebit de mari sau în insolvabilitatea societăţii comerciale; 3) legătura cauzală dintre fapta prejudiciabilă şi urmările prejudiciabile”[1559]; „Într-o altă variantă, latura obiectivă a infracţiunii prevăzute la alin. (2) art. 245^9 CP RM constă în fapta prejudiciabilă”[1560] „care este alcătuită din: a) acțiunea sau inacțiunea de încălcare a legislaţiei privind convocarea şi desfăşurarea adunării generale a asociaţilor (acţionarilor) societăţii comerciale”[1561] „și b) acțiunea de constrângere, dacă această constrângere este exprimată în şantaj sau în ameninţarea cu violenţa ori cu distrugerea sau deteriorarea bunurilor victimei”.[1562] În legătură cu aceeași infracțiune, V. Stati menționează: „Infracţiunea prevăzută la alin. (2) art. 245^9 CP RM este, *după caz, o infracţiune formală sau materială* (evid. ns.)”[1563]; „Ea se consideră consumată, după caz, din momentul: 1) încălcării legislaţiei privind convocarea şi desfăşurarea adunării generale a asociaţilor (acţionarilor) societăţii comerciale”[1564], „însoțite de constrângerea victimei să voteze într-un anumit fel sau să refuze să voteze, dacă această constrângere este exprimată în şantaj sau în ameninţarea cu violenţa”[1565] „ori cu distrugerea sau deteriorarea bunurilor victimei; 2) producerii daunelor în proporţii deosebit de mari”.[1566] Același autor descrie în termeni apropiați momentul de consumare a infracțiunii prevăzute la art. 251 CP RM.[1567]

În continuare, va fi acordată atenție altor două noțiuni ce caracterizează urmările prejudiciabile ale infracțiunilor ce sunt specificate în art. 259 CP RM: „daunele în proporții mari” și „daunele în proporții deosebit de mari”.

E necesar să menționăm că daunele – rezultate datorită distrugerii, deteriorării, modificării, blocării sau copierii informaţiei, ori a dereglării funcţionării calculatoarelor, a sistemului sau a reţelei informatice – caracterizează urmările prejudiciabile nu doar în cazul infracțiunilor prevăzute la art. 259 CP RM. Astfel de daune sunt menționate, de asemenea, în articolele corespondente cu art. 259 CP RM, pe care le conțin unele legi penale străine (și anume – în § 126a CP RA[1568], în subsecț. (5) secț. 230 CP RCe[1569] și în alin. (3) art. 273 CP RCr[1570]).

[1558] Ibidem, p. 403.
[1559] Ibidem, p. 403.
[1560] Ibidem, p. 403.
[1561] Ibidem, p. 403.
[1562] Ibidem, p. 403.
[1563] Ibidem, p. 404.
[1564] Ibidem, p. 404.
[1565] Ibidem, p. 404.
[1566] Ibidem, p. 404.
[1567] Ibidem, p. 270.
[1568] *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html
[1569] *Codul penal al Republicii Cehe*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Cehia-RO.html

Așa cum am menționat *supra*, daunele în proporții mari și, respectiv, daunele în proporții deosebit de mari au devenit părți integrante ale infracțiunilor, prevăzute la art. 259 CP RM, abia după ce a intrat în vigoare Legea nr. 278/2008.

La rândul său, perioada de prezență în art. 259 CP RM a noțiunilor „daunele în proporții mari" și „daunele în proporții deosebit de mari" cunoaște două etape: 1) până a intra în vigoare la 07.11.2015 Legea nr. 207 din 29.07.2016 pentru modificarea și completarea unor acte legislative[1571] (în continuare – Legii nr. 207/2016); 2) după intrarea în vigoare a legii date.

În prima dintre aceste etape, alin. (1) art. 126 CP RM avea dispoziția din care reieșea că proporțiile mari trebuiau să depășească limita de 50000 de lei, iar proporțiile deosebit de mari trebuiau să depășească limita de 100000 de lei. În cea de-a doua etapă, lucrurile s-au schimbat, deoarece la baza determinării proporțiilor mari și a celor deosebit de mari a fost pus criteriul salariului mediu lunar pe economie prognozat, stabilit prin hotărârea de Guvern în vigoare la momentul săvârșirii faptei. Astfel, proporțiile mari și cele deosebit de mari au început să fie stabilite pentru fiecare an aparte. De exemplu, pentru anul 2016 a fost prognozat un salariu mediu lunar pe economie în mărime de 5050 lei.[1572] Aceasta însemna că proporțiile mari trebuiau să depășească limita de 101000 de lei, iar proporțiile deosebit de mari trebuiau să depășească limita de 202000 de lei. Pentru anul 2023 a fost prognozat un salariu mediu lunar pe economie în mărime de 11700 de lei.[1573] Aceasta însemna că proporțiile mari trebuie să depășească limita de 234000 de lei, iar proporțiile deosebit de mari trebuiau să depășească limita de 468000 de lei.

În opinia lui V. Stati, „o astfel de reconsiderare a mecanismului de calcul a proporțiilor mari și deosebit de mari a avut un impact asupra aprecierii gradului prejudiciabil"[1574] „al faptelor incriminate la art. 236-258 CP RM. Acest impact vizează delimitarea ilicitului penal de ilicitul nepenal, dar și graduarea pericolului social al infracțiunilor economice".[1575] Desigur, o constatare similară este valabilă în privința aprecierii gradului prejudiciabil al faptelor incriminate la art. 259 CP RM.

[1570] *Codul penal al Republicii Croaţia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Croatia-RO.html

[1571] Legea pentru modificarea și completarea unor acte legislative: nr. 207 din 29.07.2016. În: *Monitorul Oficial al Republicii Moldova*, 2016, nr. 369-378, 751.

[1572] Hotărârea Guvernului cu privire la aprobarea cuantumului salariului mediu lunar pe economie, prognozat pentru anul 2016: nr. 879 din 23.12.2015. În: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 347-360, 980.

[1573] Hotărârea Guvernului privind aprobarea cuantumului salariului mediu lunar pe economie, prognozat pentru anul 2023: nr. 936 din 28.12.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 438-439, 1041.

[1574] STATI, Vitalie. Impactul adoptării Legii nr. 207/2016 asupra normelor din Capitolul X din partea specială a Codului penal al Republicii Moldova. În: *Актуальные научные исследования в современном мире: XIX Междунар. научн. конф., 26-27 ноября 2016 г., Переяслав-Хмельницкий // Сб. научных трудов*, 2016, Вып. 11, ч. 4, с. 25-29. ISSN 2524-0986.

[1575] Ibidem.

La prima vedere, doar începând cu momentul intrării în vigoare a Legii nr. 207/2016, putem vorbi despre posibilitatea recurgerii la criteriul determinării proporțiilor mari și a celor deosebit de mari în baza salariului mediu lunar pe economie prognozat, stabilit prin hotărârea de Guvern în vigoare la momentul săvârșirii faptei. Or, art. 8 CP RM prevede: „Caracterul infracţional al faptei şi pedeapsa pentru aceasta se stabilesc de legea penală în vigoare la momentul săvârşirii faptei”.[1576] Totuși, nu trebuie de uitat nici de prevederile art. 10 CP RM: „(1) Legea penală care înlătură caracterul infracţional al faptei, care uşurează pedeapsa”[1577] „ori, în alt mod, ameliorează situaţia persoanei ce a comis infracţiunea are efect retroactiv”[1578], „adică se extinde asupra persoanelor care au săvârşit faptele respective până la intrarea în vigoare a acestei legi”[1579], „inclusiv asupra persoanelor care execută pedeapsa ori care au executat pedeapsa, dar au antecedente penale”[1580]; „(2) Legea penală care înăspreşte pedeapsa sau înrăutăţeşte situaţia persoanei vinovate de săvârşirea unei infracţiuni nu are efect retroactiv.”[1581]

De exemplu, pentru anul 2015 a fost prognozat un salariu mediu lunar pe economie în mărime de 4500 de lei.[1582] Aceasta însemna că, în sensul Legii nr. 207/2016, proporțiile mari ar fi trebuit să depășească limita de 90000 de lei, iar proporțiile deosebit de mari ar fi trebuit să depășească limita de 180000 de lei. Bineînțeles, în comparație cu limita de 50000 de lei și, respectiv, de 100000 de lei (care erau specificate în art. 126 CP RM înainte de intrarea în vigoare a Legii nr. 207/2016), astfel de limite „ameliorează situaţia persoanei ce a comis infracţiunea”[1583] în sensul alin. (1) art. 10 CP RM, deci, trebuie să fie extinse asupra persoanelor care au săvârşit faptele respective în 2015. În mod similar, este necesar să se procedeze în privința infracțiunilor săvârșite până în 2015, verificându-se de fiecare dată dacă limitele valorice, ce caracterizează proporțiile mari și cele deosebit de mari, corespund condiției „ameliorează situaţia persoanei ce a comis infracţiunea”[1584] din alin. (1) art. 10 CP RM.

După această intervenție cu caracter clarificator, merită analizat un proiect legislativ, în care sunt propuse, printre altele, anumite amendamente în art. 259 CP RM, care vizează aspectul examinat al urmărilor prejudiciabile: „la alineatul (1), textul „dacă a cauzat daune în proporţii

[1576] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1577] Ibidem.
[1578] Ibidem.
[1579] Ibidem.
[1580] Ibidem.
[1581] Ibidem.
[1582] Hotărârea Guvernului privind aprobarea cuantumului salariului mediu lunar pe economie, prognozat pentru anul 2015: nr. 974 din 04.12.2014. În: *Monitorul Oficial al Republicii Moldova*, 2014, nr. 364-365, 1056.
[1583] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1584] Ibidem.

mari” se substituie cu textul „dacă a cauzat daune considerabile”; la alineatul (2) litera h), textul „în proporţii deosebit de mari” se substituie cu textul „în proporţii mari”; se completează cu alineatul (3) cu următorul cuprins: „(3) Acţiunile prevăzute la alin. (l) sau (2), care au cauzat daune în proporţii deosebit de mari”[1585], „se pedepseşte cu închisoare de la 3 la 7 ani sau cu amendă în mărime de la 1500 până la 3000 unităţi convenţionale”[1586], „iar persoana juridică se pedepseşte cu amendă de la 10000 la 30000 unităţi convenţionale şi lichidarea persoanei juridice.”[1587]

Aceste amendamente au atras reacția justificată a Comisiei Europene pentru Democrație prin Lege (Comisia de la Veneția): „[...] Pct. 31: [...] amendamentul care înlătură enunțul „și dacă a cauzat daune în proporții mari” corespunde abordării generale conform art. 2 al Convenției”[1588]; „Accesul ilegal este o infracțiune de criminalitate informatică fundamentală și ar trebui să fie suficient de vast ca să acopere acțiunile care nu s-au soldat cu daune”[1589]; „[...] Pct. 33: [...] în condițiile legii Republicii Moldova, criminalizarea accesului ilegal depinde de faptul ca intervenția în sistem să fi fost „însoțită de distrugerea, deteriorarea, modificarea, blocarea”[1590] „sau copierea informațiilor și perturbarea funcționării calculatoarelor, a unui sistem informatic sau a unei rețele de calculatoare”[1591] „și să fi „provocat pagube în proporții mari”. Prin urmare, este posibil ca o serie de acte de acces ilegal întreprinse, de exemplu, în scopul de a obține date informatice”[1592], „sau accesul ilegal care nu produce neapărat daune, pătrunderea neautorizată în computerele protejate, accesul prin încălcarea măsurilor de securitate, etc., să fie legale.”[1593]

În următorul capitol al tezei vom exprima propria poziție cu privire la amendamentele care vizează aspectul examinat al urmărilor prejudiciabile, care trebuie operate în art. 259 CP RM.

[1585] *Proiectul de lege pentru modificarea şi completarea unor acte legislative*. [citat 18.12.2020] Disponibil: procuratura.md/file/2020-11-12_proiect%20si%20nota%20info%20cibernetice.pdf
[1586] Ibidem.
[1587] Ibidem.
[1588] *Comisia Europeană pentru Democrație prin Lege (Comisia de la Veneția). Republica Moldova. Proiect de Aviz Comun al Comisiei de la Veneția și al Direcției Generale Drepturile Omului și Statul de Drept (DGI) a Consiliului Europei pe marginea Proiectului de Lege nr. 161 pentru modificarea și completarea legislației moldovenești din domeniul criminalității informatice*. [citat 18.12.2020] Disponibil: https://www.parlament.md/LinkClick.aspx?fileticket=IbGsshOB2Ys%3D&tabid=90&language=ro-RO
[1589] Ibidem.
[1590] Ibidem.
[1591] Ibidem.
[1592] Ibidem.
[1593] Ibidem.

2.2.3. Tentativa și pregătirea în cazul infracțiunilor prevăzute la art. 259 CP RM

În alin. (2) art. 8 din Directiva 2013/40/UE este specificat: „Statele membre se asigură că tentativa de săvârșire a oricăreia dintre infracțiunile prevăzute la articolele 4 și 5 este incriminată”.[1594] În art. 4 și 5 din această directivă sunt menționate noțiuni ca „deteriorarea datelor informatice”, „modificarea datelor informatice” și „blocarea datelor informatice”, care se referă la latura obiectivă a faptelor descrise în respectivele articole. În acest mod, există posibilitatea să se interpreteze că, în art. 259 CP RM, ar trebui să existe o dispoziție aparte în care ar fi stabilită răspunderea pentru tentativa la infracțiunile prevăzute de acest articol.

O impresie asemănătoare produc unele prevederi din art. 11 al Convenției de la Budapesta: „[...] 2. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern”[1595], „orice tentativă săvârşită cu intenţia comiterii uneia dintre infracţiunile stabilite în aplicarea art. 3-5, art. 7, 8 şi a art. 9 paragraful 1 subparagrafele a) şi c)”[1596]; „3. Fiecare parte îşi va putea rezerva dreptul de a nu aplica, în totalitate sau parţial, paragraful 2 al prezentului articol”.[1597]

În legile penale ale anumitor state găsim norme în care este implementată paradigma propusă în cele două acte internaționale sus-menționate (de exemplu, în art. 366 CPR[1598], în § 4 art. 550bis CP RBl[1599], în alin. (3) secț. 8 CP RFi[1600] și în alin. 4 art. 272 CP FR[1601] În conformitate cu art. 9c din Capitolul 4 al CP RSu, este pasibilă de răspundere „persoana care încearcă să obţină acces neautorizat la anumite date destinate prelucrării automate [...]”.[1602] Această formulare lasă semne de întrebare, întrucât în Codul penal al Regatului Suediei nu găsim nicio normă în care ar fi incriminată fapta persoanei care obţine în mod efectiv accesul neautorizat la anumite date destinate prelucrării automate. D. Martin și S. Copețchi afirmă: „Tentativa de infracțiune necesarmente implică săvârşirea unor acte de executare care să ducă la exteriorizarea

---

[1594] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en
[1595] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[1596] Ibidem.
[1597] Ibidem.
[1598] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[1599] Codul penal al Regatului Belgiei. Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html
[1600] *Codul penal al Republicii Finlanda*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Finlanda-RO.html
[1601] Уголовный кодекс Российской Федерации. În: *Собрание законодательства Российской Федерации*, 1996, № 25.
[1602] *Codul penal al Regatului Suediei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Suedia-RO.html

intenției infracționale de a comite infracțiunea”[1603]; „Deci, trebuie să existe o *încercare de a săvârşi infracțiunea* (evid. ns.).”[1604] Probabil, în art. 9c din Capitolul 4 al CP RSu este consacrată concepția, potrivit căreia infracțiunea consumată absoarbe tentativa de infracțiune, odată cu parcurgerea lui *iter criminis*.

În Codul penal al Republicii Moldova identificăm un exemplu care se apropie, sub anumite aspecte, de o astfel de concepție. Este vorba despre art. 342 CP RM prevede răspunderea pentru „atentarea la viaţa Preşedintelui Republicii Moldova, a Preşedintelui Parlamentului sau a Prim-ministrului”[1605], „săvârşită în scopul sistării activităţii lor de stat sau a altei activităţi politice ori din răzbunare pentru asemenea activitate”.[1606] În acest caz, prin „atentare la viață” se are în vedere fie omorul consumat, fie tentativa de omor. Însă, o asemenea abordare are un mare neajuns: ea presupune echivalarea pericolului social al infracțiunii consumate cu pericolul social al tentativei de infracțiune. O asemenea echivalare contravine regulii stabilite în alin. (3) art. 25 CP RM: „Răspunderea pentru [...] tentativă de infracţiune se stabileşte, conform articolului corespunzător din partea specială a prezentului cod”[1607], „ca şi pentru infracţiunea consumată, cu trimitere la art. [...] 27, respectându-se prevederile art. 81.”[1608] Diferențierea pericolului social al infracțiunii consumate cu pericolul social al tentativei de infracțiune nu trebuie lăsată la latitudinea instanței de judecată. O astfel de diferențiere trebui să reprezinte doar prerogativa legiuitorului. De aceea, norme de genul art. 342 CP RM ar trebui să dispară din legea penală autohtonă. De fapt, acest proces se realizează pas cu pas, dovadă fiind abrogarea art. 305 „Atentarea la viaţa judecătorului, a persoanei care efectuează urmărirea penală ori contribuie la înfăptuirea justiţiei”și a art. 350 „Atentarea la viaţa colaboratorului poliţiei” din Codul penal.

Unii doctrinari descriu circumstanțele în care poate fi săvârșită tentativa la infracțiunile prevăzute la art. 259 CP RM. Astfel, M. Gheorghiță afirmă: „În cazul în care fapta comisă a fost suprimată până la apariția faptică a consecințelor menționate”[1609], „aceasta trebuie examinată ca tentativă de acces ilegal la informația computerizată [...]”.[1610] D. Gurev menționează: „În

---

[1603] MARTIN, Daniel, COPEȚCHI, Stanislav. Calificarea tentativei de infracțiune. În: *Integrare prin cercetare şi inovare. Ştiinţe juridice şi economice (10-11 noiembrie 2015)*. Chișinău: CEP USM, 2015, pp. 53-56.
[1604] Ibidem.
[1605] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1606] Ibidem.
[1607] Ibidem.
[1608] Ibidem.
[1609] BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 569. 836 p. ISBN 9975-61-291-1.
[1610] Ibidem, p. 570.

condiţiile în care făptuitorul doreşte să cauzeze daune în proporţii mari”[1611], „cele comise trebuie catalogate drept tentativă la infracţiunea de acces ilegal la informaţia computerizată, în ipoteza în care făptuitorul realizează acţiunea principală”[1612], „dar din cauze independente de voinţa lui să nu-i reuşească comiterea uneia din acţiunile adiacente”.[1613] Prezintă interes, de asemenea, opinia lui D. Martin și S. Copețchi: „Calificarea tentativei de infracțiune are un anumit specific în cazul infracțiunilor materiale în raport cu infracțiunile formale”[1614]; „[...] De exemplu, este posibilă tentativa la infracțiunile formale complexe [...] ori la infracțiunile pasibile de a fi comise în mod etapizat [...] etc.”[1615]; „[...] În cazul infracțiunilor materiale, va exista tentativă atunci când urmarea prejudiciabilă prevăzută de norma incriminatoare: a) nu a survenit”[1616]; „b) a survenit dar nu în volum deplin; „c) a survenit dar alta decât cea cuprinsă de intenția făptuitorului; d) a survenit dar latura obiectivă nu este integral realizată”[1617] „(de exemplu, lipseşte acțiunea principală din cadrul infracțiunilor unice complexe).”[1618]

Astfel, la tentativă se referă următorul exemplu care, cu toate că ține de practica judiciară română, este ilustrativ pentru a percepe esența juridică a tentativei la infracțiunile prevăzute la art. 259 CP RM: „Acelaşi inculpat a pătruns în incinta (...) şi, profitând de neatenţia persoanei vătămate (...), i-a sustras un portofel ce conţinea documente personale, suma de (...) lei, două carduri bancare”[1619], „după care la aceeaşi dată, în jurul orei (...), a încercat să retragă o sumă de bani prin folosirea cardului, la un bancomat, operaţiune nereuşită din cauza tastării greşite a codului PIN”[1620], „după care, în baza aceleiaşi rezoluţii infracţionale, respectiv retragerea de sume de bani pe cardurile bancare sustrase din posesia persoanei vătămate, în jurul orei (...), a încercat să retragă sume de bani”[1621], „de pe cardul emis de (...), întrunesc sub aspect obiectiv și subiectiv elementele constitutive ale infracţiunilor de furt prev. şi ped. de art. 228 alin. 1 Cod penal”[1622], „tentativă la efectuarea de operaţiuni financiare în mod fraudulos, în formă continuată

[1611] GUREV, Dorina. Accesul ilegal la informaţia computerizată: problematica încadrării juridice și soluții. În: *Integrare prin cercetare și inovare. Rezumatele comunicărilor. Științe juridice și economice. Vol. I (10-11 noiembrie 2020)*. Chișinău: CEP USM, 2020, pp. 54-57. ISBN 978-9975-152-48-8.
[1612] Ibidem.
[1613] Ibidem.
[1614] MARTIN, Daniel, COPEȚCHI, Stanislav. Calificarea tentativei de infracțiune. În: *Integrare prin cercetare şi inovare. Ştiinţe juridice și economice (10-11 noiembrie 2015)*. Chișinău: CEP USM, 2015, pp. 53-56.
[1615] Ibidem.
[1616] Ibidem.
[1617] Ibidem.
[1618] Ibidem.
[1619] *Tribunalul București. Sentință penală **** din 02.06.2020*. [citat 18.12.2020] Disponibil: https://www.jurisprudenta.com/jurisprudenta/speta-1763657a/
[1620] Ibidem.
[1621] Ibidem.
[1622] Ibidem.

prev. şi ped. de art. 32 alin. 1 Cod penal rap. la art. 250 alin. 1 Cod penal”[1623] „cu aplic. art. 35 alin. 1 Cod penal şi *tentativă la acces ilegal la un sistem informatic* (evid. ns.)”[1624], „în formă continuată prev. şi ped. de art. 32 alin. 1 Cod penal rap. la art. 360 alin. 1, 2 şi 3 Cod penal cu aplic. art. 35 alin. 1 Cod penal”.[1625] În această speță, încercarea de obține acces la bancomat (care este un sistem informatic) confirmă temeinicia reținerii la calificare a tentativei de acces ilegal la un sistem informatic.

După ce am analizat problema tentativei la infracțiunile prevăzute la art. 259 CP RM, va fi analizată problema pregătirii de aceste infracțiuni.

Conform alin. (2) art. 26 CP RM, „răspunderii penale [...] sunt supuse numai persoanele care au săvârşit pregătirea unei infracţiuni mai puţin grave, grave, deosebit de grave sau excepţional de grave”.[1626] Infracțiunea, ce este prevăzută de alin. (1) art. 259 CP RM, este o infracțiune ușoară. La rândul său, infracțiunea prevăzută la lit. h) alin. (2) art. 259 CP RM, este o infracțiune mai puțin gravă. De aceea, cel puțin în raport cu ultima dintre aceste infracțiuni, este relevant să discutăm despre esența juridică a pregătirii de infracțiune. Spunem „cel puțin”, deoarece nu trebuie neglijată nici analiza pregătirii de infracțiunea, ce este specificată în alin. (1) art. 259 CP RM. O astfel de analiză ne ajută să delimităm pregătirea de această infracțiune de tentativa la ea.

V. Stati afirmă întemeiat: „Latura obiectivă a pregătirii de infracțiune se exprimă în crearea condițiilor pentru săvârșirea unei infracțiuni, nu în săvârșirea infracțiunii de care se pregătește făptuitorul”[1627]; „Latura obiectivă a pregătirii de infracțiune, pe de o parte, și latura obiectivă a tentativei de infracțiune sau a infracțiunii consumate, pe de altă parte, nu pot avea același conținut”[1628]; „Pentru a putea vorbi despre săvârșirea infracțiunii, trebuie să fim în prezența cel puțin a tentativei de infracțiune. Pregătirea de infracțiune este antecedentă în raport cu săvârșirea infracțiunii”[1629]; „Între pregătirea de infracțiune și săvârșirea infracțiunii trebuie să existe un decalaj temporal. Pregătirea de infracțiune trebuie să se încheie înainte de începerea săvârșirii infracțiunii”.[1630] Într-adevăr, ca și tentativa la infracțiune, pregătirea de infracțiune se referă la infracțiunea neconsumată. În ambele cazuri, infracțiunea nu-și produce efectul din cauze care nu depind de voința făptuitorului. Totuși, spre deosebire de tentativa la infracțiune, pregătirea de

[1623] Ibidem.
[1624] Ibidem.
[1625] Ibidem.
[1626] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1627] STATI, Vitalie. Interpretarea sintagmei „săvârșirea infracțiunii”, utilizate în art. 311 din Codul penal al Republicii Moldova. În: *SSRN Electronic Journal*. ISSN 1556-5068. [citat 18.12.2020] Disponibil: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4150275
[1628] Ibidem.
[1629] Ibidem.
[1630] Ibidem.

infracțiune nu presupune începerea executării faptei prejudiciabile. În ipoteza faptelor infracționale ce sunt specificate în art. 259 CP RM, aceasta înseamnă că, din cauze ce nu depind de voința făptuitorului, nu începe executarea acțiunii principale de acces ilegal la informația computerizată.

Anumite exemple ce vizează pregătirea de infracțiunile, ce sunt prevăzute de art. 259 CP RM, sunt prezentate de către A. Pareniuc și A. Ghimpu: „Primul pas în cadrul unui atac informatic îl reprezintă cercetarea sistemului informatic pentru a obţine informaţii importante care pot fi utilizate în atac”[1631]; „Aşadar, este important să se obţină informaţii, cum ar fi, de exemplu, tipul *hardware*-ului utilizat, versiunea *software*, informaţii personale ale utilizatorilor, care pot fi utilizate în următorul pas”[1632]; „Acţiunile utile în obţinerea informaţiilor includ: *„ping sweeps”* (metodă de a scana reţeaua) pentru a determina dacă sistemul informatic ţintă răspunde”[1633]; „scanarea porturilor pentru a observa care porturi pot fi deschise; întrebări care trimit mesaje de avariere înapoi la sistem, când o problemă de transmitere a fost detectată; ghicirea parolelor”.[1634] Desigur, în afară de asemenea exemple, sunt relevante alte exemple care îndeplinesc cerințele stabilite în alin. (1) art. 26 CP RM: înţelegerea prealabilă de a săvârşi infracţiunea; procurarea, fabricarea sau adaptarea mijloacelor ori instrumentelor; crearea intenţionată, pe altă cale, de condiţii pentru săvârşirea ei. Contează ca, în cazurile de această natură, să nu înceapă, din cauze care nu depind de voința făptuitorului, executarea acțiunii principale de acces ilegal la informația computerizată.

În legile penale ale unor țări, putem identifica reglementări în care se incriminează distinct pregătirea de infracțiunile care sunt similare cu infracțiunile prevăzute la art. 259 CP RM.

De exemplu, § 202c CP RFG („Pregătirea faptei de spionare şi interceptare de date”) prevede: „(1) Persoana care pregăteşte o faptă prevăzută la § 202a sau § 202b prin aceea că produce, îşi procură sau procură unei alte persoane, vinde, transmite, diseminează”[1635] „sau facilitează în alt mod accesul la 1. parole sau alte coduri de siguranţă care permit accesul la date (§ 202a alin. 2)”[1636] „sau 2. programe informatice al căror scop este săvârşirea unei astfel de fapte se pedepseşte cu închisoarea de până la 2 ani sau cu amendă”.[1637]

[1631] PARENIUC, Alexandru, GHIMPU, Andrei. Tipurile și metodele de săvârșire a infracțiunilor informaționale. În: *Legea şi Viaţa*, 2021, nr. 1-2, pp. 54-60. ISSN 2587-4365.
[1632] Ibidem.
[1633] Ibidem.
[1634] Ibidem.
[1635] *Codul penal al Republicii Federale Germania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Germania-RO.html
[1636] Ibidem.
[1637] Ibidem.

Codul penal al Republicii Moldova conține două articole în care găsim formulări apropiate de cele din § 202c CP RFG (și anume – art. 260 și 260^4 CP RM).

Un exemplu asemănător este specificat în Decizia Înaltei Curți de Casaţie și Justiţie a României nr. 15 din 14.10.2013 privind interpretarea şi aplicarea unitară a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noţiunii de acces fără drept la un sistem informatic: „Montarea la bancomat a dispozitivelor autonome de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia”[1638] „(skimmere, minivideocamere sau dispozitive tip tastatură falsă) constituie infracţiunea prevăzută de art. 46 alin. (2) din Legea nr. 161/2003”.[1639] Precizăm că art. 46 (actualmente abrogat) al Legii României nr. 161/2003 prevedea: „(1) Constituie infracţiune şi se pedepseşte cu închisoare de la 1 la 6 ani: a) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziţie, sub orice altă formă”[1640], „fără drept, a unui dispozitiv sau program informatic conceput sau adaptat în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45”[1641]; „b) fapta de a produce, vinde, de a importa, distribui sau de a pune la dispoziţie, sub orice altă formă, fără drept, a unei parole”[1642], „cod de acces sau alte asemenea date informatice care permit accesul total sau parţial la un sistem informatic în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45”[1643]; „(2) Cu aceeaşi pedeapsă se sancţionează şi deţinerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de acces sau dată informatică dintre cele prevăzute la alin. (1)”[1644] „în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45”.[1645]

În Codul penal al României[1646], prevederilor de la art. 46 al Legii României nr. 161/2003 le corespund prevederile art. 365 „Operațiuni ilegale cu dispozitive sau programe informatice”.[1647]

[1638] Decizia Înaltei Curți de Casaţie și Justiţie a României privind interpretarea şi aplicarea unitară a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noţiunii de acces fără drept la un sistem informatic: nr. 15 din 14.10.2013. În: *Monitorul Oficial al României*, 2013, nr. 760.

[1639] Ibidem.

[1640] Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice și în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.

[1641] Ibidem.

[1642] Ibidem.

[1643] Ibidem.

[1644] Ibidem.

[1645] Ibidem.

[1646] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.

[1647] Acest articol prevede: „(1) Fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziție sub orice formă”*: „a) dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre infracțiunile prevăzute în art. 360-364”*; „b) parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic, în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364”*, „se pedepsește cu închisoare de la 6 luni la 3 ani sau cu amendă”*; „(2) Deținerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces sau a altor date informatice dintre cele prevăzute în alin. (1)”*, „în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364, se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă.*

Ca urmare, explicația din Decizia Înaltei Curți de Casaţie și Justiţie a României, prezentată *supra*, își menține valabilitatea, cu ajustările de rigoare.

Această explicație poate fi aplicată (desigur, cu ajustările de rigoare) la realitățile juridice din Republica Moldova. În context, prezintă interes câteva spețe din practica judiciară autohtonă.

Propunem atenției prima dintre aceste spețe: D.M. și C.K. au fost condamnați în baza alin. (5) art. 42 și art. 260, alin. (5) art. 42 și lit. b), e) alin. (2) art. 259, alin. (5) art. 42, art. 26 și alin. (1) art. 237 CP RM. D.V. a fost condamnat în baza alin. (2) și (3) art. 42, art. 46 și art. 260, alin. (2) și (3) art. 42, art. 46 și lit. b), e) alin. (2) art. 259, alin. (2) și (3) art. 42, art. 26 și alin. (1) art. 237 CP RM. În iulie 2014, D.M., C.K. și D.V. au intrat pe teritoriul Republicii Moldova. La 30.08.2014 şi 31.08.2014, D.V. a instalat în unele bancomatele de pe teritoriul mun. Chişinău mijlocul tehnic special de tip „skimmer”, conceput şi adaptat în scopul săvârșirii infracţiunilor prevăzute la art. 237 şi 259 CP RM. D.M. a copiat şi a prelucrat informaţia accesată şi obținută ilegal de pe cardurile bancare, iar C.K. a asigurat transportarea participanților și a utilajului, precum şi a supravegheat ca participanții să nu fie identificaţi de către reprezentanţii organelor de drept. După instalarea mijlocului tehnic special de tip „skimmer”, făptuitorii au dobândit ilegal mijloace bănești în proporții mari și au încercat să dobândească ilegal alte mijloace bănești.[1648]

Într-o altă speță, D.M., D.V. și C.K. au fost condamnați în baza art. 46 și 260, art. 46 și lit. b), e), h) alin. (2) art. 259, art. 26, 46 și lit. c), d) alin. (2) art. 237 CP RM. C.K., în iulie 2014, împreună cu A.B., D.M. și D.V., au participat la crearea unei reuniuni stabile de persoane, constituind un grup criminal organizat în scopul comiterii mai multor infracţiuni cu cauzarea de daune în proporţii deosebit de mari. La 11.07.2014, în urma înţelegerii prealabile, împreună cu A.B., D.M. și D.V., C.K. a intrat pe teritoriul Republicii Moldova prin punctul de trecere a ftontierei de stat „Giurgiulești – Galați”, importând ilegal mijlocul tehnic special de tip „skimmer”, acesta fiind conceput şi adaptat în scopul săvârşirii infracţiunilor prevăzute la art. 237 şi 259 CP RM. Urmărind scopul culegerii informaţiilor de pe carcfurile bancare pentru utilizarea ulterioară la confecţionarea cardurilor bancare cu ajutorul cărora urmau să fie dobândite ilegal mijloace bănești, în perioada 13.07.2017 – 15.07.2014, făptuitorii au instalat ilegal mijlocul tehnic de tip „skimmer” pe un bancomat din mun. Chișinău, care aparţinea unei bănci comerciale. Pe această cale, făptuitorii au accesat ilegal informaţia de pe cardurile bancare ale 158 de deținători de carduri bancare, pe care au copiat-o pe un dispozitiv de stocare a

* Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.

[1648] *Sentința Judecătoriei sect. Botanica, mun. Chișinău, din 11.12.2014. Dosarul nr. 1-620/2014*. [citat 18.12.2020] Disponibil: https://jc.instante.justice.md/ro/pigd_integration/pdf/3798ed32-4281-e411-8112-005056a5d154

informaţiei. În continuare, la 15.07.2014, fiind în posesia datelor copiate ilegal, cei patru făptuitori au părăsit teritoriul Republicii Moldova prin punctul de trecere a ftontierei de stat „Leuşeni – Albița”. Ulterior, în perioada 18.07.2014 – 21.07.2014, de pe teritoriul Republicii Bulgaria, prin utilizarea datelor informatice copiate ilegal ale celor 158 de deținători de carduri bancare, făptuitorii au extras ilegal bani în sumă totală de 122925,16 lei.[1649]

În fine, în a treia speță, T.M. și P.A. au fost condamnați în baza art. 26, alin. (2) art. 42, lit. b), e) alin. (2) art. 259 și art. 27, alin. (3) art. 42 și art. 260 CP RM. La data de 24.07.2015, XXX și XXX s-au deplasat în Regatul Bahrain, având intenția de a accesa ilegal informația computerizată de pe suporții materiali de informație în scopul copierii informației de pe carduri de plată. Aceștia au organizat expedierea în Regatul Bahrain din Republica Moldova a mijloacelor tehnice speciale de tip „skimmer”. Ca urmare, la indicația lui XXX, la data de 04.08.2015, XXX împreună cu XXX au expediat în Regatul Bahrain, prin intermediul unui serviciu de expedieri, pe numele lui X, a unui colet care conținea mijlocul tehnic special de tip „skimmer”. Din motiv că echipamentul urma să ajungă la destinație în Regatul Bahrain aproximativ în 4-5 zile lucrătoare, la data de 05.08.2015, XXX a insistat ca XXX să anuleze această comandă și să caute posibilitatea de a urgenta expedierea în Regatul Bahrain a mijlocului tehnic special de tip „skimmer”. La 06.08.2015, XXX a recuperat coletul de la serviciul de expedieri, urmând să caute altă modalitate de expediere în scopul urgentării punerii la dispoziția lui XXX și XXX a mijlocului tehnic special de tip „skimmer”, moment in care XXX a fost reținut în flagrant. Ulterior, XXX și XXX, prin utilizarea mijlocului tehnic special de tip „skimmer”, ar fi urmat să acceseze informația cu privire la deținătorii de carduri bancare.[1650]

În toate cele trei spețe, aduse ca exemple, este specificat mijlocul tehnic special de tip „skimmer”, conceput şi adaptat în scopul săvârşirii, printre altele, a infracţiunilor ce sunt specificate în art. 259 CP RM. Din spețe nu este clar dacă făptuitorii au produs acest mijloc tehnic. Termenul „import”, menționat în cea de-a doua speță, este utilizat impropriu. Nu este posibil să importi ceva de la tine însuți. Pentru a vorbi despre un importator, este necesar ca o altă persoană să fie exportator. Aceleași persoane nu pot cumula ambele aceste calități. Doar în cea de-a treia speță sunt prezente anumite indicii despre punerea la dispoziţie a mijlocului tehnic special de tip „skimmer”. Cu toate acestea, lasă loc pentru dubii folosirea nereușită și abuzivă a

[1649] *Decizia Colegiului penal al Curții de Apel Chişinău din 15.06.2015. Dosarul nr. 1a-805/2015*. [citat 18.12.2020] Disponibil: https://cac.instante.justice.md/ro/pigd_integration/pdf/87ea8f58-4316-e511-b888-005056a5d154

[1650] *Sentința Judecătoriei sect. Botanica, mun. Chişinău, din 26.02.2016. Dosarul nr. 1-12/2016*. [citat 18.12.2020] Disponibil: https://instante.justice.md/ro/pigd_integration/pdf/691A992F-6DDC-E511-A1AB-005056A5D154; *Sentința Judecătoriei sect. Botanica, mun. Chişinău, din 30.06.2016. Dosarul nr. 1-163/2016*. [citat 18.12.2020] Disponibil: https://jc.instante.justice.md/ro/pigd_integration/pdf/3fd536fe-cd3e-e611-9a6d-005056a5d154

aceluiași lexem „XXX” în raport cu persoane diferite. În concluzie, în primele două spețe, este lipsită de temei invocarea art. 260 CP RM.

În afară de aceasta, atrage atenția faptul că, în primele două spețe, se aplică răspunderea atât în baza art. 260 CP RM, cât și pentru pregătirea de una dintre infracțiunile prevăzute la art. 237 CP RM. Totodată, în aceleași spețe, la calificare nu este reținută pregătirea de una dintre infracțiunile ce sunt prevăzute de art. 259 CP RM. O astfel de abordare trezește îndoieli. În art. 260 CP RM, ca scop al infracțiunii este specificată săvârșirea infracțiunilor prevăzute, printre altele, la art. 237 sau 259 CP RM. Dacă pretinsa producere și importare a mijlocului tehnic special de tip „skimmer” a fost considerată temei de aplicare a art. 260 CP RM, nu este clar de ce aceeași pretinsă producere și importare a mijlocului tehnic special de tip „skimmer” a fost considerată în plus pregătire de una dintre infracțiunile prevăzute la art. 237 CP RM. O astfel de pregătire ar trebui să se concretizeze într-o activitate diferită de pretinsa producere și importare a mijlocului tehnic special de tip „skimmer”. Doar în aceste condiții ar fi întemeiată reținerea la calificare a pregătirii de una dintre infracțiunile prevăzute la art. 237 CP RM.

În mod similar, în cea de-a treia speță, se aplică răspunderea atât în baza art. 260 CP RM, cât și pentru pregătirea de una dintre infracțiunile prevăzute la art. 259 CP RM. Însă, nu avem confirmarea faptului că o astfel de pregătire se concretizează într-o altă activitate decât punerea la dispoziție a mijlocului tehnic special de tip „skimmer”. În aceste condiții, lipsește temeiul reținerii la calificare a pregătirii de una dintre infracțiunile prevăzute la art. 259 CP RM. Trebuie aplicat doar art. 260 CP RM, care, așa cum am afirmat mai sus, constituie un exemplu de pregătire *sui generis* de infracțiunile prevăzute la art. 259 CP RM. În caz contrar – dacă se aplică răspunderea atât în baza art. 260 CP RM, cât și pentru pregătirea de una dintre infracțiunile prevăzute la art. 259 CP RM – aceeași faptă este sancționată dublu. Ceea ce este inechitabil și abuziv.

2.2.4. Legătura cauzală în cazul infracțiunilor prevăzute la art. 259 CP RM

Ultimul aspect al laturii obiective, la care ne vom referi, este legătura cauzală ca semn constitutiv al laturii obiective a infracțiunilor care sunt specificate în art. 259 CP RM.

Anterior s-a relevat că infracțiunile, care sunt prevăzute de art. 259 CP RM, sunt infracțiuni materiale. Din aceasta rezultă că, în mod obligatoriu, urmările prejudiciabile, care sunt prevăzute în acest articol, sunt legate cauzal cu fapta prejudiciabilă care este specificată în art. 259 CP RM.

În următoarea speță, această condiție nu este îndeplinită: D.M., D.V. și C.K. au fost condamnați în baza art. 46 și 260, art. 46 și lit. b), e), h) alin .(2) art. 259, art. 26, 46 și lit. c), d) alin. (2) art. 237 CP RM. C.K., în iulie 2014, împreună cu A.B., D.M. și D.V., au participat la crearea unei reuniuni stabile de persoane, constituind un grup criminal organizat în scopul comiterii mai multor infracţiuni cu cauzarea de daune în proporţii deosebit de mari. La 11.07.2014, în urma înţelegerii prealabile, împreună cu A.B., D.M. și D.V., C.K. a intrat pe teritoriul Republicii Moldova prin punctul de trecere a ftontierei de stat „Giurgiulești – Galați", importând ilegal mijlocul tehnic special de tip „skimmer", acesta fiind conceput şi adaptat în scopul săvârşirii infracţiunilor prevăzute la art. 237 şi 259 CP RM. Urmărind scopul culegerii informaţiilor de pe carcfurile bancare pentru utilizarea ulterioară la confecţionarea cardurilor bancare cu ajutorul cărora urmau să fie dobândite ilegal mijloace bănești, în perioada 13.07.2017 – 15.07.2014, făptuitorii au instalat ilegal mijlocul tehnic de tip „skimmer" pe un bancomat din mun. Chișinău, care aparţinea unei bănci comerciale. Pe această cale, făptuitorii au accesat ilegal informaţia de pe cardurile bancare ale 158 de deținători de carduri bancare, pe care au copiat-o pe un dispozitiv de stocare a informaţiei. În continuare, la 15.07.2014, fiind în posesia datelor copiate ilegal, cei patru făptuitori au părăsit teritoriul Republicii Moldova prin punctul de trecere a ftontierei de stat „Leușeni – Albița". Ulterior, în perioada 18.07.2014 – 21.07.2014, de pe teritoriul Republicii Bulgaria, prin utilizarea datelor informatice copiate ilegal ale celor 158 de deținători de carduri bancare, făptuitorii au extras ilegal bani în sumă totală de 122925,16 lei.[1651]

În această speță, lipsește legătură cauzală dintre daunele în proporții deosebit de mari și acțiunea adiacentă de copiere a informației computerizate, prevăzută la art. 259 CP RM. De fapt, proporțiile deosebit de mari se referă exclusiv la infracțiunea prevăzută la art. 237 CP RM. Accesul ilegal la informația computerizată (și anume – la informația de pe cardurile bancare), urmat de copierea acestei informații, nu a fost un scop în sine. Scopul a fost punerea în circulaţie a cardurilor în proporţii deosebit de mari. Proporțiile deosebit de mari nu pot să apară concomitent atât în contextul infracțiunii prevăzute la lit. h) alin. (2) art. 259 CP RM, cât și în contextul infracțiunii prevăzute la lit. d) alin. (2) art. 237 CP RM. Dacă interpretăm altfel, atunci ar reieși că punerea în circulaţie a cardurilor în proporţii deosebit de mari ar trebui echivalată cu distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, ori cu dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor

[1651] *Decizia Colegiului penal al Curții de Apel Chișinău din 15.06.2015. Dosarul nr. 1a-805/2015*. [citat 18.12.2020] Disponibil: https://cac.instante.justice.md/ro/pigd_integration/pdf/87ea8f58-4316-e511-b888-005056a5d154; *Decizia Colegiului penal lărgit al CSJ din 15.03.2016. Dosarul nr. 1ra-87/2016*. [citat 18.12.2020] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=6000

în proporții deosebit de mari. Însă, o astfel de echivalare nu este posibilă, fiind infirmată de cele relatate în speță.

În alt context, în prezența ambelor variante ale laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, urmările prejudiciabile sunt legate cauzal de acțiunea adiacentă de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care, la rândul său, este legată cauzal de acțiunea principală de acces ilegal la informația computerizată. După E.A. Russkevici, care ia în vizor infracțiunile ce sunt prevăzute de art. 259 CP RM, „în practică, stabilirea unui raport de cauzalitate între accesul ilegal în sine și daunele, cauzate victimei, poate provoca dificultăți semnificative”.[1652] În replică, menționăm că, chiar dacă procesul de stabilire a legăturii cauzale este dificil în cazul faptelor infracționale specificate în art. 259 CP RM, altă cale nu există. Urmările prejudiciabile, prevăzute la art. 259 CP RM, trebuie să fie legate cauzal de acțiunea adiacentă de distrugere, deteriorare sau modificare a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, nu de acțiunea principală de acces ilegal la informația computerizată. Acțiunea principală de acces ilegal la informația computerizată nu poate, de una singură, să reprezinte cauza producerii urmărilor prejudiciabile care sunt prevăzute la art. 259 CP RM. G. Zlati exclude posibilitatea producerii unui prejudiciu material în situația infracțiunii prevăzute la art. 360 CPR, care, amintim, presupune accesul, fără drept, la un sistem informatic.[1653] Susținem această opinie.

Fapta prejudiciabilă, ce este specificată în art. 259 CP RM, trebuie să reprezinte cauza indispensabilă a survenirii urmărilor prejudiciabile care sunt prevăzute în acest articol. În caz contrar, lipsește temeiul aplicării acestui articol. De pildă, într-o speță a fost pronunțată soluția de condamnare a lui P.D. în baza art. 260^4 şi alin. (1) art. 245^{10} CP RM. B.A. a fost condamnat în baza alin. (2) art. 245^{10} CP RM. În perioada 23.12.2015 – 05.01.2016, aflându-se în mun. Chişinău, P.D. a accesat neautorizat serverul unei întreprinderi și a sustras informaţii ce conţineau un secret comercial. De asemenea, P.D. a modificat şi a șters datele informatice din acest sistem informatic, în rezultat fiind perturbată activitatea respectivei întreprinderi și fiind cauzate daune în proporţii mari. La rândul său, B.A. a pus la dispoziţia lui P.D. numele de utilizator şi parola de acces, necesare accesării neautorizate a serverului respectivei

[1652] РУССКЕВИЧ, Е.А. Законодательные подходы к криминализации деяний, связанных с неправомерным доступом к компьютерной информации в странах Содружества Независимых Государств. În: *Журнал зарубежного законодательства и сравнительного правоведения*, 2018, № 1, с. 116-121. ISSN 1991-3222.
[1653] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Editura Solomon, 2020, p. 237-238. 658 p. ISBN 978-606-8892-62-7.

întreprinderi.[1654] În această speță au fost cauzate daune în proporții mari. În afară de aceasta, a fost săvârșită acțiunea de acces ilegal la informația computerizată. Această acțiune a fost succedată atât de sustragerea unor informaţii ce conţineau un secret comercial, cât și de acțiunea de modificare şi ștergere a datelor informatice din sistemul informatic. Sustragerea unor informaţii ce conţineau un secret comercial reprezintă o formă specială de copiere a informației computerizate, protejate de lege. Astfel, alin. (1) art. 245^{10} CP RM apare ca normă specială în raport cu lit. g) alin. (2) art. 259 CP RM. În aceste condiții, modificarea datelor informatice din sistemul informatic își pierde relevanța în planul calificării infracțiunii.

În același timp, în speța respectivă, lipsește temeiul aplicării art. 260^4 CP RM. Scopul infracțiunilor, ce sunt prevăzute de acest articol, este săvârșirea uneia dintre infracţiunile prevăzute la art. 237, 259, 260^1-260^3, 260^5 şi 260^6 CP RM. Comiterea infracțiunilor, care sunt prevăzute de normele, care sunt speciale față de aceste articole, nu poate să reprezinte scopul infracțiunilor prevăzute la art. 260^4 CP RM.

2.3. Latura subiectivă a infracțiunilor prevăzute la art. 259 CP RM

2.3.1. Vinovăția manifestată în cazul infracțiunilor prevăzute la art. 259 CP RM

În alin. (3) § 12 CP RE („Elementele constitutive ale infracţiunii”) se menționează: „Elementele laturii subiective a infracţiunii sunt intenţia sau neglijenţa. Legea poate prevedea un motiv, un scop sau alte elemente subiective constitutive ale infracţiunii”.[1655] În legea penală a Republicii Moldova lipsește norma în care ar fi relevată structura laturii subiective a infracțiunii. Din aceste considerente, este necesar să analizăm punctele de vedere ale doctrinarilor referitoare la o asemenea structură.

Din următoarea opinie, exprimată de S. Pilat, nu rezultă clar ce include sistemul laturii subiective a infracțiunii: „Latura subiectivă constituie altceva decât atitudinea psihică interioară a infractorului față de fapta săvârșită și consecințele ei”.[1656] Dacă atitudinea psihică a făptuitorului în raport cu fapta prejudiciabilă și cu urmările prejudiciabile nu face parte din sistemul laturii subiective a infracțiunii, atunci care alt sistem include o asemenea atitudine?

[1654] *Decizia Colegiului penal al Curții de Apel Chișinău din 21.11.2017. Dosarul nr. 1a-842/2017*. [citat 18.12.2020] Disponibil: https://cac.instante.justice.md/ro/pigd_integration/pdf/ac0d8691-62f1-e711-80d5-0050568b7027

[1655] *Codul penal al Republicii Estonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Estonia-RO.html

[1656] PILAT, Sofia. Elementele subiective ale vandalismului: concept şi caracterizare. În: *Anale ştiinţifice ale Academiei „Ştefan cel Mare” a MAIRM: ştiinţe juridice*, 2022, nr. 15, pp. 201-213. ISSN 1857-0976.

În comparație cu părerea precedentă, cea a lui E. Jenunchi este mai clară: „Latura subiectivă, ca element al infracţiunii, este determinată de atitudinea psihică a făptuitorului faţă de fapta prejudiciabilă săvârşită şi faţă de urmările prejudiciabile ale acesteia.”[1657] Aceeași autoare își completează răspunsul: „Vinovăția constituie nucleul laturii subiective a infracțiunii, dar nu cuprinde complet conținutul acesteia.”[1658] Punctul de vedere al lui A. Șavga confirmă teza, conform căreia sistemul laturii subiective a infracțiunii nu se reduce la atitudinea psihică a făptuitorului în raport cu prejudiciabilă și cu urmările prejudiciabile: „Latura subiectivă a componenţei infracţiunii constituie partea interioară a infracţiunii”[1659], „care determină atitudinea psihică a făptuitorului faţă de fapta prejudiciabilă săvârșită și de urmările acesteia, sub raportul conștiinţei, voinţei și emoţiilor sale.”[1660]

Per ansamblu, latura subiectivă a infracţiunii se exprimă în atitudinea psihică a făptuitorului în raport cu fapta prejudiciabilă și cu urmările prejudiciabile, precum și în motiv, scop și emoții.

Referitor la atitudinea psihică a făptuitorului în raport cu fapta prejudiciabilă și cu urmările prejudiciabile, în art. 6 CP RM se menționează: „Persoana este supusă răspunderii penale şi pedepsei penale numai pentru fapte săvârșite cu vinovăție”[1661] (alin. (1)); „Răspunderii penale şi pedepsei penale este supusă numai persoana care a săvârșit cu intenție sau din imprudență o faptă prevăzută de legea penală”[1662] (alin. (2)). De asemenea, conform alin. (2) art. 51 CP RM, „răspunderii penale este supusă numai persoana vinovată de săvârşirea infracţiunii prevăzute de legea penală”.[1663] Interpretarea acestor norme ne arată că vinovăția reprezintă semnul obligatoriu al laturii subiective a oricărei infracțiuni. Din aceleași norme rezultă că vinovăția: a) constă în atitudinea psihică a făptuitorului față de fapta prejudiciabilă și față de urmările prejudiciabile; b) se concretizează în intenție sau în imprudență.

În art. 259 CP RM nu este indicată forma de vinovăție. Pentru cazuri de acest gen, S. Copețchi și I. Hadârcă propun următoarea soluție: „Atunci când forma vinovăţiei nu este prevăzută expres în dispoziţia normei de incriminare”[1664], „aceasta poate să rezulte din semantismul anumitor noţiuni cu care operează legiuitorul la descrierea faptei prejudiciabile ori

---

[1657] JENUNCHI, Elena. Latura subiectivă a infracțiunii de constrângere de a face declarații. În: *Supremația Dreptului*, 2020, nr. 1, p. 171-176. ISSN 2587-4128.
[1658] Ibidem.
[1659] GRAMA, Mariana, BOTNARU, Stela, ȘAVGA, Alina, GROSU, Vladimir. *Drept penal. Partea generală. Vol. I*. Chișinău: Tipografia Centrală, 2012, p. 232. 328 p. ISBN 978-9975-53-080-4.
[1660] Ibidem.
[1661] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1662] Ibidem.
[1663] Ibidem.
[1664] COPEȚCHI, Stanislav, HADÎRCĂ, Igor. Calificarea infracţiunilor după latura subiectivă. În*: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2015, nr. 11, pp. 61-68. ISSN 1814-3199.

din esenţa faptei”.[1665] Art. 3 „Accesarea ilegală a sistemelor informatice” din Directiva 2013/40/UE prevede: „Statele membre adoptă măsurile necesare pentru a garanta că accesarea *cu intenție* (evid. ns.) și fără drept a unui sistem informatic”[1666] „sau a unei părți a acestuia este incriminată atunci când este săvârșită prin încălcarea unei măsuri de securitate”[1667], „cel puțin atunci când nu reprezintă un caz minor.”[1668] Aceeași formă de vinovăție este indicată în art. 2 „Accesarea ilegală” din Convenția de la Budapesta: „Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune”[1669], „potrivit dreptului său intern, accesarea *intenţionată* (evid. ns.) şi fără drept a ansamblului ori a unei părţi a unui sistem informatic. [...]”.[1670] În pct. 39 din Raportul explicativ la Convenția de la Budapesta se explică: „Toate infracțiunile cuprinse în Convenție trebuie să fie comise „intenționat” pentru a se aplica răspunderea penală”[1671]; „[...] Elaboratorii Convenției au fost de acord că sensul exact al cuvântului „intenționat” ar trebui lăsat la latitudinea interpretării naționale”.[1672]

În unele norme, care se aseamănă cu art. 259 CP RM, este specificată imprudența ca formă de vinovăție. Astfel, în alin. 2 art. 176[1] CP RM din 1961, era incriminat accesul ilegal (nesancţionat) la informaţia ce se păstrează în sistemul computerizat, cu încălcarea sistemului de protecţie, săvârşit „din imprudenţă, care a cauzat nimicirea sau blocarea informaţiei, precum şi scoaterea din funcţiune a utilajului computerizat ori alte urmări grave”.[1673] O concepție similară este promovată în pct. 3° § 3 art. 550bis CP RBl[1674] și în art. 251 din Codul penal al Republicii Armenia.[1675] Astfel de exemple alimentează într-o anumită măsură incertitudinile cu privire la forma de vinovăție în cazul faptelor infracționale ce sunt prevăzute de art. 259 CP RM.

Considerăm că problema dată trebuie rezolvată în contextul nu doar al art. 259 CP RM, ci al întregii părți speciale a Codului penal al Republicii Moldova. Sunt destule exemple care pot inspira legiuitorul moldovean. Astfel, alin. (6) art. 16 CPR prevede: „Fapta constând într-o

---

[1665] Ibidem.
[1666] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en
[1667] Ibidem.
[1668] Ibidem.
[1669] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[1670] Ibidem.
[1671] *Explanatory Report to the Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/16800cce5b
[1672] Ibidem.
[1673] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
[1674] *Codul penal al Regatului Belgiei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html
[1675] *Уголовный кодекс Республики Армения*. [citat 18.12.2020] Disponibil www.parliament.am/legislation.php?ID=1349&lang=rus&sel=show

acțiune sau inacțiune constituie infracțiune când este săvârșită cu intenție”[1676]; „Fapta comisă din culpă constituie infracțiune numai când legea o prevede în mod expres”.[1677] Dispoziții similare conțin alin. (1) § 7 CP RA[1678] și în art. 13 din Codul penal al Republicii Portugheze.[1679] Propunem ca legea penală autohtonă să fie completată cu o normă similară.

În legătură cu infracțiunile formale, I. Hadîrcă se întreabă: „Cum poate făptuitorul să admită conştient că săvârşeşte o acţiune (inacţiune) prejudiciabilă?”[1680]; „Odată ce el o săvârşeşte, rezultă în mod inevitabil că o şi doreşte. O altă concluzie ar intra în contradicţie cu regulile logicii”.[1681] Așadar, despre intenție directă vorbim în cazul infracțiunilor formale sau în cazul infracțiunilor materiale care presupun prezența unui scop special. Despre intenție indirectă vorbim în cazul infracțiunilor materiale care nu presupun prezența unui scop special.

Poziţia cvasiunanimă din doctrina de specialitate este că infracţiunile, prevăzute la art. 259 CP RM, pot fi comise cu intenţie directă sau cu intenție indirectă.[1682] Susținem această poziție.

2.3.2. Motivul, scopul și emoțiile în cazul infracțiunilor prevăzute la art. 259 CP RM

Mai sus am menționat că latura subiectivă a infracţiunii cuprinde nu numai atitudinea psihică a făptuitorului în raport cu fapta prejudiciabilă și cu urmările prejudiciabile, dar și motivul, scopul și emoțiile.

Motivul și scopul infracțiunii se aseamănă sub anumite aspecte, însă nu trebuie confundate. În context, E. Boțian afirmă: „Activitatea umană conștientă este declanșată de un anumit mobil și

---

[1676] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[1677] Ibidem.
[1678] *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html
[1679] *Codul penal al Republicii Portugheze*. [citat 18.12.2020] Disponibil https://codexpenal.just.ro/laws/Cod-Penal-Portugalia-RO.html
[1680] HADÎRCĂ, Igor. Elementele constitutive subiective ale infracţiunilor prevăzute la art. 217, 217[1]-217[6], 218 şi 219 C. pen. RM. În: *Revista Naţională de Drept*, 2008, nr. 2, pp. 46-53. ISSN 1811-0770.
[1681] Ibidem.
[1682] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chişinău: Tipografia Centrală, 2015, p. 355. 1300 p. ISBN 978-9975-53-470-3; BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0; BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 570. 836 p. ISBN 9975-61-291-1; BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004, p. 366. 622 p. ISBN 9975-9788-7-8; ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 19. 592 с. ISBN 978-9975-4158-2-8; ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista ştiinţifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081; SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261[1] Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf

este orientată spre un anumit scop. [...] Scopul nu trebuie confundat cu mobilul, deoarece scopul se referă la momentul finalizării actului, pe cand mobilul este legat de momentul luării hotărârii”.[1683] De asemenea, S. Copețchi menționează: „Motivul și scopul sunt organic legate între ele, în cele mai dese cazuri motivul fiind fundamentul scopului format”[1684]; „Totuși, motivul și scopul infracțiunii au un caracter de sine stătător, motiv pentru care nu trebuie suprapuse”.[1685]

Mai sus am afirmat că vinovăția reprezintă semnul obligatoriu al laturii subiective a oricărei infracțiuni. Motivul și scopul infracțiunii nu întotdeauna au un caracter obligatoriu. Conform alin. 4 art. 9 din Codul penal al Republicii Cipriote (în continuare – CP RCi), „cu excepţia cazului în care se prevede altfel în mod expres”[1686], „mobilul care a determinat făptuitorul la săvârşirea acţiunii sau inacţiunii sau la formarea intenţiei care l-a motivat în aceste practici nu afectează răspunderea penală”.[1687] Această regulă, stabilită de legiuitorul cipriot, poate fi extrapolată asupra scopului infracțiunii.

După părerea lui A. Cazacicov: „Semnele laturii subiective se subdivid în două categorii: obligatorii şi facultative. Semnele facultative au importanță pentru calificarea infracţiunii”[1688], „iar cele facultative sunt relevante doar individualizării răspunderii penale. În această ordine de idei, vinovăția este trecută la semnul obligatoriu al laturii subiective, celelalte semne – scopul”[1689], „motivul (mobilul), emoțiile, sunt considerate facultative. Prin excepție, legiuitorul utilizează în textul infracţiunii concrete unele semne facultative ale laturii subiective”[1690], „în acest caz considerându-le obligatorii pentru calificarea faptei”.[1691] Nu este clar cum un semn al laturii subiective a infracțiunii poate fi, concomitent, obligatoriu și facultativ.

Cât privește faptele infracționale specificate în art. 259 CP RM, V. Soltan menționează: „Cauzele şi scopurile infracţiunii pot fi diverse: aviditate, răzbunare, invidie, huliganism, interes

---

[1683] BOȚIAN, Elisabeta. Mobilul și scopul. De la concepte filosofice la noțiuni ale dreptului penal. În: *Acta Universitatis Lucian Blaga*, 2021, nr. 1, pp. 107-120. ISSN 1582-4608.
[1684] COPEȚCHI, Stanislav. Semnele secundare ale laturii subiective: aspecte teoretico-practice şi legislative. În: *Conferinţa ştiinţifică naţională cu participare internaţională „Infracţiunea – Răspunderea penală – Pedeapsa. Drept şi Criminologie” (25-26 martie 2021, Chişinău)*. Chişinău: CEP USM, 2021, pp. 76-85. ISBN 978-9975-158-12-1.
[1685] Ibidem.
[1686] *Codul penal al Republicii Cipriote*. [citat 11.07.2022] Disponibil: https://codexpenal.just.ro/laws/Cod-Penal-Cipru-RO.html
[1687] Ibidem.
[1688] CAZACICOV, Andrei. Latura subiectivă a infracţiunii de creare sau conducere a unei organizaţii criminale. În: *Revista Naţională de Drept*, 2021, nr. 2, pp. 118-127. ISSN 1811-0770.
[1689] Ibidem.
[1690] Ibidem.
[1691] Ibidem.

„sportiv", dorinţa de a strica reputaţia de afaceri a concurentului etc.”[1692]; „Cele menţionate nu sunt caracteristici obligatorii ale componenţei de infracţiune examinate, dar sunt luate în considerare la stabilirea pedepsei”.[1693] În primul rând, acest autor confundă cauzele infracțiunii cu motivul infracțiunii. În al doilea rând, printre exemplele prezentate de V. Soltan, nu se numără niciunul care se referă la scopul infracțiunii.

Până nu demult, am fi fost de acord cu V. Soltan că motivul infracțiunii nu are un impact asupra calificării faptei în baza art. 259 CP RM, însă poate fi luat în vedere în procesul de individualizare a pedepsei. Odată cu intrarea în vigoare a Legii nr. 111 din 21.04.2022 pentru modificarea unor acte normative[1694], lucrurile s-au schimbat. Prin această lege, alin. (2) art. 259 CP RM a fost completat cu lit. g^1) „din motive de prejudecată”. Deoarece acest motiv special îndeplinește și rolul de circumstanță agravantă, îl vom analiza *infra*, în contextul examinării unor astfel de circumstanțe. Pe planul dreptului comparat, trebuie de menționat că, în alin. 2 art. 272 CP FR, ca motiv special cu efect agravant este menționat interesul material.[1695]

Bineînțeles, motivul infracțiunii este prezent și în alte cazuri decât cel prevăzut la lit. g^1) alin. (2) art. 259 CP RM. În doctrina penală autohtonă sunt specificate următoarele motive din această categorie: „aviditate, răzbunare, invidie, huliganism, interes „sportiv”, dorinţa de a strica reputaţia de afaceri a concurentului etc.”[1696]; „interesul „sportiv”; motive huliganice; răzbunare; interesul material, etc.”[1697]; interesul material, interesul personal, interesul „sportiv”, curiozitate etc.[1698]; interesul „sportiv”, interesul material, răzbunare, gelozie etc.[1699] La această listă pot fi adăugate motivele relevate de A.C. Moise: amuzament; supărare; furie; motive politice.[1700] Astfel de motive nu sunt speciale. Deci, ele nu au un impact asupra calificării faptei în baza art. 259 CP RM.

[1692] SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261[1] Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf

[1693] Ibidem.

[1694] Legea pentru modificarea unor acte normative: nr. 111 din 21.04.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 164-169, 291.

[1695] Уголовный кодекс Российской Федерации. În: *Собрание законодательства Российской Федерации*, 1996, № 25.

[1696] SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261[1] Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf

[1697] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 355. 1300 p. ISBN 978-9975-53-470-3.

[1698] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 19. 592 с. ISBN 978-9975-4158-2-8.

[1699] ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista ştiinţifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.

[1700] MOISE, Adrian Cristian. Infractorii și victimele în cyberspatiu. În: *Curierul Judiciar*, 2016, nr. 9, pp. 475-481. ISSN 1582-7526.

În cele ce urmează, obiectul analizei îl va reprezenta scopul infracțiunilor prevăzute la art. 259 CP RM.

În articolele din unele legi penale străine, care sunt similare cu art. 259 CP RM, este menționat scopul special al infracțiunii: „scopul obținerii de date informatice”[1701] (alin. (2) art. 360 CPR); „pentru crearea unei semnături electronice”[1702] (alin. (3) art. 319a CP RBu); „scopul obţinerii unui folos patrimonial”[1703] (alin. (3) art. 319b CP RBu); „a) cu intenţia de a produce prejudicii altcuiva sau de a câştiga foloase ilegale pentru sine sau alţii”[1704], „sau b) cu intenţia de a limita funcţionalitatea unui sistem informatic sau a altui echipament tehnic de prelucrare a datelor, fără a fi autorizată”[1705] (alin. (2) secț. 230 CP RCe); „scopul de a obţine informaţii despre secretele comerciale ale unei societăţi”[1706] (art. 263 CP RD); „scopul obţinerii accesului ilicit la date cu caracter personal, secrete private, secrete comerciale sau secrete profesionale”[1707] (alin. (1) secț. 422 CPUn); „intenţia de a stabili identitatea oricărei persoane care cooperează, în secret”[1708], „cu autoritatea de urmărire penală sau cu autorităţile de aplicare a legii sau cu serviciul secret”[1709] (alin. (2) secț. 422 CPUn), etc.

Un asemenea scop este indicat, de asemenea, în art. 259 CP RM. Astfel, la lit. f) alin. (2) din acest articol este indicat „scopul săvârşirii uneia dintre infracţiunile prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6”.[1710] Deoarece acest scop special îndeplinește și rolul de circumstanță agravantă, îl vom analiza *infra*, în contextul examinării unor astfel de circumstanțe.

Fără îndoială, scopul infracțiunii este prezent și în alte cazuri decât cel prevăzut la lit. f) alin. (2) art. 259 CP RM. Despre unul dintre asemenea scopuri ne vorbește P. Tamas-Erno: „Accesul ilegal la sisteme informatice, în majoritatea cazurilor nu reprezintă finalul acțiunii ilegale săvârșite de făptuitor”[1711], „ci mai degrabă reprezintă primul pas spre comiterea de infracțiuni suplimentare”.[1712] În mod similar, L. Gîrla și Iu. Tabarcea menționează „scopul săvârșirii unei

---

[1701] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[1702] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[1703] Ibidem.
[1704] *Codul penal al Republicii Cehe*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Cehia-RO.html
[1705] Ibidem.
[1706] *Codul penal al Regatului Danemarcei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Danemarca-RO.html
[1707] *Codul penal al Ungariei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Ungaria-RO.html
[1708] Ibidem.
[1709] Ibidem.
[1710] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1711] TAMAS-ERNO, Peter. Accesarea ilegală a conturilor de Facebook privit din perspectiva dreptului penal. În: *Revista Facultății de Drept Oradea*, 2019, nr. 1, pp. 151-157. ISSN 1582-7585.
[1712] Ibidem.

alte infracțiuni”.[1713] S. Crijanovschi evidențiază scopul de obţinere de date informatice.[1714] În același context, în art. 2 din Convenția de la Budapesta se folosește sintagma „intenţia de a obţine date informatice ori [...] altă intenţie delictuală”.[1715]

În încheierea analizei laturii subiective a infracțiunilor prevăzute la art. 259 CP RM, este necesar să ne referim la emoții. Astfel, starea de afect demonstrează responsabilitatea redusă a făptuitorului. Argumente în susținerea acestei idei sunt aduse de I. Slisarenco[1716] și R. Berdilo.[1717] În conformitate cu lit. d) alin. (1) art. 76 CP RM, săvârşirea faptei de o persoană cu responsabilitate redusă se consideră circumstanță atenuantă care se ia în calcul la stabilirea pedepsei. Anume în această postură, starea de afect poate fi luată în considerare la individualizarea pedepsei care se aplică pentru infracțiunile prevăzute la art. 259 CP RM.

2.4. Subiectul infracțiunilor prevăzute la art. 259 CP RM

Conform părerii lui V. Grosu, „subiect al infracţiunii este recunoscută persoana care a comis o faptă prevăzută de legea penală”[1718] „și care, graţie faptului că posedă toate semnele prevăzute de lege pentru această categorie de subiect, este pasibilă de răspundere penală”.[1719]

Într-adevăr, „în dreptul penal al Republicii Moldova prin „subiect al infracțiunii” se are în vedere doar persoana care comite infracțiunea, nu și persoana asupra căreia se comite infracțiunea.”[1720] Or, în art. 21 CP RM, prin „subiect al infracțiunii” se are în vedere doar persoana care săvârșește infracțiunea. Aceeași idee rezultă implicit din alin. (6) art. 42 CP RM: „Participanţii trebuie să întrunească semnele subiectului infracţiunii.”[1721]

Din interpretarea dispozițiilor alin. (1) și (2) art. 21 CP RM, reiese că subiect al infracţiunilor prevăzute la art. 259 CP RM este acea „persoană fizică responsabilă care în momentul săvârșirii

---

[1713] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 19. 592 с. ISBN 978-9975-4158-2-8.
[1714] CRIJANOVSCHI, Sergiu. Accesul ilegal la informația computerizată în practica judiciară a Republicii Moldova și a României. În: *Conferința „Integrare prin cercetare și inovare” (Chișinău, Moldova, 28-29 septembrie). Vol. 1*. Chișinău: CEP USM, 2016, pp. 250-253. ISBN 978-9975-71-815-8.
[1715] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[1716] SLISARENCO, Ion. Conceptul omorului săvârșit în stare de afect. În: *Anale ştiinţifice ale Academiei „Ştefan cel Mare” a MAIRM: ştiinţe juridice*, 2016, nr. XVI, pp. 100-103. ISSN 1857-0976.
[1717] BERDILO, Rodica. Responsabilitatea redusă și starea emoțională a subiectului infracțiunilor prevăzute la art. 146, 147 și 156 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 3, pp. 150-159. ISSN 1814-3199.
[1718] GRAMA, Mariana, BOTNARU, Stela, ȘAVGA, Alina, GROSU, Vladimir. *Drept penal. Partea generală. Vol. I*. Chișinău: Tipografia Centrală, 2012, p. 207. 328 p. ISBN 978-9975-53-080-4.
[1719] Ibidem, p. 207.
[1720] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.
[1721] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

infracţiunii a atins vârsta de 16 ani."[1722] Din interpretarea sancțiunilor din alin. (1) și (2) art. 259 CP RM, precum și a dispoziției de la alin. (4) art. 21 CP RM, deducem că subiect al infracţiunilor analizate poate fi, de asemenea, persoana juridică, cu excepţia autorităţii publice. O astfel de interpretare este susținută cvasiunanim în doctrina de specialitate din țara noastră.[1723]

2.4.1. Persoana fizică – subiect al infracțiunilor prevăzute la art. 259 CP RM

Condiția privitoare la vârsta minimă a subiectului infracțiunii derivă din alin. 3 art. 40 din Convenția ONU cu privire la drepturile copilului: „Statele părţi se vor strădui să promoveze adoptarea de legi şi proceduri, înfiinţarea de autorităţi şi instituţii, special concepute pentru copiii bănuiţi"[1724], „acuzaţi sau găsiţi vinovaţi de încălcarea legii penale şi, în special"[1725]: „a) să stabilească o vârstă minimă sub care copiii să fie prezumaţi ca neavând capacitatea de a încălca legea penală; [...]."[1726] Legiuitorul moldovean nu a stabilit vârsta de 14 ca vârstă minimă a răspunderii penale în cazul infracţiunilor prevăzute la art. 259 CP RM. Prin aceasta se recunoaște implicit că minorul cu vârsta între 14 și 16 ani nu are capacitate suficientă pentru a percepe gradul și caracterul pericolului social al faptelor incriminate în acest articol.

În doctrina penală a fost exprimată opinia, potrivit căreia „vârsta de la care survine răspunderea penală în Republica Moldova ar trebui micșorată de legiuitor cu cel puțin 1 an"[1727], „deoarece progresul tehnic din ziua de astăzi, accesul pe larg la resursele media, televiziune, la spațiul online"[1728] „face posibil ca minorii să cunoască încă de la o vârstă fragedă ce este bine și ce este rău, ce este permis și ce este interzis".[1729] Același autor afirmă: „Vârsta minimă de la care persoana devine subiect al infracțiunii diferă mult de la ţară la ţară și variază ([...] 14 ani –

[1722] Ibidem.

[1723] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 355. 1300 p. ISBN 978-9975-53-470-3; BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009, p. 568. 860 p. ISBN 978-9975-105-20-0; BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003, p. 570. 836 p. ISBN 9975-61-291-1; ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 19-20. 592 с. ISBN 978-9975-4158-2-8; ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista ştiinţifică a USM „Studia Universitatis". Seria „Ştiinţe sociale"*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081; SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261[1] Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf

[1724] *United Nations Convention on the Rights of the Child*. [citat 06.03.2022] Disponibil: https://www.unicef.org/child-rights-convention/convention-text#

[1725] Ibidem.

[1726] Ibidem.

[1727] MIHALAȘ, Ion. Vârsta – condiție a răspunderii penale. Aspecte comparative cu legislația altor state. În: *Sesiune naţională de comunicări ştiinţifice studenţeşti: Ştiinţe sociale. Ştiinţe juridice şi economice (4-5 mai 2017, Chişinău)*. Chişinău: CEP USM, 2017, pp. 18-20.

[1728] Ibidem.

[1729] Ibidem.

Germania [...])”[1730], (15 ani – în Suedia, Danemarca și Polonia), (16 ani – SUA, 14 ani – Japonia, [...] 15 ani – Finlanda [...]).[1731] Cu siguranță, în statele sus-menționate, minorii au un acces mai facil la resursele pe care le implică progresul tehnico-științific. Însă, legiuitorii din aceste state nu se grăbesc să reducă vârsta minimă a răspunderii penale. Considerăm că o astfel de abordare cumpătată ar trebui să fie urmată de către legiuitorul moldovean. Aplicarea mijloacelor nepenale de influențare este preferabilă în orice societate în care minorul este privit ca personalitate în dezvoltare, care are șanse de a se corecta fără a fi supus represiunii penale.

Cu privire la noțiunea de responsabilitate, S. Botnaru explică: „Responsabilitatea se apreciază prin prisma a doi factori: unul intelectiv, ce constă în capacitatea persoanei de a-şi da seama de acţiunile sau inacţiunile sale”[1732], „de semnificaţia lor socială şi de urmările acestora şi unul volitiv, constând în aptitudinea aceleiaşi persoane de a fi stăpână pe faptele sale”[1733], „în sensul că le putea dirija în mod conştient. Ambii factori sunt necesari şi decisivi în stabilirea responsabilităţii”[1734]; „Prin urmare, putem conchide că starea de responsabilitate este starea psihofizică normală a individului”[1735], „pe când iresponsabilitatea constituie o stare psihofizică anormală, reprezentând, de fapt, o stare de excepţie.”[1736]

La rândul lor, A. Mariț și M. Șomicu (Banu) menționează: „O persoană iresponsabilă nu înţelege de ce acţiunile sau inacţiunile sale prezintă pericol social şi de ce acestea au caracter ilicit”[1737]; „O asemenea persoană nu este pedepsită, căci n-ar putea fi îndreptată prin aplicarea şi executarea pedepsei”[1738]; „Caracteristica stării de iresponsabilitate este deci lipsa acestor facultăţi psihice ale persoanei”[1739], „care permit acesteia să înţeleagă caracterul şi semnificaţia actelor sale de conduită sau să fie stăpână pe ele”.[1740] Această opinie o confirmă dispoziția din alin. (1) art. 23 CP RM, din care rezultă că iresponsabilă trebuie considerată acea persoană căreia îi lipsesc oricare dintre cele două capacități menționate *supra*, ce caracterizează starea de responsabilitate:

a) capacitatea de a percepe caracterul prejudiciabil al faptei *sau*

b) capacitatea de a-şi manifesta voinţa, precum şi de a-şi dirija acţiunile.

[1730] Ibidem.
[1731] Ibidem.
[1732] BOTNARU, Stela. *Iresponsabilitatea – cauză care înlătură vinovăţia făptuitorului: definitivarea conceptului*. În: *Revista Naţională de Drept*, 2014, nr. 2, pp. 33-37. ISSN 1811-0770.
[1733] Ibidem.
[1734] Ibidem.
[1735] Ibidem.
[1736] Ibidem.
[1737] MARIȚ, Alexandru, ȘOMICU (BANU), Marcela. Responsabilitatea și iresponsabilitatea, responsabilitatea redusă în dreptul penal. În: *Vector European*, 2014, nr. 2, pp. 106-111. ISSN 2345-1106.
[1738] Ibidem.
[1739] Ibidem.
[1740] Ibidem.

2.4.2. Persoana juridică – subiect al infracțiunilor prevăzute la art. 259 CP RM

Nu oricare persoană juridică poate avea calitatea de subiect al infracțiunii. În alin. (4) art. 21 CP RM este stabilită condiția negativă pe care trebuie s-o posede subiectul - persoană juridică: să nu aibă calitatea de autoritate publică. În principiu, toate autoritățile publice sunt specificate în Titlul III al Constituției Republicii Moldova.[1741] O listă a autorităților publice a fost prevăzută în Anexa nr. 1 la Hotărârea Guvernului nr. 1001 din 26.12.2011 privind punerea în aplicare a unor acte legislative.[1742] Însă, acest act normativ a fost abrogat prin Hotărârea Guvernului nr. 942 din 28.12.2022 pentru modificarea unor hotărâri ale Guvernului (privind funcția publică și statutul funcționarului public).[1743]

Necesitatea de a supune subiectul - persoană juridică răspunderii penale pentru infracţiunile, prevăzute la art. 259 CP RM, rezultă din anumite acte internaționale.

În primul rând, se are în vedere Directiva 2013/40/UE. La lit. c) art. 2 din acest act este definită noțiunea „persoană juridică": „entitate care are statutul de persoană juridică în conformitate cu legislația aplicabilă"[1744], „dar nu include statele sau alte organisme publice aflate în exercițiul autorității de stat și organizațiile internaționale de drept public".[1745]

Așadar, sub incidența acestei definiții nu intră statul, autoritățile publice și organizațiile internaționale de drept public.

În art. 10 al Directivei 2013/40/UE sunt stabilite condițiile în care persoanele juridice devin pasibile de răspundere penală. În linii mari, aceste condiții sunt similare cu cele din alin. (3) și (3^1) art. 21 CP RM:

„(1) Statele membre iau măsurile necesare pentru a garanta angajarea răspunderii persoanelor juridice pentru oricare dintre infracțiunile prevăzute la articolele 3-8"[1746], „săvârșite în beneficiul lor de către orice persoană, acționând fie în nume propriu"[1747], „fie ca parte a unui organism al persoanei juridice și având o funcție de conducere în cadrul persoanei juridice"[1748], „în temeiul:

[1741] Constituția Republicii Moldova. În: *Monitorul Oficial al Republicii Moldova*, 1994, nr. 1, 140.
[1742] Hotărârea Guvernului privind punerea în aplicare a unor acte legislative: nr. 1001 din 26.12.2011. În: *Monitorul Oficial al Republicii Moldova*, 2011, nr. 238-242, 1100.
[1743] Hotărârea Guvernului pentru modificarea unor hotărâri ale Guvernului (privind funcția publică și statutul funcționarului public): nr. 942 din 28.12.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 460-462, 1072.
[1744] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en
[1745] Ibidem.
[1746] Ibidem.
[1747] Ibidem.
[1748] Ibidem.

(a) unei împuterniciri din partea persoanei juridice; (b) unei prerogative de a lua decizii în numele persoanei juridice”[1749]; „(c) unei prerogative de a exercita controlul în cadrul persoanei juridice”[1750];

„(2) Statele membre adoptă măsurile necesare pentru a garanta angajarea răspunderii persoanelor juridice în cazul în care nesupravegherea sau neexercitarea controlului”[1751], „imputabile unei persoane menționate la alineatul (1), a permis săvârșirea, de către o persoană aflată în subordine”[1752], „a oricăreia dintre infracțiunile menționate la articolele 3-8, în beneficiul acelei persoane juridice.”[1753]

În fine, alin. (3) art. 10 al Directivei 2013/40/UE prezintă vădite similitudini cu alin. (5) art. 21 CP RM: „Răspunderea persoanelor juridice în temeiul alineatelor (1) și (2) nu exclude procedurile penale îndreptate împotriva persoanelor fizice care sunt autori, instigatori sau complici la oricare dintre infracțiunile prevăzute la articolele 3-8”.[1754]

În al doilea rând, se are în vedere Convenția de la Budapesta. Această Convenție nu conține definiția noțiunii de persoană juridică. În celelalte privințe, dispozițiile privind răspunderea penală a persoanei juridice din Convenția de la Budapesta se aseamănă cu dispozițiile corespunzătoare din Directiva 2013/40/UE.

Astfel, art. 12 al Convenției de la Budapesta prevede:

„1. Fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru ca persoanele juridice să poată fi trase la răspundere”[1755] „pentru infracţiunile stabilite în aplicarea prezentei convenţii, atunci când acestea sunt comise pe cont propriu de către orice persoană fizică care acţionează fie individual”[1756], „fie în calitate de membru al unui organ al persoanei juridice, care exercită o funcţie de conducere în cadrul acesteia, având la bază”[1757]: „a) o calitate de reprezentare a persoanei juridice”[1758]; „b) puterea de luare a deciziilor în numele persoanei juridice; c) puterea de a exercita controlul în cadrul persoanei juridice”[1759];

„2. Cu excepţia cazurilor deja prevăzute la paragraful 1 al prezentului articol, fiecare parte va adopta măsurile care se dovedesc necesare”[1760] „pentru a se asigura că o persoană juridică poate

[1749] Ibidem.
[1750] Ibidem.
[1751] Ibidem.
[1752] Ibidem.
[1753] Ibidem.
[1754] Ibidem.
[1755] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[1756] Ibidem.
[1757] Ibidem.
[1758] Ibidem.
[1759] Ibidem.
[1760] Ibidem.

fi trasă la răspundere atunci când absenţa supravegherii sau a controlului”[1761] „din partea persoanei fizice menţionate la paragraful 1 a permis comiterea infracţiunilor stabilite în aplicarea prezentei convenţii”[1762] „pentru numita persoană juridică de către o persoană fizică care acţionează sub autoritatea acesteia”[1763];

„3. În funcţie de principiile juridice ale părţii, răspunderea unei persoane juridice poate fi penală, civilă sau administrativă”[1764];

„4. Această răspundere va fi stabilită fără a prejudicia răspunderea penală a persoanelor fizice care au comis infracţiunea.”[1765]

Interpretarea art. 12 al Convenției de la Budapesta este înlesnită de Raportul explicativ la această Convenție. Rețin atenția următoarele pasaje din Raportul explicativ la Convenția de la Budapesta:

„123. Articolul 12 [...] este destinat să impună răspunderea corporațiilor, asociațiilor și persoanelor juridice similare pentru acțiunile penale”[1766] „întreprinse de o persoană care ocupă o poziție de conducere în cadrul acestei persoane juridice, atunci când sunt întreprinse în beneficiul acelei persoane juridice”[1767];

„124. [...] Noțiunea „persoană care ocupă o poziție de conducere” se referă la o persoană fizică care deține o poziție înaltă în organizație, cum ar fi un director. [...]”[1768];

„125. În plus, paragraful 2 obligă părțile să aibă capacitatea de a impune răspunderea unei persoane juridice în cazul în care infracțiunea”[1769] „este săvârșită nu de persoana principală descrisă la paragraful 1, ci de o altă persoană care acționează sub autoritatea persoanei juridice”[1770], „adică una dintre angajații sau agenții săi care acționează în sfera autorității lor. [...]”[1771];

„127. Paragraful 4 clarifică faptul că răspunderea corporativă nu exclude răspunderea individuală.”[1772]

Trebuie de menționat că nu doar legiuitorul moldovean s-a inspirat din prevederile lit. c) art. 2 și ale art. 10 al Directivei 2013/40/UE, precum și ale art. 12 al Convenției de la Budapesta. De

---

[1761] Ibidem.
[1762] Ibidem.
[1763] Ibidem.
[1764] Ibidem.
[1765] Ibidem.
[1766] *Explanatory Report to the Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/16800cce5b
[1767] Ibidem.
[1768] Ibidem.
[1769] Ibidem.
[1770] Ibidem.
[1771] Ibidem.
[1772] Ibidem.

exemplu, conform alin. (3) § 217 CP RE („Accesul ilegal la un sistem informatic"), „faptele prevăzute la alineatul (1) sau (2) din acest articol, dacă sunt săvârşite de o persoană juridică, se pedepsesc cu amendă".[1773] Potrivit alin. 3 art. 198(1) „Conectarea ilicită la un sistem informatic" din Codul penal al Republicii Lituania, „persoana juridică răspunde penal pentru faptele prevăzute în prezentul articol".[1774] Nu în ultimul rând, alin. 4 art. 264 CP RSp prevede: „[...] o persoană juridică este responsabilă de infracţiunile incluse în acest articol [...]."[1775] Pe de altă parte, în legile penale ale altor state se promovează ideea că doar persoana fizică trebuie să răspundă pentru infracțiunile similare cu cele prevăzute la art. 259 CP RM.

2.4.3. Calitatea specială a subiectului infracțiunilor prevăzute la art. 259 CP RM

În viziunea lui S. Brînza și V. Stati, „numai persoana care nu este autorizată în temeiul legii sau al unui contract, care depăşeşte limitele autorizării"[1776] „ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic"[1777] „ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic, poate fi subiectul infracţiunii specificate la alin. (1) art. 259 CP RM."[1778]

O părere apropiată o exprimă L. Gîrla și Iu. Tabarcea: „În legea penală se indică statutul special al subiectului infracţiunilor analizate"[1779]; „În sensul legii, este considerat a fi un astfel de subiect: persoana care nu este autorizată în temeiul legii sau al unui contract"[1780]; „persoana care depăşeşte limitele autorizării"[1781]; „persoana care nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic"[1782] „ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic."[1783]

Acești autori își formulează opinia, bazându-se pe sintagma „al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are

---

[1773] *Codul penal al Republicii Estonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Estonia-RO.html
[1774] *Codul penal al Republicii Lituania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Lituania-RO.html
[1775] *Codul penal al Regatului Spaniei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Spania-RO.html
[1776] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 355. 1300 p. ISBN 978-9975-53-470-3.
[1777] Ibidem, p. 355.
[1778] Ibidem, p. 355.
[1779] ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010, с. 19. 592 с. ISBN 978-9975-4158-2-8.
[1780] Ibidem, с. 19.
[1781] Ibidem, с. 19.
[1782] Ibidem, с. 19-20.
[1783] Ibidem, с. 20.

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", care este folosită în art. 259 CP RM.

Calitatea specială a subiectului infracțiunilor, prevăzute la art. 259 CP RM, poate fi lesne stabilită prin raportare la analiza acestei sintagme.

L. Gîrla și Iu. Tabarcea menționează: „Cel mai adesea, astfel de infracțiuni (adică infracțiunile prevăzute la art. 259 CP RM – *n.a.*) sunt comise de persoane care au acces la un calculator"[1784], „la un sistem informatic sau la o rețea informatică"[1785]; „La astfel de persoane se raportează cele ale căror activități profesionale sunt legate de asigurarea funcționării unui sistem informatic"[1786] „sau al unei rețele informatice (programatori, operatori de calculatoare, reglatori de echipamente etc.)."[1787]

Această opinie ar trebui completată: din art. 259 CP RM rezultă că informația computerizată, accesată ilegal, se poate afla nu doar într-un un calculator, într-un un sistem informatic sau într-o rețea informatică, ci și pe un suport material de informaţie. Totodată, accentuăm că autorii precitați se referă, în mod întemeiat, la persoanele care *au dreptul de acces* anume la un calculator, la un suport material de informaţie, la un sistem informatic sau la o rețea informatică. În același timp, trebuie să subliniem că asemenea persoane *nu trebuie să aibă dreptul de acces* la informația computerizată din calculatorul, de pe suportul material de informaţie, din sistemul informatic sau din reţeaua informatică la care au acces legal.

L. Gîrla și Iu. Tabarcea utilizează expresia „cel mai adesea". Totuși, este dificil de stabilit care anume este proporția persoanelor, care au drept de acces la un calculator, la un suport material de informaţie, la un sistem informatic sau la o rețea informatică, în ansamblul persoanelor care au calitatea de subiecți ai infracțiunilor prevăzute de art. 259 CP RM. În afară de persoanele, care au drept de acces la un calculator, la un suport material de informaţie, la un sistem informatic sau la o rețea informatică, subiecți ai acestor infracțiuni pot fi, de asemenea, persoanele care nu au un asemenea drept. Desigur, astfel de persoane nu au nici drept de acces la informația computerizată.

În legile penale ale anumitor state, în articolele care sunt similare cu art. 259 CP RM, poate fi identificată circumstanța agravantă „cu folosirea situației de serviciu". De exemplu, pct. 1) art. 615-ter „Acces abuziv la un sistem informatic sau de telecomunicaţii" prevede: „dacă fapta este

[1784] Ibidem, c. 20.
[1785] Ibidem, c. 20.
[1786] Ibidem, c. 20.
[1787] Ibidem, c. 20.

comisă de un funcţionar public sau de un însărcinat cu o funcţie publică”[1788], „prin abuz de putere sau prin încălcarea îndatoririlor legate de funcţie sau de serviciu”[1789] „sau de cel care practică fie şi abuziv profesia de detectiv particular sau prin abuz de calitatea de operator de sistem”.[1790] De asemenea, alin. 3 art. 272 CP FR („Accesul ilegal la informația computerizată”) se referă, printre altele, la „persoana care-și folosește situația de serviciu”.[1791]

O eventuală completare a art. 259 CP RM cu o dispoziție, în care ar fi stabilită circumstanța agravantă „cu folosirea situației de serviciu”, ar putea genera riscul de aplicare atât a acestei dispoziții, cât și a art. 327, 335 sau 370 CP RM sau a art. 312 CC RM. Ceea, ce ar veni în contradicție cu art. 118 CP RM, care acordă prioritate normei - întreg, nu normei - parte.

2.5. Circumstanțele agravante ale infracțiunilor prevăzute la art. 259 CP RM

În art. 259 CP RM este prevăzută răspunderea pentru două infracțiuni. Așa cum menționează pe bună dreptate S. Brînza și V. Stati, „sub denumirea marginală de acces ilegal la informaţia computerizată, în art. 259 CP RM”[1792], „sunt reunite două variante-tip de infracțiuni și o singură variantă agravată de infracțiune”.[1793] Aceiași autori argumentează: „La alin. (1) și lit. h) alin. (2) art. 259 CP RM, sunt prevăzute două infracțiuni de sine stătătoare. [...]”[1794]; „Explicația faptului că art. 259 CP RM stabilește răspunderea pentru două infracțiuni de sine stătătoare”[1795] „constă în următoarele: nu există o componență „de bază” de acces ilegal la informaţia computerizată, componență”[1796] „care: 1) nu ar presupune producerea unor daune având o mărime concretă și 2) pe care s-ar grefa în calitate de circumstanțe agravante”[1797]: „a) producerea unor daune în proporţii mari; b) producerea unor daune în proporţii deosebit de mari” [1798]; „Iată de ce cauzarea de daune în proporţii deosebit de mari nu poate fi privită în calitate de circumstanță agravantă pentru infracțiunea prevăzută la alin. (1) art. 259 CP RM”[1799], „infracțiune care presupune

---

[1788] *Codul penal al Republicii Italia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Italia-RO.html
[1789] Ibidem.
[1790] Ibidem.
[1791] Уголовный кодекс Российской Федерации. În: *Собрание законодательства Российской Федерации*, 1996, № 25.
[1792] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 346. 1300 p. ISBN 978-9975-53-470-3.
[1793] Ibidem, p. 346.
[1794] Ibidem, p. 346.
[1795] Ibidem, p. 346.
[1796] Ibidem, p. 346.
[1797] Ibidem, p. 346.
[1798] Ibidem, p. 346.
[1799] Ibidem, p. 346.

producerea unor daune în proporții mari”[1800]; „În alți termeni, cauzarea de daune în proporții deosebit de mari nu poate fi privită ca apendice, ca adaos”[1801], „ca supliment, ca anexă la componența de infracțiune specificată la alin. (1) art. 259 CP RM, care deja presupune cauzarea de daune în proporții mari”.[1802]

Respectiv, la lit. b)-g) și g^1) alin. (2) art. 259 CP RM, sunt specificate circumstanțele agravante ale infracțiunilor reunite sub denumirea marginală de acces ilegal la informaţia computerizată. La concret, este vorba despre următoarele circumstanțe agravante:

– de două sau mai multe persoane (lit. b) alin. (2) art. 259 CP RM);

– cu violarea sistemelor de protecţie (lit. c) alin. (2) art. 259 CP RM);

– cu conectarea la canalele de telecomunicaţii (lit. d) alin. (2) art. 259 CP RM);

– cu folosirea unor mijloace tehnice speciale (lit. e) alin. (2) art. 259 CP RM);

– cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice, în scopul săvârşirii uneia dintre infracţiunile prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6 (lit. f) alin. (2) art. 259 CP RM);

– în privinţa informaţiei protejate de lege (lit. g) alin. (2) art. 259 CP RM);

– din motive de prejudecată (lit. g^1) alin. (2) art. 259 CP RM).

În continuare, aceste circumstanțe agravante vor fi examinate în aceeași ordine.

2.5.1. Săvârșirea infracțiunii de două sau mai multe persoane

În legile penale ale unor state, în articolele care sunt corespondente cu art. 259 CP RM, pot fi identificate circumstanțe agravante similare. Spre exemplu, potrivit alin. (4) § 118a CP RA, „persoana care săvârşeşte fapta prevăzută la alin. (1)[1803] în cadrul unui grup infracţional se

---

[1800] Ibidem, p. 346.
[1801] Ibidem, p. 346.
[1802] Ibidem, p. 346.
[1803] Acest alineat prevede: „Fapta persoanei care își creează acces la un sistem informatic sau la o parte a unui sistem informatic”* „în legătură cu care nu este autorizată sau este autorizată doar împreună cu o altă persoană, prin depăşirea unui dispozitiv de securitate specific”* „din interiorul sistemului informatic, cu intenţia: 1. de a cunoaşte sau de a facilita unei alte persoane neautorizate accesul la date cu caracter personal”*, „cunoaştere care lezează interese confidenţiale protejate ale persoanei vătămate”* „sau 2. de a produce un dezavantaj unei alte persoane prin utilizarea datelor salvate în sistem”* „și care nu îi sunt destinate și la care își creează acces sau prin utilizarea sistemului informatic”*, „se pedepseşte cu închisoare de până la 6 luni sau cu amendă de până la 360 de zile-amendă”.*
* *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html

pedepseşte cu închisoare de până la 2 ani”[1804], „iar persoana care săvârşeşte fapta prevăzută la alin. (2)[1805] în cadrul unui grup infracţional se pedepseşte cu închisoare de până la 3 ani”.[1806]

Nu este clar dacă două ori mai multe persoane, ce săvârșesc infracțiunea ce este prevăzută de lit. b) alin. (2) art. 259 CP RM, trebuie să posede calitatea de coautori sau nu. De aceea, în contextul examinării circumstanței agravante prevăzute la lit. b) alin. (2) art. 259 CP RM, este necesar să facem o comparație între ipoteza, în care o infracțiune este săvârșită de către două ori mai multe persoane care posedă calitatea de subiecți speciali, și ipoteza în care o infracțiune este săvârșită de către două ori mai multe persoane ce nu posedă calitatea de subiecți speciali.

În legătură cu ipoteza în care o infracțiune este săvârșită de către două ori mai multe persoane care nu posedă calitatea de subiecți speciali, considerăm potrivit să reproducem următoarea părere a lui C. Brînza: „Darea de mită (art. 334 CP RM) este săvârșită de un subiect general. Din cauza lipsei calității speciale a subiectului”[1807], „darea de mită săvârșită de două sau mai multe persoane (lit. b) alin. (2) art. 334 CP RM) presupune oricare din următoarele trei ipoteze”[1808]: „1) darea de mită săvârșită de doi sau mai mulți coautori”[1809]; „2) darea de mită săvârșită de o persoană care are semnele subiectului infracțiunii împreună cu o persoană care nu este pasibilă de răspundere penală [...]”[1810]; „3) darea de mită săvârșită de o persoană care are semnele subiectului infracțiunii prin intermediul unei persoane care nu este pasibilă de răspundere penală [...].”[1811] În legătură cu ipoteza în care o infracțiune este săvârșită de către două ori mai multe persoane care posedă calitatea de subiecți speciali, C. Brînza menționează: „În ce privește luarea de mită (art. 333 CP RM), aceasta este săvârșită de un subiect special”[1812] – „arbitru ales sau numit să soluţioneze prin arbitraj un litigiu; persoană care gestionează o organizaţie comercială, obştească ori o altă organizaţie nestatală”[1813]; „persoană care lucrează pentru o organizaţie comercială, obştească ori o altă organizaţie nestatală; participant la un eveniment sportiv de pariat”[1814]; „Apare întrebarea dacă luarea de mită săvârșită de două sau mai multe persoane (lit.

[1804] *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html

[1805] Acest alineat prevede: „Persoana care săvârşeşte fapta în legătură cu un sistem informatic care este parte esenţială a infrastructurii critice”* „(§ 74 alin. 1 punctul 11) se pedepseşte cu închisoare de până la 2 ani”.*

* *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html

[1806] Ibidem.

[1807] BRÎNZA, Cristian. *Răspunderea penală pentru luarea de mită și darea de mită*: tz. de doct. în drept. Chișinău, 2021, p. 293. 351 p.

[1808] Ibidem, p. 293.

[1809] Ibidem, p. 293.

[1810] Ibidem, p. 293.

[1811] Ibidem, p. 293.

[1812] Ibidem, p. 293.

[1813] Ibidem, p. 293.

[1814] Ibidem, p. 293.

b) alin. (2) art. 333 CP RM)”[1815] „presupune sau nu ipoteza exclusivă a prezenței a cel puțin doi coautori care au cu toții calitatea specială sus-menționată”.[1816]

Răspunzând afirmativ la această întrebare, C. Brînza susține: „Infracțiunile prevăzute la art. 333 CP RM au nu pur și simplu un subiect special. Ele au o componență specială”[1817]; „Calitatea specială cerută de art. 333 CP RM face să fie speciale toate celelalte elemente constitutive ale luării de mită”[1818]; „Prin aceasta luarea de mită se deosebește de infracțiuni ca violul care are subiect special, dar nu are o componență specială”[1819]; „Persoanele, care nu au calitatea specială cerută de art. 333 CP RM, nu pot leza obiectul juridic al luării de mită”[1820], „nu pot realiza nemijlocit latura obiectivă a luării de mită, nu pot avea atitudinea psihică specifică luării de mită”.[1821]

În ceea ce privește infracțiunile prevăzute la art. 259 CP RM, considerăm că acestea au, de asemenea, o componență specială. De aceea, persoanele, care nu răspund penal datorită vârstei, iresponsabilității etc., nu se au în vedere în dispoziția de la lit. b) alin. (2) art. 259 CP RM.

În alt context, pentru aplicarea prevederii de la lit. b) alin. (2) art. 259 CP RM, nu este relevant dacă înțelegerea dintre două ori mai multe persoane, care comit infracțiunea, este prealabilă sau spontană. Caracterul unei asemenea înțelegeri poate fi luată în seamă poate doar la individualizarea pedepsei. Pentru comparație, conform alin. (2) art. 319a CP RBu[1822], este obligatorie prezența înțelegerii prealabile dintre cofăptuitori.

Printre circumstanțele agravante ale infracțiunilor, prevăzute la art. 259 CP RM, nu se numără săvârșirea acestor infracțiuni de către un grup criminal organizat. Însă, aceasta nu trebuie să ducă spre concluzia că respectivele infracțiuni nu pot fi comise de către un grup criminal organizat. În context este necesar să-l cităm pe O. Vară: „Criminalitatea organizată se serveşte de criminalitatea informatică, ceea ce nu reprezintă altceva decât un aspect ce nu surprinde”[1823], „„firesc”, având în vedere că domeniul informatic cuprinde atât de multe aspecte ale vieţii cotidiene a unei persoane”[1824]; „Chiar şi pentru reţelele de crimă organizată care au în vedere

[1815] Ibidem, p. 293.
[1816] Ibidem, p. 293.
[1817] Ibidem, p. 293.
[1818] Ibidem, p. 293.
[1819] Ibidem, p. 293.
[1820] Ibidem, p. 293.
[1821] Ibidem, p. 293.
[1822] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[1823] VARĂ, Octavian. Criminalitatea informatică şi criminalitatea organizată. Elemente de drept comparat. În: *Revista de Investigare a Criminalităţii*, 2014, nr. 1, pp. 101-104. ISSN 1844-7945.
[1824] Ibidem.

traficul de droguri ori de fiinţe umane, criminalitatea informatică”[1825] „poate să contribuie la desfăşurarea activităţii reţelelor prin furtul de date personale, falsificarea de date de identificare în vederea traficării victimelor”[1826] „ori facilitarea trecerii frontierelor prin eludarea atenţiei autorităţilor (emiterea de documente de călătorie false)”.[1827]

În legile penale ale anumitor state, în articolele ce corespund cu art. 259 CP RM, săvârșirea infracțiunii de către un grup criminal organizat se consideră circumstanță agravantă care are un impact asupra calificării (de exemplu, în pct. 1 alin. (5) art. 319b CP RBu[1828], la lit. a) alin. (4) secț. 230 CP RCe[1829], în pct. 1 alin. (1) secț. 8(a) din Capitolul 38 al CP RFi[1830] și la lit. b) alin. (4) § 247 CP RSl[1831]).

Prevederea de la lit. b) alin. (2) art. 259 CP RM a fost invocată la calificare în speța următoare: C.K., D.M. și D.V. au fost condamnați în baza art. 26, 46 și lit. c), d) alin. (2) art. 237, art. 46 și lit. b), e), h) alin. (2) art. 259 și art. 46 și 260 CP RM. În fapt, în luna iulie a anului 2014, C.K., A.B., D.M. și D.V. au participat la crearea unui grup criminal organizat în vederea comiterii mai multor infracţiuni informatice cu cauzarea de daune în proporţii deosebit de mari. La 11.07.2014, pentru a realiza această intenție, C.K., A.B., D.M. și D.V. au intrat pe teritoriul Republicii Moldova prin punctul de trecere a frontierei de stat „Giurgiulești – Galați”. Aceștia au importat ilegal mijlocul tehnic de tip „skimmer”, conceput şi adaptat în vederea săvârşirii infracţiunilor prevăzute la art. 237 și 259 CP RM. Urmărind culegerea informaţiilor de pe cardurile bancare autentice pentru a confecţiona carduri bancare false cu ajutorul cărora urmau a fi extrase ilegal surse bănești care aparțineau altor persoane, în perioada 13.07.2014 – 15.07.2014, cei patru făptuitori au instalat ilegal mijlocul tehnic de tip „skimmer” pe bancomatul ce aparţinea unei bănci comerciale, amplasat pe bd. Ştefan cel Mare şi Sfânt din mun. Chișinău. Pe această cale făptuitorii au accesat ilegal informaţia de pe cardurile bancare ale 158 de posesori de carduri bancare, pe care au copiat-o pe un dispozitiv de stocare a informaţiei. În continuare, la 15.07.2014, fiind în posesia datelor copiate ilegal, cei patru făptuitori au părăsit teritoriul Republicii Moldova prin punctul de trecere a frontierei de stat „Leușeni – Albița”. Apoi, în perioada 18.07.2014 – 21.07.2014, pe teritoriul Republicii Bulgaria, prin utilizarea datelor

[1825] Ibidem.
[1826] Ibidem.
[1827] Ibidem.
[1828] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[1829] *Codul penal al Republicii Cehe*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Cehia-RO.html
[1830] *Codul penal al Republicii Finlanda*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Finlanda-RO.html
[1831] *Codul penal al Republicii Slovace*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovacia-RO.html

informatice copiate ilegal ale celor 158 de posesori de carduri bancare, făptuitorii au extras ilegal bani în sumă totală de 122925,16 lei.[1832]

În această speță, cu toate că se vorbește despre săvârșirea infracțiunilor de un grup criminal organizat, iar la calificare se reține art. 46 CP RM, nu a fost prezentat vreun argument care ar demonstra prezența acestei forme de participație. Făcându-se abstracție de prevederile art. 46 CP RM, nu s-a argumentat că C.K., A.B., D.M. și D.V. au constituit „o reuniune stabilă de persoane care s-au organizat în prealabil pentru a comite una sau mai multe infracţiuni”.[1833] În această privință, suntem de acord cu D. Gurev care afirmă: „Simplul fapt al comiterii în comun a uneia sau mai multor infracţiuni, chiar dacă făptuitorii se întâlnesc în prealabil şi discută cum să procedeze”[1834], „determinând şi aportul fiecăruia, nu [presupune] săvârşirea infracţiunii de către un grup criminal organizat. În astfel de cazuri ne aflăm doar în prezenţa participaţiei simple sau complexe”[1835], „iar înţelegerea anterioară săvârşirii faptei dintre făptuitori, cu privire la locul, metoda, mijloacele de săvârşire a infracţiunii”[1836], „la contribuţia fiecăruia, încă nu semnifică că pluralitatea de făptuitori reprezintă un grup criminal organizat”[1837]; „Această înţelegere demonstrează intenţia făptuitorilor de a săvârşi infracţiunea – condiţie *sine qua non* a participaţiei penale”.[1838]

În opinia lui M. Grama, S. Botnaru, A. Șavga și D. Martin, „stabilitatea grupului [criminal organizat] este caracterizată de existenţa unor legături strânse permanente între membrii grupului”[1839] „și formele și metodele individuale, specifice ale activităţii acestuia. În practica judiciară, în calitate de indicatori ai stabilităţii se evidenţiază”[1840]: „a) gradul înalt de organizare [...]; b) stabilitatea activului de bază al grupului și structurii ei organizaţionale [...]”[1841]; „c) existenţa unor metode și forme de activitate individuale după caracterul lor [...]; d) stabilitatea (constanţa) formelor și metodelor activităţii criminale.”[1842] Păreri asemănătoare au I.

[1832] *Decizia Colegiului penal al Curții de Apel Chișinău din 15.06.2015. Dosarul nr. 1a-805/2015*. [citat 18.12.2020] Disponibil: https://cac.instante.justice.md/ro/pigd_integration/pdf/87ea8f58-4316-e511-b888-005056a5d154

[1833] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

[1834] GUREV, Dorina. Răpirea unei persoane săvârşită prin participaţie. În: *Studia Universitatis Moldaviae, Seria Ştiinţe Sociale*, 2013, nr. 8, pp. 121-131. ISSN 1814-3199.

[1835] Ibidem.

[1836] Ibidem.

[1837] Ibidem.

[1838] Ibidem.

[1839] GRAMA, Mariana, BOTNARU, Stela, ȘAVGA, Alina, MARTIN, Daniel. *Drept penal. Partea generală. Vol. II*. Chișinău: Tipografia Centrală, 2016, p. 82. 336 p. ISBN 978-9975-53-612-7.

[1840] Ibidem, p. 82.

[1841] Ibidem, p. 82.

[1842] Ibidem, p. 82.

Selevestru[1843] și E. Visterniceanu.[1844] Privitor la condiția organizării în prealabil a membrilor grupului criminal organizat pentru a comite una sau mai multe infracţiuni, M. Grama, S. Botnaru, A. Șavga și D. Martin arată că aceasta presupune că „participanţii nu doar s-au înţeles privitor la săvârșirea în comun a infracţiunii, ceea ce este caracteristic grupului de persoane care acţionează cu înţelegere prealabilă”[1845], „ci au atins și o anumită comunitate obiectivă și subiectivă.”[1846] Puncte de vedere similare au I. Selevestru[1847] și E. Visterniceanu.[1848]

În speța pe care am reprodus-o mai sus, nu sunt prezente indicii ce ar confirma că reuniunea dintre C.K., A.B., D.M. și D.V. avea un caracter stabil și că aceștia s-au organizat în prealabil pentru a comite una sau mai multe infracţiuni. Nu este limpede cât de durabile erau legăturile dintre cei patru făptuitori și dacă asocierea acestora a reușit să devină o comuniune sub aspect atât obiectiv, cât şi subiectiv. Această lipsă de claritate compromite temeinicia reținerii la calificare a art. 46 CP RM.

În alt context, din prevederea de la lit. a) alin. (2) art. 45 CP RM rezultă că latura obiectivă a infracţiunii cu participaţie complexă poate fi realizată de către un singur autor. Dacă infracțiunea este săvârșită de către un singur autor, iar alte persoane apar în rolul de organizator, instigator sau complice, atunci lipsește temeiul aplicării lit. b) alin. (2) art. 259 CP RM. În doctrina penală, ideea în cauză este promovată de către S. Brînza și V. Stati: „Participaţia complexă, atunci când latura obiectivă a sustragerii este realizată de un singur autor, nu poate fi considerată sustragere săvârşită de două ori mai multe persoane”[1849]; „Chiar dacă alături de acest autor mai participă un organizator, instigator sau complice, aceştia doar contribuie la săvârşirea sustragerii, deci nu o săvârşesc”.[1850] O opinie apropiată o exprimă S. Copețchi.[1851]

În următoarea speță, la calificare nu a fost reținută nici lit. b) alin. (2) art. 259 CP RM, nici alin. (5) art. 42 și lit. c) alin. (2) art. 259 CP RM. La concret, M.E. a fost condamnat în conformitate cu art. 260 CP RM. În fapt, acesta a desfășurat activitatea infracțională între anii

---

[1843] SELEVESTRU, Irina. Circumstanţele agravante prevăzute la lit. b) şi d) alin. (2) şi la alin. (3) art. 191 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2015, nr. 11, pp. 126-140. ISSN 1814-3199.
[1844] VISTERNICEANU, Emilia. *Răspunderea penală pentru tâlhărie*. Chișinău: Tipografia Centrală, 2006, p. 179. 232 p. ISBN 978-9975-78-192-3.
[1845] GRAMA, Mariana, BOTNARU, Stela, ȘAVGA, Alina, MARTIN, Daniel. *Drept penal. Partea generală. Vol. II*. Chișinău: Tipografia Centrală, 2016, p. 83. 336 p. ISBN 978-9975-53-612-7.
[1846] Ibidem, p. 83.
[1847] SELEVESTRU, Irina. Circumstanţele agravante prevăzute la lit. b) şi d) alin. (2) şi la alin. (3) art. 191 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2015, nr. 11, pp. 126-140. ISSN 1814-3199.
[1848] VISTERNICEANU, Emilia. *Răspunderea penală pentru tâlhărie*. Chișinău: Tipografia Centrală, 2006, p. 180. 232 p. ISBN 978-9975-78-192-3.
[1849] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. I*. Chișinău: Tipografia Centrală, 2015, p. 852. 1328 p. ISBN 978-9975-53-469-7.
[1850] Ibidem, p. 852.
[1851] COPEŢCHI, Stanislav. Încadrarea infracţiunilor săvârşite în participaţie: aspecte discutabile. În: *Revista Institutului Naţional al Justiţiei*, 2020, nr. 4, pp. 35-42. ISSN 1857-2405.

2012 – 2018. În anul 2015 M.E. s-a asociat cu T.A., iar în anul 2017 în grupul infracțional au intrat C.I. și T.A. Prin intermediul sistemelor informatice conectate la Internet, toți acești făptuitori au oferit servicii de producere, comercializare și punere la dispoziție în mod ilegal a produselor program concepute și adaptate de către M.E. și T.A. *în scopul comiterii de către persoane terțe a infracțiunilor de acces ilegal la informația computerizată*, de fals informatic și de fraudă informatică, exprimate în accesarea ilegală a conturilor bancare ale unor companii cu sediul în SUA și în extragerea ilegală a mijloacelor bănești din aceste conturi. În anul 2018, M.E. a recepționat în contul său mijloace bănești în sumă de 344374,75 lei pentru prestarea serviciilor de producere, comercializare și punere la dispoziție în mod ilegal, a produselor program malițioase.[1852]

La prima vedere, această faptă ar trebui calificată în toate cazurile drept complicitate la infracțiunile prevăzute la art. 259, 260^5 și 260^6 CP RM. Totuși, dacă vom compara sancțiunea din art. 260 CP RM cu sancțiunile din alin. (2) art. 259 CP RM (accesarea ilegală a unor conturi bancare nu poate fi săvârșită fără violarea sistemelor de protecţie, iar această circumstanță agravantă este prevăzută la lit. c) alin. (2) art. 259 CP RM), art. 260^5 și alin. (1) art. 260^6 CP RM, ne dăm seama că fapta lui M.E. și T.A. nu poate fi calificată în toate cazurile în baza alin. (5) art. 42 și lit. c) alin. (2) art. 259, alin. (5) art. 42 și art. 260^5 și alin. (5) art. 42 și alin. (1) art. 260^6 CP RM. O astfel de calificare nediferențiată ar putea să nu respecte regula, conform căreia norma absorbantă (care prevede răspunderea pentru o infracțiune comparativ mai gravă) trebuie să prevadă pedepse mai severe decât cele stabilite în norma absorbită (care prevede răspunderea pentru o infracțiune de o gravitate comparativ mai redusă). Or, în ceea ce privește pedeapsa cu închisoare, stabilită în sancțiunea din art. 260 CP RM, aceasta este mai severă sau de aceeași intensitate în comparație cu pedeapsa cu închisoare, stabilită în sancțiunile din art. 260^5 și alin. (1) art. 260^6 CP RM. În ceea ce privește pedeapsa cu amendă pentru persoanele fizice, stabilită în sancțiunea din art. 260 CP RM, aceasta este mai puțin severă sau de aceeași intensitate în comparație cu pedeapsa cu amendă pentru persoanele fizice, stabilită în sancțiunile din art. 260^5 și alin. (1) art. 260^6 CP RM. În speța analizată, lui M.E. și T.A. le-a fost stabilită pedeapsa cu închisoare. Deci, este întemeiată reținerea la calificare a art. 260 CP RM.

În legătură cu ultima speță care a fost analizată mai sus, trebuie să menționăm că, în conformitate cu alin. (1) art. 8 din Directiva 2013/40/UE, „statele membre asigură că instigarea și complicitatea la săvârșirea oricăreia dintre infracțiunile menționate la articolele 3-7 sunt

[1852] *Decizia Colegiului penal al Curții de Apel Bălți din 24.03.2021. Dosarul nr. 1a-568/2020*. [citat 18.12.2020] Disponibil: https://instante.justice.md/ro/pigd_integration/pdf/FA8E4DB5-A215-4DBA-A2C4-45141DCC4185; *Decizia Colegiului penal lărgit al CSJ din 01.02.2022. Dosarul nr. 1ra-1735/2021*. [citat 18.12.2020] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=20563

incriminate”.[1853] Potrivit alin. 1 art. 11 al Convenției de la Budapesta, „fiecare parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a incrimina ca infracţiune”[1854], „potrivit dreptului său intern, orice complicitate intenţionată la comiterea uneia dintre infracţiunile stabilite în aplicarea art. 2-10, săvârşite cu intenţie”.[1855]

În art. 259 CP RM nu găsim dispoziții în care contribuția organizatorului, a instigatorului sau a complicelui ar fi asimilată cu fapta autorului infracțiunii. Pentru comparație, o asemenea dispoziție conține Codul penal al Regatului Belgiei. Conform § 6 art. 550bis din acest cod, „cel care ordonă comiterea uneia din infracţiunile prevăzute la §§ 1[1856] la 5[1857] sau care incită la comiterea acestora”[1858], „este pedepsit cu închisoarea de la şase luni la cinci ani şi cu o amendă de la o sută [de euro] la două sute de mii [de euro] sau doar cu una din aceste pedepse.”[1859]

Totuși, așa cum rezultă din speța analizată mai sus, infracțiunile, prevăzute la art. 260 și 260^4 CP RM, pot fi considerate exemple de complicitate *sui generis*, printre altele, la oricare dintre infracțiunile prevăzute la art. 259 CP RM. Această idee va fi dezvoltată în capitolul următor al tezei.

2.5.2. Săvârșirea infracțiunii cu violarea sistemelor de protecţie

Oportunitatea agravării răspunderii penale pentru accesul ilegal la informaţia computerizată, săvârșit cu violarea sistemelor de protecţie, rezultă din punctul de vedere exprimat de către N. Chirpat și O. Cerbu: „Protecţia datelor împotriva atacurilor informatice din exterior a fost mereu

---

[1853] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en

[1854] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561

[1855] Ibidem.

[1856] § 1 din acest articol prevede: „Cel care, ştiind că nu este autorizat, accesează un sistem informatic sau se menţine în acesta, este pedepsit cu [închisoarea de la şase luni la doi ani]”* „şi cu o amendă de la douăzeci şi şase [de euro] la douăzeci şi cinci de mii [de euro] sau doar la una din aceste pedepse”*; „Dacă infracţiunea menţionată la § 1 este comisă cu intenţie frauduloasă, pedeapsa cu [închisoarea este de la şase luni la trei ani]”.*

* *Codul penal al Regatului Belgiei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html

[1857] § 5 din acest articol prevede: „Cel care, fără a avea dreptul, posedă, produce vinde, obţine în vederea utilizării, importă, difuzează sau pune la dispoziţie sub orice altă formă, orice dispozitiv”*, „inclusiv date informatice, conceput în principal sau adaptat în principal pentru a permite comiterea infracţiunilor prevăzute la §§ 1 la 4”*, „este pedepsit cu închisoarea de la şase luni la trei ani şi cu o amendă de la douăzeci şi şase de euro la o sută de mii de euro sau doar cu una din aceste pedepse”.*

* *Codul penal al Regatului Belgiei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html

[1858] *Codul penal al Regatului Belgiei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html

[1859] Ibidem.

una dintre principalele provocări”[1860]; „Odată cu evoluţia tehnologiei, securizarea informaţiilor importante a devenit un proces din ce în ce mai complicat şi mai stringent”[1861]; „În timp ce specialiştii dezvoltă soluţii avansate pentru a cripta şi securiza datele digitale, se găsesc rapid modalităţi pentru anularea acestor eforturi”[1862]; „[...] Pentru că sistemele informatice să-şi realizeze scopul, informaţia trebuie să ie disponibilă atunci când este necesar”[1863]; „Este important ca sistemele critice să fie disponibile mereu şi o măsură de precauţie este prevenirea atacurilor din exterior”.[1864] Așadar, menirea sistemelor de protecție este de a împiedica accesul ilegal la informaţia computerizată. Sfidând efortul de contracarare a accesului ilegal la informaţia computerizată, făptuitorul demonstrează o mai mare periculozitate socială decât în cazul în care nu ar viola sisteme de protecție.

Trebuie menționat precedentul istoric al dispoziției de la lit. c) alin. (2) art. 259 CP RM. Astfel, în art. 176^1 CP RM din 1961, la alineatul 1 era prevăzută răspunderea pentru „accesul ilegal (nesancţionat) la informaţia ce se păstrează în sistemul computerizat, cu încălcarea sistemului de protecţie.”[1865] Observăm că, în cazul infracțiunii prevăzute la alin. 1 art. 176^1 CP RM din 1961, încălcarea sistemului de protecţie reprezenta condiția obligatorie, în a cărei lipsă nu putea fi aplicată răspunderea pentru această infracțiune. În ipoteza prevăzută la lit. c) alin. (2) art. 259 CP RM, poziția legiuitorului este alta. Violarea sistemelor de protecție nu constituie condiția obligatorie pentru aplicarea art. 259 CP RM. Lipsa în cele săvârșite a violării sistemelor de protecție înseamnă lipsa agravantei de la lit. c) alin. (2) art. 259 CP RM, ceea ce nu exclude aplicarea alin. (1) art. 259 CP RM.

În legile penale ale altor state putem să identificăm norme care se apropie conceptual de alin. 1 art. 176^1 CP RM din 1961 (de exemplu, în alin. (1) secţ. 230 CP RCe[1866], în alin. (1) § 217 CP RE[1867], în alin. (1) § 202a CP RFG[1868], în alin. (1) secţ. 241 CP RLe[1869] și în alin. 1 art. $198^{(1)}$ CP RLi[1870]).

[1860] CHIRPAT, Nicolae, CERBU, Olga. Metode de utilizare a instrumentelor de securitate a informaţiei. În: *Teoria şi practica administrării publice (20 mai 2013, Chişinău)*. Chișinău: Academia de Administrare Publică, 2013, pp. 462-464. ISBN 978-9975-4241-5-8.
[1861] Ibidem.
[1862] Ibidem.
[1863] Ibidem.
[1864] Ibidem.
[1865] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
[1866] *Codul penal al Republicii Cehe*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Cehia-RO.html
[1867] *Codul penal al Republicii Estonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Estonia-RO.html
[1868] *Codul penal al Republicii Federale Germania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Germania-RO.html

În contextul analizei laturii obiective a faptelor infracționale ce sunt prevăzute de art. 259 CP RM, am afirmat: În consecință, apreciem că trebuie abrogată prevederea de la lit. c) alin. (2) art. 259 CP RM („cu violarea sistemelor de protecţie"). Totodată, dispoziția de la alin. (1) art. 259 CP RM trebuie completată cu sintagma „prin violarea măsurilor de securitate". Cu acest prilej trebuie să reiterăm că violarea măsurilor de securitate trebuie să devină condiția obligatorie pentru existența variantei-tip a faptei specificate în art. 259 CP RM.

În Codul penal al Republicii Moldova nu găsim definiția noțiunii „sisteme de protecție", care se utilizează la lit. c) alin. (2) art. 259 CP RM. Din acest motiv suntem nevoiți să căutăm sensul acestei noțiuni în alte surse normative.

Spre exemplu, conform art. 2 al Legii nr. 1069/2000, prin „protecţia datelor" se înțelege „totalitatea procedurilor organizaţional-tehnice şi actelor normative utilizate pentru a se evita cauzarea oricăror pagube intereselor proprietarilor de date"[1871], „sistemelor informatice, precum şi utilizatorilor de informaţii".[1872] Considerăm mai apropiată contextului din lit. c) alin. (2) art. 259 CP RM definiția formulată în art. 2 din Legea nr. 20/2009: „măsuri de securitate – folosirea unor proceduri"[1873], „dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricţionat sau interzis pentru anumite categorii de utilizatori".[1874] La lit. e) alin. (1) art. 7 al aceleiași legi se stabilește că „furnizorii de servicii[1875] sunt obligaţi [...] să întreprindă *măsuri de securitate prin utilizarea unor proceduri, dispozitive"*[1876] *„sau programe informatice specializate cu al căror ajutor accesul la un sistem informatic să fie restricţionat sau interzis utilizatorilor neautorizaţi* (evid. ns.)".[1877]

O dispoziție cu conținut asemănător poate fi găsită în Legea României nr. 161/2003. Astfel, potrivit lit. h) alin. (1) art. 35 al acestei legi, „prin măsuri de securitate se înţelege folosirea unor

---

[1869] *Codul penal al Republicii Letonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Letonia-RO.html

[1870] *Codul penal al Republicii Lituania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Lituania-RO.html

[1871] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.

[1872] Ibidem.

[1873] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.

[1874] Ibidem.

[1875] Conform art. 2 al Legii nr. 20/2009, furnizor de servicii este „orice entitate publică sau privată care oferă utilizatorilor serviciilor sale posibilitatea de a comunica prin intermediul unui sistem informatic"*, „precum şi orice altă entitate care prelucrează sau stochează date informatice pentru acest serviciu de comunicaţii sau pentru utilizatorii săi".*

* Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.

[1876] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.

[1877] Ibidem.

proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la un sistem informatic este restricționat sau interzis pentru anumite categorii de utilizatori”.[1878] În același context, comportă interes interpretarea dată în Decizia Curții Constituționale a României nr. 183 din 29.03.2018 referitoare la excepţia de neconstituţionalitate a dispoziţiilor art. 360 alin. (3) din Codul penal: „[...] 31. Susținerea autorului excepției, potrivit căreia nu avea cum să cunoască ce se înțelege prin „proceduri, dispozitive sau programe specializate””[1879] „nu poate fi primită, deoarece, așa cum s-a arătat, legiuitorul a definit în cuprinsul art. 35 alin. (1) lit. h) din Legea nr. 161/2003 ce se înțelege prin acestea”[1880]; „Legiuitorul noului Cod penal nu a făcut altceva decât să înlocuiască termenul generic „măsuri de securitate” cu definiția dată acestuia de legea mai sus menționată”[1881]; „[...] 35. De aceea, nu poate fi primită susținerea potrivit căreia destinatarii dispozițiilor legale criticate nu își pot adapta conduita în funcție de conținutul lor”[1882], „deoarece acestea sunt suficient de clare, precise și previzibile, sens în care legiuitorul a definit în termeni lipsiți de echivoc”[1883] „că accesul fără drept la un sistem informatic protejat de măsuri de securitate este interzis”[1884]; „Mai mult, în anumite situații determinate chiar de evoluția tehnică informatică, suplețea legii este de preferat”[1885], „întrucât nu se pot stabili aprioric exhaustiv și în mod concret care sunt sistemele informatice și măsurile de securitate care le însoțesc”.[1886]

În literatura de specialitate se propune clasificarea măsurilor de securitate. De pildă, V. Coman vorbește despre „măsuri de protecție logică (parole) și procedurală (prin stabilirea unor politici de securitate)”.[1887] La rândul său, C. Hlopeatnicov afirmă că „metodele criptografice sunt utilizate în mod tradițional pentru a construi mecanisme de securitate”[1888]; „Metodele de criptare simetrice se bazează pe blocuri simple și ușor implementate de permutare a datelor”[1889];

[1878] Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.

[1879] Decizia Curții Constituționale a României referitoare la excepţia de neconstituţionalitate a dispoziţiilor art. 360 alin. (3) din Codul penal: nr. 183 din 29.03.2018. În: *Monitorul Oficial al României*, 2018, nr. 486.

[1880] Ibidem.

[1881] Ibidem.

[1882] Ibidem.

[1883] Ibidem.

[1884] Ibidem.

[1885] Ibidem.

[1886] Ibidem.

[1887] COMAN, Vasile. *Accesarea contului de e-mail și de Facebook. Noțiunea de date informatice. Forma agravată prevăzută de art. 360 alin. (3) CP*. [citat 06.03.2022] Disponibil: https://www.universuljuridic.ro/accesarea-contului-de-e-mail-si-de-facebook-notiunea-de-date-informatice-forma-agravata-prevazuta-de-art-360-alin-3-cp/

[1888] HLOPEATNICOV, Claudia. Mecanisme și protocoale de protecția informației în rețele și sisteme informaționale. În: *Conferinţa tehnico-ştiinţifică a studenţilor, masteranzilor şi doctoranzilor. Vol. 1 (26-29 martie 2019, Chişinău)*. Chișinău: Universitatea Tehnică a Moldovei, 2019, pp. 421-422. ISBN 978-9975-45-588-6.

[1889] Ibidem.

„Metodele de criptografie a cheilor publice se bazează pe utilizarea problemei teoretice și complexe corespunzătoare (factorizare, logaritmă discretă etc.).”[1890] Prezintă interes, de asemenea, opinia lui G. Zlati. Acesta distinge, întâi de toate: 1) măsurile de interzicere a accesului: procedura de autentificare în cadrul sistemului informatic[1891]; permiterea accesului doar a unor anumitor IP-uri sau clase de IP-uri[1892]; interzicerea totală a accesului utilizatorilor dintr-o anumită țară etc.[1893]; 2) măsurile de restricționare a accesului (de exemplu, crearea unui cont pentru vizitatori ce permite accesul într-o manieră extrem de limitată).[1894] În al doilea rând, G. Zlati deosebește: 1) procedurile de interzicere ori de restricționare a accesului: parole sau coduri de acces; criptarea datelor informatice[1895]; utilizarea unor elemente biometrice (urmele papilare, scanarea retinei, scanarea facială, analiza vocii); setarea adreselor MAC (media access control address); securizarea unui browser web[1896]; 2) dispozitivele de interzicere ori de restricționare a accesului: card bancar (privit ca o veritabilă cheie de acces[1897]; dispozitiv ce necesită a fi introdus în portul USB pentru decriptarea sistemului informatic, în vederea accesării acestuia[1898]; card ce trebuie introdus într-un *slot* al sistemului informatic și care atestă identitatea utilizatorului[1899]; 3) programele informatice ce interzic ori restricționează accesul: programe informatice de tip *firewall*; programe informatice de tip antivirus sau *antispyware*.[1900]

Considerăm mai reușite clasificările propuse de către G. Zlati, deoarece acestea corespund definiției noțiunii „măsuri de securitate” formulate în art. 2 din Legea nr. 20/2009. Totodată, accentuăm că, în accepțiunea lit. c) alin. (2) art. 259 CP RM, au relevanță măsurile de securitate împotriva accesului ilegal nu la sistemul informatic, ci la informația computerizată din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau rețeaua informatică.[1901]

În analiza noastră nu putem face abstracție de opinia pe care o exprimă V. Coman. Referitor la o ipoteză care este asemănătoare cu cea prevăzută la lit. c) alin. (2) art. 259 CP RM, acest autor menționează: „Introducerea corectă a numelui de cont (identificatorului) și a parolei [...]

[1890] Ibidem.
[1891] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 255. 658 p. ISBN 978-606-8892-62-7.
[1892] Ibidem, p. 255.
[1893] Ibidem, p. 255.
[1894] Ibidem, p. 255.
[1895] Ibidem, p. 260.
[1896] Ibidem, p. 260.
[1897] Ibidem, p. 261.
[1898] Ibidem, p. 261.
[1899] Ibidem, p. 262.
[1900] Ibidem, p. 262.
[1901] STRÎMBEANU, Alexandru. *Răspunderea penală pentru accesul ilegal la informaţia computerizată: Monografie*. Chișinău: Tipografia Centrală, 2023, p. 350. 430 p. ISBN 978-5-88554-178-7.

exclude o forțare a măsurilor de securitate (parole, coduri de acces etc.)”[1902]; „[...] În cazul în care accesul se realizează de către făptuitor în urma autentificării corecte în sistem pe baza utilizării numelui de cont”[1903] „(identificatorului) și parolei corecte, încadrarea în prevederile art. 42 alin. (3) din Legea nr. 161/2003 ar fi eronată, întrucât”[1904], „din punct de vedere tehnic (al sistemului informatic), autentificarea (chiar frauduloasă) s-a făcut corect, fiind introduse datele pe care acesta le recunoaște”[1905]; „Acceptând doar aceste două elemente de siguranță – nume de cont și parolă”[1906] – „sistemul nu are alte posibilități de a verifica identitatea utilizatorului de drept și nici nu consideră că au fost încălcate măsurile de securitate.”[1907] În pct. 37 din Decizia Curții Constituționale a României nr. 183 din 29.03.2018 referitoare la excepţia de neconstituţionalitate a dispoziţiilor art. 360 alin. (3) din Codul penal, găsim o explicație, care cel puțin în aparență, nu diferă ca esență de opinia lui V. Coman: „Forma agravată a infracțiunii prevăzută de art. 360 alin. (3) din Codul penal există atunci când făptuitorul utilizează „mijloace calificate” de acces”[1908], „apte să depășească ori să eludeze protecția sporită instituită prin măsurile de securitate. Textul de lege criticat nepunând vreo condiție cât privește modul concret în care restricția este nesocotită”[1909], „Curtea constată că își menține astfel actualitatea jurisprudența care, anterior Codului penal, a reținut incidența art. 42 alin. (3) din Legea nr. 161/2003 pentru fapte”[1910] „precum *accesul, prin utilizarea frauduloasă a unui user-name și a parolei aferente acestuia* (evid. ns.), în sistemul informatic al unei bănci [...]”[1911], „ori accesarea contului de mesagerie instalat pe calculatorul comun al făptuitorului și al persoanei vătămate [...]”[1912]; „Pentru aceleași rațiuni, forma agravată subzistă și atunci când nesocotirea restricției este facilitată de disfuncțiile sau carențele sistemului de protecție”[1913], „care permit înlăturarea sau ocolirea/eludarea facilă a protecției”.[1914]

Mai flexibilă este părerea lui G. Zlati care diferențiază două ipoteze: „1) făptuitorul violează măsurile de securitate: obținerea în mod fraudulos a codului de acces de la victimă nu face să

[1902] COMAN, Vasile. *Accesul prin „încălcarea măsurilor de securitate” prevăzută de art. 42 alin. (3) din Legea nr. 161/2003. Condiţii de apreciere*. [citat 30.12.2022] Disponibil: https://www.universuljuridic.ro/accesul-prin-incalcarea-masurilor-de-securitate-prevazuta-de-art-42-alin-3-din-legea-nr-161-2003-conditii-de-apreciere/
[1903] Ibidem.
[1904] Ibidem.
[1905] Ibidem.
[1906] Ibidem.
[1907] Ibidem.
[1908] Decizia Curții Constituționale a României referitoare la excepţia de neconstituţionalitate a dispoziţiilor art. 360 alin. (3) din Codul penal: nr. 183 din 29.03.2018. În: *Monitorul Oficial al României*, 2018, nr. 486.
[1909] Ibidem.
[1910] Ibidem.
[1911] Ibidem.
[1912] Ibidem.
[1913] Ibidem.
[1914] Ibidem.

dispară sistemul de protecție”[1915] „împotriva unui acces neautorizat, acesta continuând să fie unul efectiv *in abstracto*”.[1916] „[...] Faptul că agentul a fost autorizat la un moment dat să acceseze sistemul informatic și a deținut, în acest sens, un nume de utilizator”[1917] „și o parolă nu exclude reținerea agravantei, dacă ulterior pierderii autorizării acesta folosește respectivele date pentru a obține un acces neautorizat la respectivul sistem informatic”[1918]; „2) făptuitorul nu violează măsurile de securitate: dacă numele de utilizator și parola sunt memorate în mod automat la prima autentificare a victimei”[1919], „iar autorul se folosește de această împrejurare pentru a accesa neautorizat sistemul informatic”[1920]; „autentificarea se realizează în mod automat, cau urmare a unei opțiuni activate de către victimă”.[1921] Agreăm în cele mai multe privințe aceste opinii ale lui G. Zlati.

În altă privință, numărul de sisteme de protecție care sunt violate de către făptuitor, nu influențează asupra aplicării lit. c) alin. (2) art. 259 CP RM. Acest număr poate fi însă luat în considerare la individualizarea pedepsei. De exemplu, într-o concluzie, formulată într-o speță care se conține în practica judiciară română, se vorbește despre violarea câtorva sisteme de protecție (măsuri de securitate): ATM-ul, prin natura sa, reprezintă un sistem informatic prevăzut cu măsuri de securitate, al cărui acces se face prin utilizarea a două categorii de măsuri de securitate: prima este reprezentată de datele prezente pe banda magnetică[1922] și/sau pe CIP-ul suportului din material PVC (element de identificare unic în sistemul informatic bancar, similar unui nume de utilizator, prin intermediul căruia este identificat titularul)[1923], iar a doua categorie este reprezentată de codul PIN, măsură fără de care nu se poate realiza accesul total la sistemul informatic al ATM-ului.[1924]

[1915] ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020, p. 263. 658 p. ISBN 978-606-8892-62-7.
[1916] Ibidem, p. 263.
[1917] Ibidem, p. 263.
[1918] Ibidem, p. 263.
[1919] Ibidem, p. 264.
[1920] Ibidem, p. 264.
[1921] Ibidem, p. 264.
[1922] *Tribunalul Prahova. Sentință penală 614 din 15.12.2017*. [citat 30.12.2022] Disponibil: https://www.jurisprudenta.com/jurisprudenta/speta-144rmtop/
[1923] Ibidem.
[1924] Ibidem.

2.5.3. Săvârșirea infracțiunii cu conectarea la canalele de telecomunicaţii

Prevederi asemănătoare cu lit. d) alin. (2) art. 259 CP RM pot fi identificate în legile penale ale altor state (spre exemplu, în alin. 2 art. 370C CPGr[1925], în alin. 3 subsecţ. 138ab CP RȚJ(O)[1926] și în § 1 art. 267 CP RP[1927]).

Există o probabilitate mare că la lit. d) alin. (2) art. 259 CP RM, prin „canalele de telecomunicaţii" se înțelege „reţeaua de comunicaţii electronice" în sensul art. 2 al Legii nr. 241 din 15.11.2007 a comunicaţiilor electronice (în continuare – Legii nr. 241/2007): „reţeaua de comunicaţii electronice o constituie sistemele de transmisie şi, după caz, echipamentele de comutare sau rutare"[1928], „precum şi alte resurse care permit transmiterea semnalelor prin suport fizic, electromagnetic sau prin orice alte mijloace, incluzând reţele de comunicaţii prin satelit"[1929], „reţele fixe (cu comutare de circuite sau comutare de pachete, inclusiv Internet) şi reţele mobile terestre, reţele de transport al energiei electrice"[1930], „în cazul în care acestea sunt utilizate şi pentru transmiterea semnalelor"[1931], „reţele utilizate pentru difuzarea programelor audiovizuale, reţele de televiziune prin cablu, indiferent de tipul informaţiei transmise".[1932]

Din același articol aflăm că sunt rețele de comunicaţii electronice: reţeaua publică de telefonie, adică „reţeaua de comunicaţii electronice utilizată pentru furnizarea serviciilor publice de telefonie şi care permite comunicarea vocală sau altă formă de comunicare, cum ar fi comunicarea prin fax sau transmiterea de date, între punctele terminale ale reţelei"[1933]; reţeaua de comunicaţii speciale, adică „reţeaua de comunicaţii electronice destinată pentru asigurarea necesităţilor autorităţilor publice, apărării, securităţii naţionale şi ordinii publice".[1934]

Tipurile de reţele publice de comunicaţii electronice sunt specificate în Nomenclatorul tipurilor de reţele şi servicii de comunicaţii electronice supuse regimului de autorizare generală (anexa nr. 1 la Hotărârea ANRCETI nr. 57 din 21.12.2010 cu privire la Regulamentul privind

---

[1925] *Codul penal al Greciei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Grecia-RO.html
[1926] *Codul penal al Regatului Ţărilor de Jos (Olanda)*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Olanda-RO.html
[1927] *Codul penal al Republicii Polone*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Polonia-RO.html
[1928] Legea comunicaţiilor electronice: nr. 241 din 15.11.2007. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 51-54, 155.
[1929] Ibidem.
[1930] Ibidem.
[1931] Ibidem.
[1932] Ibidem.
[1933] Ibidem.
[1934] Ibidem.

regimul de autorizare generală şi eliberare a licenţelor de utilizare a resurselor limitate pentru furnizarea reţelelor şi serviciilor publice de comunicaţii electronice[1935]).

În contextul analizei obiectului imaterial al infracțiunilor prevăzute la art. 259 CP RM, am afirmat: noțiunea „rețea informatică" se intersectează cu noțiunea „rețea de comunicații electronice". În cazul în care rețeaua de comunicații electronice oferă posibilitatea realizării unui schimb de date informatice, ea cumulează calitatea de rețea informatică. În acest caz, este posibil concursul ideal al infracțiunilor prevăzute la art. 259 și 261^1 CP RM.[1936]

2.5.4. Săvârșirea infracțiunii cu folosirea unor mijloace tehnice speciale

Noțiunea „mijloace tehnice speciale" nu este definită în Codul penal al Republicii Moldova. Găsim însă definiția corespunzătoare în Hotărârea Guvernului nr. 100 din 09.02.2009 privind aprobarea Regulamentului cu privire la importul, exportul, proiectarea, producerea şi comercializarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei şi a Clasificatorului mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei (în continuare – Hotărârea Guvernului nr. 100/2009). Conform pct. 2 din Anexa nr. 1 la acest act normativ, „la mijloace tehnice speciale destinate pentru obţinerea ascunsă a informaţiei [...] sunt atribuite mijloacele tehnice şi/sau de program"[1937], „proiectate, modificate sau programate pentru captarea, obţinerea, interceptarea, culegerea, ascultarea, înregistrarea şi transmiterea semnalelor informaţionale de natură sonoră, vizuală, electromagnetică sau de altă natură"[1938], „inclusiv din reţelele de comunicaţii electronice, în scopul obţinerii accesului ascuns la informaţia străină".[1939]

În practica judiciară autohtonă[1940] skimmer-ul este menționat ca mijloc tehnic special, pe care făptuitorul îl folosește la săvârșirea accesului ilegal la informaţia computerizată.

[1935] Hotărârea ANRCETI cu privire la Regulamentul privind regimul de autorizare generală şi eliberare a licenţelor de utilizare a resurselor limitate pentru furnizarea reţelelor şi serviciilor publice de comunicaţii electronice: nr. 57 din 21.12.2010. În: *Monitorul Oficial al Republicii Moldova*, 2011, nr. 22-24, 127.

[1936] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale"*, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

[1937] Hotărârea Guvernului privind aprobarea Regulamentului cu privire la importul, exportul, proiectarea, producerea şi comercializarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei şi a Clasificatorului mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei: nr. 100 din 09.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 37-40, 164.

[1938] Ibidem.

[1939] Ibidem.

[1940] *Decizia Colegiului penal al Curții de Apel Chișinău din 15.06.2015. Dosarul nr. 1a-805/2015*. [citat 18.12.2020] Disponibil: https://cac.instante.justice.md/ro/pigd_integration/pdf/87ea8f58-4316-e511-b888-005056a5d154; *Sentința Judecătoriei sect. Botanica, mun. Chișinău, din 26.02.2016. Dosarul nr. 1-12/2016*. [citat 18.12.2020] Disponibil: https://instante.justice.md/ro/pigd_integration/pdf/691A992F-6DDC-E511-A1AB-005056A5D154

Detalii despre acest mijloc sunt prezentate în Decizia Înaltei Curți de Casaţie și Justiţie a României nr. 15 din 14.10.2013 privind interpretarea şi aplicarea unitară a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noţiunii de acces fără drept la un sistem informatic: „Skimmingul reprezintă activitatea de copiere a datelor valide de pe banda magnetică a unui card autentic prin intermediul unui dispozitiv de citire a cardurilor”[1941], „fără cunoștința posesorului legitim, cu intenția de a fi folosite în scopuri frauduloase”[1942]; „Există dispozitive de skimming în cazul cărora datele de pe banda magnetică sunt copiate în momentul când cardul este înmânat de către titular unei alte persoane”[1943] „(de regulă, un comerciant în timpul efectuării unei tranzacții) sau montate la ATM-uri sau POS-uri – ATM/POS skimmers”[1944], „datele de pe banda magnetică fiind înregistrate în momentul când titularul cardului introduce cardul în bancomat, pentru a efectua o tranzacție”[1945]; „Dispozitivele de skimming sunt însoțite de minivideocamere și/sau de dispozitive modificate”[1946] „de tip tastatură (keypads) care înregistrează codul PIN aferent cardului, în momentul tastării acestuia.”[1947]

În aceeași decizie se menționează: „Montarea la bancomat a dispozitivelor autonome de citire a benzii magnetice a cardului autentic şi a codului PIN aferent acestuia”[1948] „(skimmere, minivideocamere sau dispozitive tip tastatură falsă) constituie infracţiunea prevăzută de art. 46 alin. (2) din Legea nr.161/2003”.[1949] Așadar, nu doar skimmer-ul, ci și dispozitivul tip tastatură falsă pot fi considerate mijloace tehnice speciale în sensul lit. e) alin. (2) art. 259 CP RM. Minivideocamera nu îndeplinește această condiție. Deși poate avea calitatea de mijloc tehnic special, minivideocamera nu poate asigura accesul la o informație computerizată.

Precizăm că alin. (2) art. 46 (actualmente abrogat) al Legii României nr. 161/2003 prevedea răspunderea pentru „deţinerea, fără drept, a unui dispozitiv, program informatic, parolă, cod de

[1941] Decizia Înaltei Curți de Casaţie și Justiţie a României privind interpretarea şi aplicarea unitară a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noţiunii de acces fără drept la un sistem informatic: nr. 15 din 14.10.2013. În: *Monitorul Oficial al României*, 2013, nr. 760.
[1942] Ibidem.
[1943] Ibidem.
[1944] Ibidem.
[1945] Ibidem.
[1946] Ibidem.
[1947] Ibidem.
[1948] Ibidem.
[1949] Ibidem.

acces sau dată informatică”[1950] „dintre cele prevăzute la alin. (1) în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 42-45”.[1951]

În Codul penal al României[1952], prevederilor de la art. 46 al Legii României nr. 161/2003 le corespund prevederile art. 365 „Operațiuni ilegale cu dispozitive sau programe informatice”.[1953] Ca urmare, explicația din Decizia Înaltei Curți de Casaţie și Justiţie a României, prezentată anterior, își menține valabilitatea cu anumite ajustări.

În Codul penal al Republicii Moldova, art. 260 corespunde, într-o măsură anumită, cu art. 365 CPR. Art. 260 CP RM prevede răspunderea pentru „producerea, importul, comercializarea sau punerea la dispoziţie, sub orice altă formă, în mod ilegal, a mijloacelor tehnice sau produselor program” [1954], „concepute sau adaptate, în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 237, 259, 260^1-260^3, 2605 şi 260^6”.[1955] Aceste idei vor fi dezvoltate în capitolul următor al tezei.

2.5.5. Săvârșirea infracțiunii cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice, în scopul săvârşirii uneia dintre infracţiunile prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6 CP RM

În alte cazuri decât cel prevăzut la lit. f) alin. (2) art. 259 CP RM, scopul infracțiunii nu este special și poate fi luat în considerare numai la individualizarea pedepsei. Dacă vorbim despre alte cazuri decât cel prevăzut la lit. f) alin. (2) art. 259 CP RM, atunci este important ca scopul infracțiunii să presupună săvârşirea altor infracțiuni decât cele „prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6”.[1956]

[1950] Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnitatilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.
[1951] Ibidem.
[1952] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[1953] Acest articol prevede: „(1) Fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziție sub orice formă”*: „a) dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre infracțiunile prevăzute în art. 360-364”*; „b) parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic”*, „în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364, se pedepsește cu închisoare de la 6 luni la 3 ani sau cu amendă”*; „(2) Deținerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces sau a altor date informatice”* „dintre cele prevăzute în alin. (1), în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364”*, „se pedepsește cu închisoare de la 3 luni la 2 ani sau cu amendă.*
* Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[1954] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[1955] Ibidem.
[1956] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

Prevederea de la lit. f) alin. (2) art. 259 CP RM constituie, probabil, viziunea legiuitorului moldovean asupra unui fragment al art. 2 „Accesarea ilegală” din Convenția de la Budapesta: „Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern”[1957], „accesarea intenţionată şi fără drept a ansamblului ori a unei părţi a unui sistem informatic”[1958]; „O parte poate condiţiona o astfel de incriminare de comiterea încălcării respective prin violarea măsurilor de securitate, cu intenţia de a obţine date informatice”[1959] „ori *cu altă intenţie delictuală* (evid. ns.), sau de legătura dintre încălcarea respectivă şi un sistem informatic conectat la alt sistem informatic”.[1960]

V. Stati menționează: „Miningul poate atrage răspunderea penală în ipoteza despre care ne vorbesc V.A. Perov și R. Abrihan”[1961]; „Astfel, primul dintre acești autori menționează „utilizarea unui program-virus de computer care permite folosirea unui anumit procent”[1962] „din puterea de calcul a computerului infectat, pentru ca făptuitorul să poată practica mining”[1963].[1964]; „La rândul său, R. Abrihan opinează: „Minarea profitabilă de monede necesită o cantitate imensă de putere de calcul, de aceea atacatorii instalează programe malware”[1965] „pe computerele utilizatorilor pentru a „sustrage‖ puterea de calcul necesară‖”[1966].[1967]; „În circumstanțele descrise de cei doi autori precitați, [...] este aplicabilă [printre altele] prevederea de la lit. f) alin. (2) art. 259 CP RM”[1968], „care stabilește răspunderea pentru accesul ilegal la informaţia computerizată, săvârşit cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice”[1969], „în scopul săvârşirii, inter alia, a uneia dintre infracţiunile prevăzute la art. 260^6 CP RM.”[1970] Cu toate acestea, este oportună abrogarea dispoziției de la lit. f) alin. (2) art. 259 CP RM. Or, dacă, după o

---

[1957] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[1958] Ibidem.
[1959] Ibidem.
[1960] Ibidem.
[1961] STATI, Vitalie. Fabricarea sau punerea în circulație a monedelor virtuale în Republica Moldova: conotații juridico-penale. În: *Актуальные научные исследования в современном мире // Журнал*. Переяслав, 2019, Вып. 11, ч. 5, с. 100-108. ISSN 2524-0986.
[1962] Ibidem.
[1963] ПЕРОВ, В.А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют. În: *Безопасность бизнеса*, 2018, № 2, с. 25-29. ISSN 2072-3644.
[1964] STATI, Vitalie. Fabricarea sau punerea în circulație a monedelor virtuale în Republica Moldova: conotații juridico-penale. În: *Актуальные научные исследования в современном мире // Журнал*. Переяслав, 2019, Вып. 11, ч. 5, с. 100-108. ISSN 2524-0986.
[1965] Ibidem.
[1966] ABRIHAN, Raluca. *Tendințe în securitate IT: România, peste medie la minare ilicită de criptomonede, atacuri phishing şi ransomware*. [citat 05.09.2020] Disponibil: https://www.startupcafe.ro/smart-tech/tendinte-securitate-it-atac-minare-ilegalacriptomonede-microsoft.htm
[1967] STATI, Vitalie. Fabricarea sau punerea în circulație a monedelor virtuale în Republica Moldova: conotații juridico-penale. În: *Актуальные научные исследования в современном мире // Журнал*. Переяслав, 2019, Вып. 11, ч. 5, с. 100-108. ISSN 2524-0986.
[1968] Ibidem.
[1969] Ibidem.
[1970] Ibidem.

infracțiune specificată în alin. (1) art. 259 CP RM, este săvârșită o altă infracțiune prevăzută la aceeași normă, ar fi suficient să vorbim despre concursul real dintre două infracțiuni prevăzute la alin. (1) art. 259 CP RM.

2.5.6. Săvârșirea infracțiunii în privinţa informaţiei protejate de lege

Noțiunea „informaţie protejată de lege" nu este definită nici în Codul penal al Republicii Moldova, nici în legislația extrapenală. Din acest motiv vom apela la doctrină pentru a percepe semnificația acestei noțiuni utilizate în dispoziția de la lit. g) alin. (2) art. 259 CP RM.

De pildă, Iu. Gulbin consideră că „noțiunea „informația computerizată protejată de lege" este foarte vagă și se referă aproape la orice informație computerizată"[1971]; „Informația computerizată este protejată de o gamă destul de largă de acte legislative"[1972]; „Dacă informația computerizată nu constituie obiectul de protecție al unuia dintre aceste acte, atunci, de regulă, ea devine obiectul protecției unui alt act legislativ"[1973]; „Practic, nu există informații computerizate neprotejate".[1974] Nu putem accepta un asemenea punct de vedere. Nu oricare informație computerizată reprezintă obiectul de protecție al unei legi. Este întemeiată opinia lui S. Kocioi și D. Saveliev care menționează că protejată de lege trebuie considerată doar acea informație computerizată la care accesul este restrâns în conformitate cu legea.[1975]

Printre principalele legi care protejează informațiile, inclusiv informațiile computerizate, se numără Legea nr. 982 din 11.05.2000 privind accesul la informaţie (în continuare – Legea nr. 982/2000). Potrivit pct. 3) alin. (1) art. 11 al acestei legi, „furnizorul de informaţii, în conformitate cu competenţele care îi revin, este obligat [...] să respecte limitările accesului la informaţie"[1976], „prevăzute de legislaţie, în scopul *protejării informaţiei confidenţiale* (evid. ns.) [...]."[1977] Potrivit alin. (2) art. 7 al Legii nr. 982/2000, „[...] accesul la informaţiile oficiale nu poate fi îngrădit, cu excepţia: a) informaţiilor atribuite la secret de stat, reglementate prin lege organică"[1978], „a căror divulgare neautorizată sau pierdere poate aduce atingere intereselor şi/sau

---

[1971] ГУЛЬБИН, Ю. Преступления в сфере компьютерной информации. În: *Российская юстиция*, 1997, № 10, с. 24-25. ISSN 0131-6761.
[1972] Ibidem.
[1973] Ibidem.
[1974] Ibidem.
[1975] КОЧОИ, С., САВЕЛЬЕВ, Д. Ответственность за неправомерный доступ к компьютерной информации. În: *Российская юстиция*, 1999, № 1, с. 44-45. ISSN 0131-6761.
[1976] Legea privind accesul la informaţie: nr. 982 din 11.05.2000. În: *Monitorul Oficial al Republicii Moldova*, 2000, nr. 88-90, 664.
[1977] Ibidem.
[1978] Ibidem.

securităţii Republicii Moldova”[1979]; „b) informaţiilor confidenţiale din domeniul afacerilor, prezentate instituţiilor publice cu titlu de confidenţialitate”[1980], „reglementate de legislaţia privind secretul comercial, şi care ţin de producţie, tehnologie, administrare, finanţe, de altă activitate a vieţii economice”[1981], „a căror divulgare (transmitere, scurgere) poate atinge interesele întreprinzătorilor; c) informaţiilor cu caracter personal, a căror divulgare este considerată drept o imixtiune”[1982] „în viaţa privată a persoanei, protejată de legislaţia privind protecţia datelor cu caracter personal; d) informaţiilor ce ţin de activitatea operativă”[1983] „şi de urmărire penală a organelor de resort, dar numai în cazurile în care divulgarea acestor informaţii ar putea prejudicia urmărirea penală”[1984], „interveni în desfăşurarea unui proces de judecată, lipsi persoana de dreptul la o judecare corectă şi imparţială a cazului său”[1985], „ori ar pune în pericol viaţa sau securitatea fizică a oricărei persoane – aspecte reglementate de legislaţie”[1986]; „e) informaţiilor ce reflectă rezultatele finale sau intermediare ale unor investigaţii ştiinţifice şi tehnice”[1987] „şi a căror divulgare privează autorii investigaţiilor de prioritatea de publicare sau influenţează negativ exercitarea altor drepturi protejate prin lege.”[1988]

În Legea nr. 982/2000 este folosită sintagma „informaţii oficiale cu accesibilitate limitată”.[1989] Din alin. (1) art. 7 al acestei legi rezultă că, prin „informaţii oficiale cu accesibilitate limitată” se are în vedere acele informații a căror accesare este supusă restricţiilor reglementate prin lege organică”[1990] „şi care corespund necesităţilor: a) respectării drepturilor şi reputaţiei altei persoane; b) protecţiei securităţii naţionale, ordinii publice, ocrotirii sănătăţii sau protecţiei moralei societăţii.”[1991]

Făcând o paralelă, putem afirma că, prin „informaţie protejată de lege” în sensul lit. g) alin. (2) art. 259 CP RM, se înțelege informația a cărei accesare este supusă restricţiilor reglementate prin lege. Acestei abordări îi corespund următoarele categorii de informații: informaţiile referitoare la boală, la viaţa intimă şi familială (în accepția alin. (1) art. 14 al Legii nr. 411 din 28.03.1995 a ocrotirii sănătăţii[1992]); informaţiile despre tulburările psihice, despre solicitarea de

[1979] Ibidem.
[1980] Ibidem.
[1981] Ibidem.
[1982] Ibidem.
[1983] Ibidem.
[1984] Ibidem.
[1985] Ibidem.
[1986] Ibidem.
[1987] Ibidem.
[1988] Ibidem.
[1989] Ibidem.
[1990] Ibidem.
[1991] Ibidem.
[1992] Legea ocrotirii sănătăţii: nr. 411 din 28.03.1995. În: *Monitorul Oficial al Republicii Moldova*, 1995, nr. 34, 373.

asistenţă psihiatrică şi tratament într-o instituţie de psihiatrie, precum şi alte informaţii despre starea sănătăţii psihice a persoanei (în sensul art. 9 al Legii nr. 1402 din 16.12.1997 privind sănătatea mentală[1993]); informaţia cunoscută de persoanele, care practică activitate particulară de detectiv şi de pază, în procesul activității acestora (în sensul lit. e) alin. (1) art. 8 al Legii nr. 283 din 04.07.2003 privind activitatea particulară de detectiv şi de pază[1994]), etc.

În dispoziția de la lit. g) alin. (2) art. 259 CP RM sunt avute în vedere informațiile protejate de *lege*. Cum ar trebui de interpretat termenul „lege" în acest context? Răspunsul la această întrebare este important în vederea stabilirii sferei de aplicare a lit. g) alin. (2) art. 259 CP RM și, implicit, a cercului de victime ale faptei prevăzute de această normă. Conform alin. (1) art. 8 al Legii nr. 100 din 22.12.2017 cu privire la actele normative, „legea este un act normativ adoptat de Parlament în temeiul normelor constituţionale, conform procedurii stabilite de Constituţia Republicii Moldova"[1995], „de Regulamentul Parlamentului, aprobat prin Legea nr. 797/1996, precum şi de prezenta lege".[1996] De asemenea, în pct. 94 din Hotărârea Curții Constituționale nr. 33 din 07.12.2017 privind excepţia de neconstituţionalitate a unor prevederi din articolele 327 alin. (1) și 361 alin. (2) lit. d) din Codul penal, se menționează: „[...] conceptul de lege poate fi înțeles doar ca act adoptat de Parlament în temeiul art. 72 din Constituție".[1997]

Din considerentele sus-menționate, nu putem aplica lit. g) alin. (2) art. 259 CP RM în cazul când se accesează ilegal informațiile computerizate protejate de actele normative care nu au caracter de lege: informațiile care se prelucrează şi se păstrează la Prestatorul superior (în sensul pct. 139 din anexa nr. 2 Ordinul SIS nr. 70 din 15.07.2016 cu privire la aprobarea unor acte normative în domeniul organizării funcţionării prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice[1998]); informaţiile ce ţin de tranzacţiile încheiate sau tranzacțiile în curs de desfășurare (în sensul subpct. 5) pct. 111 din Hotărârea BNM nr. 170 din 19.07.2018 cu privire la aprobarea Regulamentului cu privire la plasarea, tranzacționarea şi răscumpărarea

---

[1993] Legea privind sănătatea mentală: nr. 1402 din 16.12.1997. În: *Monitorul Oficial al Republicii Moldova*, 1998, nr. 44-46, 310.
[1994] Legea privind activitatea particulară de detectiv şi de pază: nr. 283 din 04.07.2003. În: *Monitorul Oficial al Republicii Moldova*, 2003, nr. 200-203, 769.
[1995] Legea cu privire la actele normative: nr. 100 din 22.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 7-17, 34.
[1996] Ibidem.
[1997] Hotărârea Curții Constituționale privind excepţia de neconstituţionalitate a unor prevederi din articolele 327 alin. (1) și 361 alin. (2) lit. d) din Codul penal: nr. 33 din 07.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 27-32, 04.
[1998] Ordinul SIS cu privire la aprobarea unor acte normative în domeniul organizării funcţionării prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice: nr. 70 din 15.07.2016. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 27-32, 1202.

valorilor mobiliare de stat în formă de înscriere în cont[1999]), etc. Actele normative enumerate mai sus sunt adoptate în temeiul unor legi. Cu toate acestea ele nu au caracter de lege. Cu atât mai puțin, în ipoteza prevăzută de lit. g) alin. (2) art. 259 CP RM, nu trebuie considerată protejată de lege informaţia computerizată care circulă între autorităţile publice ale Republicii Moldova, între acestea și autorităţile altor state, importante pentru stat (în sensul Hotărârii Guvernului nr. 735 din 11.06.2002 cu privire la sistemele speciale de telecomunicaţii ale Republicii Moldova[2000]). În acest act normativ nici măcar nu este specificată o lege în temeiul căreia actul în cauză a fost adoptat.[2001]

În alt context, S. Brînza și V. Stati afirmă că „dacă se accesează ilegal informaţia computerizată protejată de lege, despre viaţa personală care constituie secretul personal ori familial al altei persoane, nu este exclus concursul”[2002] „dintre infracţiunea prevăzută de lit. g) alin. (2) art. 259 CP RM şi una din infracţiunile specificate la art. 177 CP RM.”[2003] În dispoziția de la lit. g) alin. (2) art. 259 CP RM se folosește noțiunea „informație protejată de lege”. În alin. (1) și (1^1) art. 177 CP RM se recurge la noțiunea „informaţiile ocrotite de lege despre viaţa personală, care constituie secretul personal sau familial al unei alte persoane.”[2004] Întrucât cele două noțiuni nu sunt echipolente, concluzia este: în situația când se accesează ilegal informaţia computerizată protejată de lege (iar această informație se referă la viaţa personală a victimei, constituind un secret personal sau familial al acesteia), informația dată fiind distrusă, deteriorată, modificată, blocată sau copiată, aceeași persoană poate apărea atât ca victimă a infracțiunii prevăzute la lit. g) alin. (2) art. 259 CP RM, cât și ca victimă a uneia dintre infracţiunile ce sunt specificate în alin. (1) sau (1^1) art. 177 CP RM.

Subliniem: persoana, vizată în informația computerizată distrusă, deteriorată, modificată, blocată sau copiată, poate fi „victimă a uneia dintre infracţiunile prevăzute la art. 259 CP RM numai dacă va avea calitatea de participantă la relațiile sociale ocrotite de acest articol”[2005] „(de

---

[1999] Hotărârea BNM cu privire la aprobarea Regulamentului cu privire la plasarea, tranzacționarea și răscumpărarea valorilor mobiliare de stat în formă de înscriere în cont: nr. 170 din 19.07.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 277-284, 1171.

[2000] Hotărârea Guvernului cu privire la sistemele speciale de telecomunicaţii ale Republicii Moldova: nr. 735 din 11.06.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 79-81, 833.

[2001] STRÎMBEANU, Alexandru. Victima secundară a infracțiunilor prevăzute la art. 259 din Codul penal. În: *Conferința științifică națională cu participare internațională dedicată aniversării a 75-a a Universității de Stat din Moldova „Integrare prin cercetare și inovare” (10-11 noiembrie 2021)*. Chișinău: CEP USM, 2021, pp. 6-8. ISBN 978-9975-152-48-8.

[2002] BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015, p. 538. 1300 p. ISBN 978-9975-53-470-3.

[2003] Ibidem, p. 538.

[2004] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

[2005] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.

exemplu, va avea calitatea de utilizator al informației computerizate distruse, deteriorate, modificate, blocate sau copiate).”[2006] În caz contrar, se va aplica doar alin. (1) sau (1^1) art. 177 CP RM.

2.5.7. Săvârșirea infracțiunii din motive de prejudecată

În conformitate cu Legea nr. 111 din 21.04.2022 pentru modificarea unor acte normative[2007] (în continuare – Legea nr. 111/2022), Codul penal al Republicii Moldova a fost completat, printre altele, cu art. 134^{21}. Acest articol conține definiția noțiunii „motive de prejudecată”, precum și anumite clarificări privind caracteristicile motivelor de prejudecată.

Necesitatea unei astfel de completări decurge implicit din următoarea opinie doctrinară: „Legislaţia penală actuală (se are în vedere legea penală dinaintea intrării în vigoare a Legii nr. 111/2022 – *n.a.*)” [2008] „stipulează „ura socială, naţională, rasială sau religioasă” ca principal motiv de părtinire”[2009]; „[...] Motivele de discriminare sunt incriminate [...] numai în circumstanţe adiacente pentru anumite infracţiuni, care contribuie considerabil la nivelul înalt de impunitate în domeniu”.[2010] În aceeași ordine de idei se înscrie viziunea lui S. Brînza și V. Stati: „Creșterea numărului de considerente, pe care se pot baza ideile preconcepute ale făptuitorului, a fost dictată de noile realități sociale”[2011]; „Noțiunea „ură socială, naţională, rasială sau religioasă” nu mai corespundea demult acestor realități”[2012]; „Pentru comparație, legiuitorii din alte state au reacționat mai prompt la necesitatea reflectării în legea penală a noilor realități sociale”.[2013]

Într-adevăr, posibilele modele de inspirație pentru art. 134^{21} CP RM pot fi găsite în legile penale ale altor state. Astfel, potrivit art. 132-76 CP RFr, „în cazurile prevăzute de lege, pedepsele aplicate pentru o crimă sau un delict sunt agravate atunci când infracţiunea este comisă din cauza apartenenţei”[2014] „sau neapartenenţei, reale sau presupuse, a victimei la o

---

[2006] Ibidem.
[2007] Legea pentru modificarea unor acte normative: nr. 111 din 21.04.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 164-169, 291.
[2008] *Manual anti-discriminare pentru judecători*. [citat 18.12.2020] Disponibil: https://cnajgs.md/uploads/asset/file/ro/419/Manual_Anti-Discriminare_pentru_Judecatori.pdf
[2009] Ibidem.
[2010] Ibidem.
[2011] BRÎNZA, Serghei, STATI, Vitalie. Rațiunea și efectele adoptării Legii nr. 111/2022. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 3-15. ISSN 1814-3199.
[2012] Ibidem.
[2013] Ibidem.
[2014] *Codul penal al Republicii Franceze*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Franta-RO.html

anumită etnie, naţiune, rasă sau religie”[2015]; „Circumstanţa agravantă definită la primul alineat este constituită atunci când infracţiunea este precedată, însoţită sau urmată de discuţii, înscrisuri, imagini, obiecte sau acte”[2016] „de orice natură ce aduc atingere onoarei sau respectului victimei sau unui grup de persoane din care face parte victima”[2017] „din cauza apartenenţei sau neapartenenţei lor, reale sau presupuse, la o anumită etnie, naţiune, rasă sau religie”.[2018] Conform art. 132-77 din același cod, „în cazurile prevăzute de lege, pedepsele [...] sunt agravate atunci când infracţiunea este comisă din cauza orientării sexuale a victimei” [2019]; „Circumstanţa agravantă definită la primul paragraf este realizată atunci când infracţiunea este precedată, însoţită sau urmată de discuţii, înscrisuri, folosiri de imagini sau obiecte”[2020] „sau acte de orice natură ce aduc atingere onoarei sau respectului victimei”[2021] „sau unui grup de persoane din care face parte victima din cauza orientării sexuale reale sau presupuse”.[2022] În corespundere cu art. 35 a CP RCi, „instanţa, în exercitarea atribuţiilor sale de a stabili şi de a aplica o pedeapsă, poate lua în considerare ca factor agravant motivaţia discriminării”[2023] „împotriva unui grup de persoane pe motive de rasă, culoare, origine naţională sau etnică, religie sau altă credinţă, descendenţă, orientare sau identitate sexuală”.[2024] Potrivit pct. 12) alin. 1 art. 60 CP RLi, „următoarele sunt considerate circumstanţe agravante: [...] fapta a fost săvârşită pentru a exprima ură faţă de un grup de persoane sau faţă de o persoană”[2025] „care aparţine acestuia pe motive de vârstă, sex, orientare sexuală, handicap, rasă, naţionalitate, limbă, descendenţă, statut social, religie, convingeri sau opinii”.[2026] Conform art. 83B CP RMa, „pedeapsa stabilită pentru orice infracţiune se majorează cu una până la două grade atunci când infracţiunea este agravată sau motivată în totalitate sau în parte”[2027] „de ura împotriva unei persoane sau grup din cauza sexului, identităţii sexuale, orientării sexuale, rasei, culorii, limbii, naţionalităţii sau originii etnice”[2028], „cetăţeniei, religiei sau opiniei politice sau de altă natură, în sensul alin. (3)-(6),

---

[2015] Ibidem.
[2016] Ibidem.
[2017] Ibidem.
[2018] Ibidem.
[2019] Ibidem.
[2020] Ibidem.
[2021] Ibidem.
[2022] Ibidem.
[2023] *Codul penal al Republicii Cipriote*. [citat 11.07.2022] Disponibil: codexpenal.just.ro/laws/Cod-Penal-CipruRO.html
[2024] Ibidem.
[2025] *Codul penal al Republicii Lituania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Lituania-RO.html
[2026] Ibidem.
[2027] *Codul penal al Republicii Malta*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Malta-RO.html
[2028] Ibidem.

inclusiv”.[2029] În conformitate cu pct. 4 art. 22 CP RSp, „sunt circumstanţe agravante: [...] comiterea delictului din motive rasiste, antisemite sau alt tip de discriminare cu privire la ideologia, religia sau convingerile victimei”[2030], „etnia, rasa sau naţionalitatea căreia îi aparţine, sexul sau orientarea sexuală, boala sau handicapul de care suferă victima”.[2031] Nu în ultimul rând, lit. d) § 140 CP RSl prevede că „motivaţia specifică înseamnă că o infracţiune a fost comisă [...] din cauza urii cauzate de naţionalitate, etnie, rasă ori culoare a pielii”.[2032]

2.5.8. Oportunitatea agravării răspunderii în cazul săvârșirii infracțiunii fie asupra unui sistem informatic care este parte integrantă a infrastructurii critice, fie în privința informației sensibile privind protecția infrastructurilor critice

În opinia noastră, este necesară completarea listei de circumstanțe agravante ale infracțiunilor prevăzute la art. 259 CP RM.

În acest sens, în pct. 10 al Anexei nr. 1 la Hotărârea Parlamentului Republicii Moldova nr. 134 din 19.07.2018 pentru aprobarea Strategiei naționale de apărare și a Planului de acțiuni privind implementarea Strategiei naționale de apărare pentru anii 2018-2022, se arată: „Ansamblul de ameninţări şi riscuri identificate în urma analizei mediului strategic de securitate la nivel internaţional”[2033], „regional şi naţional reprezintă elemente interdependente ale războiului hibrid, o formă de exprimare a războiului de nouă generaţie”[2034]; „Acest tip de război se evidenţiază printr-o formă specifică de manifestare, una care oscilează între spectrul convenţional şi cel neconvenţional al războiului”[2035], „creând efecte variate, greu de anticipat şi de contracarat. Totodată, acesta se caracterizează prin acţiuni diverse, de la utilizarea de trupe fără însemne de identificare”[2036] „sau acţiuni disimulate ale trupelor militare şi paramilitare pînă la acţiuni de propagandă, război informaţional şi *atacuri cibernetice* (evid. ns.).”[2037] În același context, trebuie să menționăm că, potrivit pct. 10 al Anexei la Legea nr. 299 din 21.12.2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova (în continuare –

[2029] Ibidem.
[2030] *Codul penal al Regatului Spaniei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Spania-RO.html
[2031] Ibidem.
[2032] *Codul penal al Republicii Slovace*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovacia-RO.html
[2033] Hotărârea Parlamentului Republicii Moldova pentru aprobarea Strategiei naționale de apărare și a Planului de acțiuni privind implementarea Strategiei naționale de apărare pentru anii 2018-2022: nr. 134 din 19.07.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 285-294, 441.
[2034] Ibidem.
[2035] Ibidem.
[2036] Ibidem.
[2037] Ibidem.

Legea nr. 299/2017), prin „amenințare hibridă de securitate” se înțelege „operațiunea subversivă și/sau de informație, condusă ori plasată sub comanda unor state, entități non-statale”[2038], „organizații, indivizi, care vizează, în mod special, slăbiciunile și vulnerabilitățile unei guvernări suverane, independente și integre.”[2039]

Privită dintr-un asemenea unghi, noțiunea „infrastructură critică” dobândește o semnificație care nu ar trebui neglijată de către legiuitor.

În această privință trebuie să menționăm că Comitetul Convenției Consiliului Europei privind criminalitatea informatică (în continuare – CCCECI) a pus la dispoziția statelor semnatare Îndrumări privind interpretarea Convenției de la Budapesta. În legătură cu noțiunea „infrastructură informatică critică”, în aceste Îndrumări se explică: „Infrastructurile critice pot fi definite ca sisteme și active, fizice sau virtuale, atât de vitale pentru o țară încât funcționarea necorespunzătoare, incapacitatea sau distrugerea lor”[2040] „ar avea un impact epuizant asupra securității și apărării naționale, securității economice, sănătății sau siguranței publice sau oricărei combinații a acestor aspecte”[2041]; „[...] Infrastructurile critice sunt adesea dirijate prin intermediul unor sisteme informatice [...]. În general, astfel de sisteme sunt cunoscute ca infrastructuri informatice critice”[2042]; „Potrivit unor surse private și guvernamentale, în fiecare an se înregistrează un număr mare, dar necunoscut, de atacuri asupra infrastructurilor informatice critice în întreaga lume”[2043]; „[...] Atât formele actuale, cât și cele viitoare de atacuri asupra infrastructurii informatice critice sunt acoperite de următoarele articole ale Convenției”[2044], „în funcție de caracterul atacului: [...] Articolul 2 „Accesarea ilegală”: atacurile la infrastructura informatică critică pot presupune accesarea unui sistem informatic”.[2045]

Într-un alt act normativ nu mai puțin important, și anume în Directiva 2008/114/CE a Consiliului din 08.12.2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora (în continuare – Directiva 2008/114/CE), în art. 2 atrag atenția următoarele definiții: „(a) „infrastructură critică” înseamnă un element, un sistem sau o componentă a acestuia, aflat pe teritoriul statelor membre”[2046], „care

---

[2038] Legea privind aprobarea Concepției securității informaționale a Republicii Moldova: nr. 299 din 21.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 48-57, 122.
[2039] Ibidem.
[2040] *T-CY Guidance Notes*. [citat 18.12.2020] Disponibil: https://rm.coe.int/16802e7132
[2041] Ibidem.
[2042] Ibidem.
[2043] Ibidem.
[2044] Ibidem.
[2045] Ibidem.
[2046] *Directiva 2008/114/CE a Consiliului din 08.12.2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32008L0114

este esențial pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor”[2047], „și a căror perturbare sau distrugere ar avea un impact semnificativ într-un stat membru ca urmare a incapacității de a menține respectivele funcții”[2048]; „[...] (d) „informații sensibile privind protecția infrastructurilor critice” înseamnă informații cu privire la o infrastructură critică ce ar putea fi utilizate, în cazul divulgării”[2049], „în scopul planificării și al realizării unor acțiuni care să determine perturbarea sau distrugerea instalațiilor unor infrastructuri critice”[2050]; „[...] (e) „protecție” înseamnă orice activitate care are drept scop asigurarea funcționalității, a continuității” [2051] „și a integrității infrastructurilor critice pentru a descuraja, diminua și neutraliza o amenințare, un risc sau un punct vulnerabil; [...]”.[2052] Ultima noțiune definită – „protecție” – nu exclude aplicarea mijloacelor juridico-penale în vederea descurajării, diminuării și neutralizării unei amenințări, a unui risc sau unui punct vulnerabil în ceea ce privește informațiile sensibile (inclusiv în formă computerizată) privind protecția infrastructurilor critice.

În acest context, V. Țurcanu și I. Rusu au dreptate când afirmă: „Republica Moldova dispune de o protecție limitată și fragmentată a infrastructurii critice. Stabilirea noilor reglementări privind infrastructura critică și securizarea acesteia”[2053], „trebuie să devină una din prioritățile cheie naționale și necesită a fi abordată sistemic prin adoptarea și implementarea unei legi-cadru”[2054] „cu privire la gestionarea și protecția infrastructurii critice naționale a Republicii Moldova”[2055]; „Un proiect de lege privind protejarea obiectelor de infrastructură esențială pentru asigurarea securității naționale și a ordinii publice”[2056], „deja se află în Parlamentul Republicii Moldova, fiind adoptat la sfârșitul lunii aprilie 2021 în prima lectură”[2057]; „Cel mai important pas va consta în generarea unei noi voințe politice care să impulsioneze implementarea reformelor în sectorul infrastructurii critice din Republica Moldova.”[2058] Într-adevăr, în vederea transpunerii Directivei 2008/114/CE, a fost elaborat Proiectul legii privind protejarea obiectelor de

[2047] Ibidem.
[2048] Ibidem.
[2049] Ibidem.
[2050] Ibidem.
[2051] Ibidem.
[2052] Ibidem.
[2053] ȚURCANU, Valeriu, RUSU, Iulian. *Protecția infrastructurii critice: o nouă prioritate a Republicii Moldova*. [citat 18.12.2020] Disponibil: ipre.md/2021/07/02/protectia-infrastructurii-critice-o-noua-prioritate-a-republicii-moldova-comentariu-de-valeriu-turcanu-si-iulian-rusu-ipn-md/
[2054] Ibidem.
[2055] Ibidem.
[2056] Ibidem.
[2057] Ibidem.
[2058] ȚURCANU, Valeriu, RUSU, Iulian. *Protecția infrastructurii critice: o nouă prioritate a Republicii Moldova*. [citat 18.12.2020] Disponibil: ipre.md/2021/07/02/protectia-infrastructurii-critice-o-noua-prioritate-a-republicii-moldova-comentariu-de-valeriu-turcanu-si-iulian-rusu-ipn-md/

infrastructură esențială pentru asigurarea securității naționale și a ordinii publice. Art. 2 al acestui proiect conține, între altele, următoarele două definiții: „Infrastructură esențială reprezintă un element, un sistem sau o componentă a acestuia, aflat pe teritoriul național”[2059], „care este esențial pentru menținerea funcțiilor esențiale ale statului și societății, a sănătății, siguranței, transportului, securității, bunăstării sociale ori economice a persoanelor”[2060] „și a cărei stare poate avea un impact semnificativ la nivel național ca urmare a incapacității de a menține aceste funcții”[2061]; „Informații sensibile privind protecția infrastructurii esențiale [...] reprezintă informații cu privire la o infrastructură esențială ce ar putea fi utilizate, în cazul divulgării”[2062], „în scopul planificării și al realizării unor acțiuni de perturbare sau distrugere a unui element, sistem sau componentă de infrastructură esențială.”[2063]

Cu regret, acest proiect de lege nu a fost adoptat. Mai mult decât atât, nu sunt deloc clare perspectivele adoptării unui astfel de proiect.

Lipsa în legislația Republicii Moldova a unei legi, care ar transpune prevederile Directivei 2008/114/CE, este compensată într-o anumită măsură de existența unor reglementări care, în mod direct sau indirect, se referă la protecția infrastructurii critice și la informațiile sensibile privind protecția infrastructurilor critice. Astfel, în subpct. 8) pct. 2 din Hotărârea Guvernului nr. 811 din 29.11.2015 cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020 este formulată următoarea definiție: „infrastructuri cibernetice de interes național (ICIN) – infrastructuri cibernetice care susțin servicii publice sau de interes public”[2064], „precum și servicii ale societății informaționale a căror afectare poate aduce atingere securității naționale ori prejudicii grave statului sau cetățenilor acestuia.”[2065] Mai relevante însă sunt următoarele definiții din pct. 4 al Hotărârii Guvernului nr. 701 din 11.07.2018 pentru aprobarea Regulamentului privind protecția antiteroristă a infrastructurii critice: „Nomenclatorul național al infrastructurii critice (în continuare – Nomenclator) – lista obiectivelor infrastructurii critice, elaborată în conformitate cu criteriile subsectoriale și tipologia specifică. Nomenclatorul este gestionat de Centrul Antiterorist al Serviciului de Informații și Securitate al Republicii

---

[2059] *Proiectul legii privind protejarea obiectelor de infrastructură esențială pentru asigurarea securității naționale și a ordinii publice*. [citat 18.12.2020] Disponibil: https://www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/5019/language/ro-RO/Default.aspx
[2060] Ibidem.
[2061] Ibidem.
[2062] Ibidem.
[2063] Ibidem.
[2064] Hotărârea Guvernului cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020: nr. 811 din 29.11.2015. În: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 306-310, 905.
[2065] Ibidem.

Moldova”[2066]; „obiectiv al infrastructurii critice – obiectiv de importanţă vitală din domeniul administraţiei publice, tehnologiei informaţiei şi comunicaţiilor electronice şi poştale, de infrastructură, energetică”[2067], „din sfera social-economică, sănătăţii, cultural-educativă, industrială, ecologică, din sistemul informaţional al ţării în ansamblu, din infrastructura complexului militar şi de apărare al organelor de forţă”[2068], „de perturbarea sau distrugerea căruia poate provoca un impact negativ pentru siguranța, securitatea, bunăstarea socială”[2069] „și economică a statului, pierderi de servicii esențiale, pericol pentru viața, sănătatea oamenilor și efecte negative asupra mediului”[2070]; „servicii esențiale – servicii, facilități ori activități care sunt necesare pentru a asigura un standard minim de trai și bunăstare a societății și a căror degradare sau întrerupere a furnizării lor ar afecta semnificativ siguranța sau securitatea populației și funcționarea instituțiilor statului.”[2071]

Cu referire la actul normativ care conține aceste definiții, V. Sîli și I. Soroceanu menționează: „Regulamentul privind protecția antiteroristă a infrastructurii critice (aprobat prin Hotărârea Guvernului nr. 701 din 11.07.2018), reglementează doar procedura de identificare, desemnare și protecție antiteroristă a infrastructurii critice”.[2072] Acești autori lasă să se înțeleagă că sunt lipsite de apărare penală relațiile sociale ce apar și se dezvoltă în legătură cu: sistemele informatice care sunt părți integrante ale infrastructurii critice; informația sensibilă privind protecția infrastructurilor critice.

Între timp, art. 1 al Deciziei (PESC) 2019/797 a Consiliului din 17.05.2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre prevede la lit. (a) art. (4) prevede: „Printre atacurile cibernetice care constituie o amenințare pentru statele membre se numără cele care afectează sistemele informatice legate, printre altele, de: [...] infrastructura critică”[2073], „inclusiv cablurile submarine și obiectele lansate în spațiul cosmic, care sunt esențiale pentru menținerea funcțiilor vitale ale

[2066] Hotărârea Guvernului pentru aprobarea Regulamentului privind protecția antiteroristă a infrastructurii critice: nr. 701 din 11.07.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 277-284, 773.
[2067] Ibidem.
[2068] Ibidem.
[2069] Ibidem.
[2070] Ibidem.
[2071] Ibidem.
[2072] SÎLI, Vitalie, SOROCEANU, Igor. Protecţia infrastructurii critice în contextul asigurării securităţii naţionale. În: *Securitatea națională a Republicii Moldova: provocări și tendințe (14 mai 2022, Chișinău)*. Chișinău: Institutul naţional de informaţii şi securitate „Bogdan, întemeietorul Moldovei”, 2022, pp. 51-57.
[2073] *Decizia (PESC) 2019/797 a Consiliului din 17.05.2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32019D0797&from=RO

societății”[2074] „sau pentru sănătatea, siguranța, securitatea și bunăstarea economică sau socială a oamenilor; [...]”.[2075]

Nu oricare sistem informatic, ci doar cel de maximă importanță constituie obiectul material al unora dintre infracțiunile prevăzute de articolele care corespund ca esență cu art. 259 CP RM, care fac parte din legile penale ale statelor membre ale UE (de pildă, în § 118a CP RA[2076], în art. 319b CP RBu[2077], în § 217 CP RE[2078], în art. 615-ter CP RI[2079] și în art. 198[(1)] CP RLi[2080]). Nu oricare date informatice, ci doar datele informatice de o anumită categorie pot să reprezinte obiectul imaterial al unora dintre infracțiunile prevăzute de articolele care corespund ca esență cu art. 259 CP RM, care fac parte din legile penale ale statelor membre ale UE (de pildă, în art. 196 CP RLi[2081] și în art. 269 CP RP[2082]).

Aceste exemple prezintă interes pentru legea penală moldavă, mai ales dacă le privim prin prisma pct. 8 din Anexa la Legea nr. 299 din 21.12.2017 privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova: „Interesele naționale în domeniul securității informaționale sînt: asigurarea respectării drepturilor și libertăților privind accesul la resursele informaţionale”[2083]; „dezvoltarea domeniului tehnologiei informaţiei şi al comunicaţiilor electronice și sporirea utilizării acestora; *asigurarea protecţiei [...] infrastructurii critice* (evid. ns.)”[2084], „a informațiilor atribuite la secret de stat și a celor cu accesibilitate limitată; prevenirea, depistarea şi contracararea riscurilor şi ameninţărilor la adresa securității informaţionale”[2085] „a Republicii Moldova, precum şi protecția spațiului informațional național și a societății [...] de impactul propagandei și al agresiunii mediatice din exterior şi din interior.”[2086]

Urmare acestui fapt, considerăm oportună agravării răspunderii în cazul săvârșirii infracțiunilor, prevăzute la art. 259 CP RM, fie asupra unui sistem informatic care este parte

---

[2074] Ibidem.
[2075] Ibidem.
[2076] *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html
[2077] *Codul penal al Republicii Bulgaria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
[2078] *Codul penal al Republicii Estonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Estonia-RO.html
[2079] *Codul penal al Republicii Italia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Italia-RO.html
[2080] *Codul penal al Republicii Lituania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Lituania-RO.html
[2081] Ibidem.
[2082] *Codul penal al Republicii Polone*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Polonia-RO.html
[2083] Legea privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova: nr. 299 din 21.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 48-57, 122.
[2084] Ibidem.
[2085] Ibidem.
[2086] Ibidem.

integrantă a infrastructurii critice, fie în privința informației sensibile privind protecția infrastructurilor critice.

2.6. Sinteza problematicii tratate și a rezultatelor obținute în Capitolul 2

Considerăm necesară formularea anumitor concluzii după ce am efectuat analiza de drept penal a infracțiunilor prevăzute la art. 259 CP RM:

1) sintagma „infracţiuni în domeniul tehnologiilor informaţionale”, ca și sintagma „infracțiuni cibernetice”, nu sunt potrivite pentru a desemna grupul de infracțiuni prevăzute în Capitolul XI din partea specială a Codului penal al Republicii Moldova;

2) titlul Capitolului XI din partea specială a Codului penal demonstrează lipsa de congruență dintre prevederile legii penale autohtone și prevederile Convenției de la Budapesta;

3) în măsura în care asigură prin executarea unui program prelucrarea automată a datelor informatice, televizoarele inteligente, consolele Playstation, Xbox-ul, telefoanele mobile inteligente, imprimanta, faxul, scanerul sau alte asemenea dispozitive reprezintă sisteme informatice;

4) deoarece asigură prin executarea unui program prelucrarea automată a datelor informatice, bancomatul și terminalul de tip POS reprezintă sisteme informatice;

5) în măsura în care asigură prin executarea unui program prelucrarea automată a datelor informatice, cardul de plată reprezintă un sistem informatic. O asemenea ipoteză se atestă atunci când cardul de plată este introdus în bancomat, formând astfel un tandem cu acest sistem informatic;

6) în condițiile în care atacul cibernetic (care poate presupune accesul ilegal la informaţia computerizată) corespunde noțiunii de folosire a forței în sensul alin. 4 art. 2 din Carta ONU, statul atacat nu este victimă în sensul dreptului penal al Republicii Moldova. Într-un asemenea caz, victime pot fi persoanele (fizice sau juridice) care participă la relațiile sociale apărate împotriva infracțiunilor prevăzute la art. 259 CP RM. Statul atacat poate fi considerat victimă numai în sensul dreptului penal internațional;

7) infracțiunea are o singură victimă în cazul în care aceeași persoană este atât proprietarul, alt posesor sau utilizatorul informaţiilor computerizate accesate ilegal, cât și proprietarul sau alt posesor al informației distruse, deteriorate, modificate, blocate sau copiate, ori al calculatorului, al sistemului informatic sau al reţelei informatice, ale căror funcționare a fost dereglată. În alte cazuri, proprietarul, alt posesor sau utilizatorul informaţiilor computerizate accesate ilegal poate fi altcineva decât proprietarul sau alt posesor al calculatorului, al sistemului informatic sau al

reţelei informatice, ale căror funcționare a fost dereglată. Doar în aceste din urmă cazuri, putem vorbi despre prezența victimei principale și a victimei secundare;

8) indiferent de modalitatea faptică sub care se înfățișează accesul la un sistem informatic, trebuie să stabilim dacă acest acces a avut o continuitate, astfel încât să putem vorbi despre accesul la informația computerizată din acel sistem. Doar într-un asemenea caz putem vorbi despre accesul la informația computerizată în accepția art. 259 CP RM;

9) indiferent de modalitatea faptică sub care se înfățișează accesul la un calculator, la un suport material de informaţie ori la o rețea informatică – trebuie să stabilim dacă acest acces a avut o continuitate, astfel încât să putem vorbi despre accesul la informația computerizată din acel calculator, din acel suport material de informaţie ori din acea reţea informatică. În lipsa unei astfel de continuități, nu putem vorbi despre accesul la informația computerizată în accepția art. 259 CP RM;

10) persoana, care realizează accesul la informația computerizată, nu este pasibilă de răspundere în baza art. 259 CP RM în oricare din următoarele cazuri: a) este autorizată în temeiul legii sau al unui contract; b) nu depășește limitele autorizării; c) are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic;

11) în art. 259 CP RM este incriminat nu pur și simplu accesul ilegal la informaţia computerizată, ci accesul ilegal la informaţia computerizată însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, dacă, în rezultat, s-au produs daune în proporţii mari / deosebit de mari;

12) nu este întemeiat să reținem concursul ideal dintre una din infracțiunile, ce sunt specificate în art. 259 CP RM, și una din infracțiunile care sunt prevăzute de art. 260^2 sau 260^3 CP RM. Aceeași distrugere, deteriorare, modificare, blocare sau copiere a informaţiei ori dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice nu trebuie calificată în baza a două articole;

13) ștergerea sau eliminarea informaţiei computerizate nu pot să reprezinte exemple care decurg din noțiunea „distrugerea informaţiei computerizate”, folosite în art. 259 CP RM;

14) noțiunea „distrugerea informaţiei computerizate”, folosită în art. 259 CP RM, poate fi reprezentată numai de distrugerea sau deteriorarea calculatorului, a suportului material de informaţie, a sistemului informatic sau a reţelei informatice, care are ca efect distrugerea informației computerizate ce se afla în acel calculator, pe acel suport material de informaţie, în

acel sistem informatic sau în acea reţea informatică. În aceste condiții, art. 259 CP RM trebuie aplicat împreună cu art. 197 CP RM sau cu art. 104 CC RM;

15) noțiunea „deteriorarea informaţiei computerizate”, folosită în art. 259 CP RM, poate fi reprezentată numai de deteriorarea calculatorului, a suportului material de informaţie, a sistemului informatic sau a reţelei informatice, care are ca efect deteriorarea informației computerizate ce se afla în acel calculator, pe acel suport material de informaţie, în acel sistem informatic sau în acea reţea informatică. În asemenea împrejurări, art. 259 CP RM trebuie aplicat împreună cu art. 197 CP RM sau cu art. 104 CC RM;

16) în art. 259 CP RM, prin „copierea informației computerizate” se are în vedere copierea logică a informației computerizate (care presupune folosirea unui program de calculator), nu copierea fizică a acesteia (de exemplu: reproducerea manuală; reproducerea prin fotografierea textului sau a imaginii de pe ecranul calculatorului etc.);

17) reproducerea în creierul uman prin memorare a unei informații văzute, auzite sau altfel percepute nu formează conținutul noțiunii „copierea informației computerizate”, folosite în art. 259 CP RM;

18) condiția esențială pentru atestarea copierii informației computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, este ca informația computerizată copiată să fie stocată într-un alt calculator, pe un alt suport material de informaţie, într-un alt sistem informatic sau într-o altă reţea informatică, decât cel/cea pe care se păstra informația computerizată originală;

19) este posibil ca: a) la același calculator, la același suport material de informaţie, la același sistem informatic sau la aceeași reţea informatică să aibă acces două ori mai multe persoane; b) totodată, să fie restricționat accesul pentru una sau unele dintre aceste persoane la o parte a unui astfel de calculator, suport material de informaţie sau sistem informatic ori a unei astfel de reţele informatice. Într-o asemenea situație, pentru a aplica art. 259 CP RM, informația computerizată copiată trebuie să fie stocată în acea parte din calculator, din suportul material de informaţie, din sistemul informatic sau din reţeaua informatică, la care nu are acces victima;

20) copierea informației computerizate, dacă nu produce daune în proporții mari sau deosebit de mari și dacă nu este precedată de accesul ilegal la acea informație, poate să reprezinte pregătirea de infracțiunile care presupun divulgarea anumitor informații (de exemplu, pregătirea de infracțiunile prevăzute la art. 204, alin. (1) art. 315, art. 316, 337, 344 etc. din Codul penal). În asemenea cazuri, nu este necesară aplicarea art. 259 CP RM;

21) nu este oportun ca în art. 259 CP RM să existe o dispoziție aparte în care ar fi stabilită răspunderea pentru tentativa la infracțiunile prevăzute de acest articol;

22) spre deosebire de tentativa la infracțiune, pregătirea de infracțiune nu presupune începerea executării faptei prejudiciabile. În cazul infracțiunilor prevăzute la art. 259 CP RM, aceasta înseamnă că, din cauze ce nu depind de voința făptuitorului, nu începe executarea acțiunii principale de acces ilegal la informația computerizată;

23) urmările prejudiciabile, prevăzute la art. 259 CP RM, trebuie să fie legate cauzal de acțiunea adiacentă de distrugere, deteriorare sau modificare a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, nu de acțiunea principală de acces ilegal la informația computerizată. Acțiunea principală de acces ilegal la informația computerizată nu poate, de una singură, să constituie cauza producerii urmărilor prejudiciabile ce sunt specificate în art. 259 CP RM;

24) incertitudinile cu privire la forma de vinovăție în cazul infracțiunilor, ce sunt prevăzute de art. 259 CP RM, ar putea să fie depășite pe calea completării Codului penal al Republicii Moldova cu o prevedere de genul celei din alin. (6) art. 16 CPR, al alin. (1) § 7 CP RA și al art. 13 din Codul penal al Republicii Portugheze;

25) nu este oportună reducerea vârstei minime a răspunderii pentru infracțiunile care sunt prevăzute de art. 259 CP RM;

26) persoanele, care nu răspund penal datorită vârstei, iresponsabilității etc., nu se au în vedere în dispoziția de la lit. b) alin. (2) art. 259 CP RM;

27) este oportun ca violarea măsurilor de securitate să devină condiția obligatorie pentru existența variantei-tip a faptei prevăzute la art. 259 CP RM;

28) prin „informaţie protejată de lege” în sensul lit. g) alin. (2) art. 259 CP RM, se înțelege informația a cărei accesare este supusă restricţiilor reglementate prin lege, nu și prin actele normative care nu au caracter de lege.

3. REZULTATELE OBȚINUTE ÎN URMA ANALIZEI DE DREPT PENAL A INFRACȚIUNILOR PREVĂZUTE LA ART. 259 CP RM

3.1. Rezultatele obținute în urma analizei de drept penal a obiectului infracțiunilor prevăzute la art. 259 CP RM

Din alin. (1) art. 2 CP RM deducem că incriminarea faptelor, prevăzute la art. 259 CP RM, urmărește, în ultimă instanță, apărarea ordinii de drept. Ordinea de drept este valoarea socială generală, care este protejată împotriva tuturor infracțiunilor prevăzute de partea specială a Codului penal al Republicii Moldova. Nu este posibil ca obiectul juridic general să fie comun doar pentru un grup de infracțiuni. Concretizarea primară a obiectului juridic general se realizează tocmai prin stabilirea obiectului juridic generic. În partea specială a Codului penal al Republicii Moldova, componențele de infracțiuni sunt grupate în capitole, în funcție de obiectul juridic generic. Așadar, obiectul juridic generic reprezintă factorul unificator pentru un grup de infracțiuni prevăzute de un capitol anumit al părții speciale a Codului penal al Republicii Moldova.

Pe cale de consecință, urmând principiul „de la general la particular", analiza obiectului juridic al infracțiunilor, ce sunt prevăzute de art. 259 CP RM, trebuie să înceapă cu examinarea obiectului juridic generic al infracțiunilor ce sunt prevăzute în Capitolul XI al părții speciale a Codului penal.

Din titlul Capitolului XI al părții speciale a Codului penal al Republicii Moldova – „Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor"[2087] – deducem că informatica și telecomunicațiile reprezintă perechea de valori sociale fundamentale, care sunt protejate contra infracțiunilor prevăzute în acest capitol. Astfel, *de lege lata,* obiectul juridic generic al grupului infracțiunilor, care sunt specificate în Capitolul XI al părții speciale a Codului penal, poate fi format doar din relaţiile sociale din domeniul informaticii şi al telecomunicaţiilor. *De lege ferenda*, acest obiect ar putea avea un alt conținut.

În această ordine de idei, enunțăm ipoteza, conform căreia titlul „Infracţiuni contra securității datelor informatice şi a comunicaţiilor electronice" este potrivit pentru a deveni titlul Capitolului XI din partea specială a Codului penal. În rândurile de mai jos vom verifica validitatea acestei ipoteze.

[2087] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

În primul rând, de ce propunem sintagma „infracţiuni contra securității datelor informatice” în locul sintagmei „infracțiuni informatice”?

Această inițiativă este determinată de lipsa de congruență dintre prevederile legii penale autohtone și prevederile Convenției de la Budapesta. În Capitolul II „Măsuri care trebuie luate la nivel naţional” al Convenției de la Budapesta, Secţiunea 1 „Drept penal material” conține, printre altele, două titluri:

– Titlul 1 „Infracţiuni împotriva confidenţialităţii, integrităţii şi disponibilităţii datelor şi sistemelor informatice”[2088];

– Titlul 2 „Infracţiuni informatice”[2089].

Primul dintre aceste titluri cuprinde: art. 2 „Accesarea ilegală”; art. 3 „Interceptarea ilegală”; art. 4 „Afectarea integrităţii datelor”; art. 5 „Afectarea integrităţii sistemului”; art. 6 „Abuzurile asupra dispozitivelor”.

La rândul său, Titlul 2 cuprinde: art. 7 „Falsificarea informatică”; art. 8 „Frauda informatică”.

Fiecare dintre aceste articole ale Convenției de la Budapesta corespund anumitor articole din Capitolul XI al părții speciale a Codului penal. În pofida acestui fapt, sintagma „infracțiuni informatice”, folosită în titlul Capitolului XI al părții speciale a Codului penal, reflectă prezența în acest capitol doar a articolelor care corespund art. 7 și 8 ale Convenției de la Budapesta. Din această sintagmă nu rezultă prezența în Capitolul XI din partea specială a Codului penal a unor articole care ar corespunde art. 2-6 ale Convenției de la Budapesta.

Cât privește noțiunea „securitatea datelor”, aceasta este definită în art. 2 al Legii nr. 1069/2000: „atribut al datelor ce caracterizează siguranţa lor faţă de evenimente ce le-ar putea afecta integralitatea.”[2090] Noțiunea derivată „date” este definită în același articol: „fapte, noţiuni, fenomene, evenimente, însuşiri, indici, instrucţiuni etc.”[2091], „reprezentate sub o formă convenţională, adecvată comunicării, interpretării sau prelucrării manuale ori cu mijloace automate.”[2092] Conform art. 2 al Legii nr. 20/2009, prin „date informatice” se înțelege „orice reprezentare de fapte, informaţii sau concepte sub o formă adecvată prelucrării într-un sistem informatic”[2093], „inclusiv un program capabil să determine executarea unei funcţii de către un

[2088] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[2089] Ibidem.
[2090] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[2091] Ibidem.
[2092] Ibidem.
[2093] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.

sistem informatic”.[2094] Sub acest aspect, noțiunea „securitatea datelor informatice”, având un suport legislativ, este clară și previzibilă.

Un alt argument ar fi recurgerea la noțiuni apropiate în legile penale ale altor state. De pildă, în Codul penal al României din 2004, Titlul X se numea „Delicte contra datelor și sistemelor informatice”.[2095] În Codul penal al României din 2009, Titlul VII „Infracțiuni contra siguranței publice” conține Capitolul VI „Infracțiuni contra siguranței și integrității sistemelor și datelor informatice”.[2096] În Codul penal al Republicii Croaţia, Capitolul XXV poartă titlul „Infracţiuni împotriva sistemelor, programelor şi datelor informatice”.[2097] În Codul penal al Republicii Lituania, Capitolul XXX se numește „Infracţiunile împotriva securităţii datelor electronice şi a sistemelor de informaţii”.[2098] Nu în ultimul rând, în Codul penal al Republicii Finlanda, Capitolul 38 poartă titlul „Infracţiuni privitoare la date şi comunicaţii”.[2099]

Noțiunea „date informatice” este primară în raport cu noțiunile derivate „sisteme informatice” și „programe informatice”. Sistemele informatice și programele informatice își pierd semnificația în lipsa datelor informatice. Din aceste considerente, sintagma „infracţiuni contra securității datelor informatice” (pe care o propunem pentru o parte din titlul Capitolului XI al părții speciale a Codului penal al Republicii Moldova) este preferabilă în comparație cu sintagmele utilizate în legile penale străine exemplificate mai sus.

Din definiția noțiunii „securitatea datelor”, formulată în art. 2 al Legii nr. 1069/2000, rezultă că integralitatea datelor informatice este o caracteristică inerentă a securității datelor informatice. Din aceste considerente, sintagma „infracţiuni contra securității datelor informatice” este preferabilă în comparație cu sintagma „infracțiuni contra siguranței și integrității sistemelor și datelor informatice”[2100], folosită în Codul penal al României din 2009.

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

[2094] Ibidem.
[2095] Codul penal al României: nr. 301 din 28.06.2004. În: *Monitorul Oficial al României*, 2004, nr. 575.
[2096] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
[2097] *Codul penal al Republicii Croaţia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Croatia-RO.html
[2098] *Codul penal al Republicii Lituania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Lituania-RO.html
[2099] *Codul penal al Republicii Finlanda*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Finlanda-RO.html
[2100] Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.

260^3, 260^5 și 260^6 CP RM). Cât privește infracțiunile prevăzute la art. 260 și 260^4 CP RM, acestea reprezintă exemple de pregătire de infracțiunile prevăzute la art. 259, 260^1-260^3, 260^5, 260^6 și 261 CP RM, incriminate din considerente de politică penală ca fapte distincte. În ipoteza faptelor infracționale ce sunt prevăzute de art. 260 și 260^4 CP RM, vorbim despre crearea intenționată de condiții pentru influenţarea directă asupra datelor informatice.

Sintagma „infracţiuni contra securității datelor informatice" (pe care o propunem pentru o parte din titlul Capitolului XI al părții speciale a Codului penal al Republicii Moldova) este preferabilă în comparație cu sintagmele „delicte contra datelor și sistemelor informatice", „infracţiuni împotriva sistemelor, programelor şi datelor informatice", și „infracţiuni privitoare la date şi comunicaţii", utilizate în legile penale prezentate mai sus cu titlu de exemplu. Or, legea penală protejează nu datele informatice în sine, care reprezintă obiectul imaterial al infracțiunii, ci securitatea acestor date, care constituie o valoare socială.

În viziunea lui N. Postovanu, „în partea specială a Codului penal, termenul „securitate" este folosit expres în denumirea Capitolului I „Infracţiuni contra păcii şi securităţii omenirii, infracţiuni de război""[2101], „a Capitolului XIII „Infracţiuni contra securităţii publice şi a ordinii publice" și a Capitolului XVII „Infracţiuni contra autorităţilor publice şi a securităţii de stat""[2102]; „Securitatea omenirii constituie securitatea internațională. Securitatea publică, securitatea de stat și securitatea în transportul feroviar, naval, aerian și rutier reprezintă componente ale securității naționale".[2103] Definiția legislativă a noțiunii de securitate este formulată în pct. 1.2 din anexa la Legea nr. 112 din 22.05.2008 pentru aprobarea Concepţiei securităţii naţionale a Republicii Moldova, „Securitatea naţională nu este numai securitatea statului, ci şi securitatea societăţii şi a cetăţenilor Republicii Moldova, atât pe teritoriul Republicii Moldova, cât şi peste hotare"[2104]; „Securitatea naţională a Republicii Moldova se realizează prin măsuri adecvate de natură politică, economică, diplomatică, socială, juridică, educativă, administrativă şi militară, prin activitate de informaţii"[2105], „contrainformaţii, precum şi prin depăşirea eficientă a crizelor, în conformitate cu legislaţia în vigoare şi cu dreptul internaţional".[2106]

[2101] POSTOVANU, Nicolae. Obiectul juridic generic și obiectul juridic de subgrup al infracțiunilor prevăzute la art. 264 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Științe sociale"*, 2020, nr. 3, pp. 236-243. ISSN 1814-3199.
[2102] Ibidem.
[2103] Ibidem.
[2104] Legea pentru aprobarea Concepţiei securităţii naţionale a Republicii Moldova: nr. 112 din 22.05.2008. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 97-98, 357.
[2105] Ibidem.
[2106] Ibidem..

În contextul denumirii propuse de noi mai sus pentru Capitolul XI din partea specială a Codului penal, securitatea datelor informatice trebuie privită ca parte nu doar a securității naționale. O astfel de abordare ar fi prea îngustă. Având în vedere caracterul adesea transnațional al infracțiunilor ce sunt prevăzute în capitolul sus-menționat, sfera securității datelor informatice depășește deseori cadrul securității naționale, deci poate avea conotații supranaționale. Așadar, securitatea datelor informatice trebuie privită la nivel internațional, regional și național.

Nu este admisibilă confundarea noțiunilor „securitatea informațională" și „securitatea informatică (cibernetică)". Indiferent dacă sintagma „securitatea informațională" se referă la securitatea informațiilor sau la securitatea împotriva amenințărilor de ordin informațional, semantismul acesteia nu corespunde conceptului de „infracțiuni informatice" din titlul Capitolului XI din partea specială a Codului penal.

În altă ordine de idei, la nivel normativ, conceptul „telecomunicații" a fost substituit prin conceptul „comunicații electronice". Actuala denumire a Capitolului XI al părții speciale a Codului penal este anacronică, întrucât nu ține cont de această substituire.

Prin „comunicații electronice" se înțelege comunicațiile care alcătuiesc reţeaua de comunicaţii electronice. Această concluzie reiese din art. 2 al Legii nr. 241/2007. În același timp, noțiunea „securitatea comunicațiilor electronice" derivă din noțiunea „securitatea rețelelor și serviciilor de comunicații electronice", definită în alin. 21 art. 2 al Directivei (UE) 2018/1972 a Parlamentului European și a Consiliului din 11.12.2018 de instituire a Codului european al comunicațiilor electronice.[2107] Interpretând aceste prevederi, putem afirma că securitatea comunicațiilor electronice înseamnă starea de lipsă de pericole pentru aceste comunicații, implicând protecția lor împotriva unor pericole. Pe o asemenea cale se asigură protecția intereselor persoanei, ale societății și ale statului împotriva unor amenințări de ordin interne sau extern. Având în vedere caracterul acestor amenințări, securitatea comunicațiilor electronice, ca și securitatea datelor informatice, trebuie privită la nivel internațional, regional și național.

În acest mod, am stabilit validitatea ipotezei, conform căreia titlul „Infracţiuni contra securității datelor informatice şi a comunicaţiilor electronice" este potrivit pentru Capitolul XI din partea specială a Codului penal. În afară de aceasta, am determinat că relațiile sociale cu privire la securitatea datelor informatice şi a comunicaţiilor electronice prezintă suficientă semnificație sub aspect axiologic, astfel încât să fie pasibile de apărare penală.

[2107] *Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11.12.2018 de instituire a Codului european al comunicațiilor electronice*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32018L1972&from=ro

Oricare relație socială presupune interacționarea, relaționarea a doi sau mai multor subiecți. O relație este socială în virtutea legăturii dintre membrii societății, care îndeplinesc rolul de participanți în cadrul respectivei relații. Dacă lipsesc subiecții relației sociale, atunci lipsește relația socială însăși. Subiecții relațiilor sociale cu privire la securitatea datelor informatice şi a comunicaţiilor electronice sunt statul Republica Moldova, alte state, persoanele fizice sau persoanele juridice din Republica Moldova sau din alte state, care participă la respectivele relații sociale.

Conținutul relațiilor sociale cu privire la securitatea datelor informatice şi a comunicaţiilor electronice îl reprezintă drepturile subiective și/sau obligațiile corelative ale subiecților acestor relații sociale.

În fine, conduita subiecților relației sociale constituie obiectul acestei relații. Drepturile subiective sunt exercitate, iar obligațiile corelative sunt executate doar în contextul unui comportament activ. Totodată, drepturile subiective nu sunt exercitate (deși trebuiau și puteau să fie exercitate), iar obligațiile corelative nu sunt executate (deși trebuiau și puteau să fie executate) doar în contextul unui comportament pasiv.

În concluzie, relațiile sociale cu privire la securitatea datelor informatice şi a comunicaţiilor electronice au o structură completă, suficientă, care le face susceptibile de apărare penală.

Obiectul juridic al infracțiunii, în general, și obiectul juridic special al infracțiunii, în particular, nu pot fi percepute în mod nemijlocit de cei care aplică legea penală. Totodată, așa cum rezultă din art. 15, 50-52 și 113 CP RM, identificarea obiectului juridic special al infracțiunii este indispensabilă în procesul de calificare a oricărei infracțiuni. În acest plan, infracțiunile, prevăzute la art. 259 CP RM, nu constituie o excepție.

Să nu uităm că art. 259 CP RM prevede răspunderea pentru două infracțiuni. În cazul infracțiunilor ce sunt prevăzute la alin. (1) și lit. h) alin. (2) art. 259 CP RM, proporțiile daunelor cauzate reprezintă factorul ce le particularizează una în raport cu cealaltă. Mărimea categorisită legalmente a acestor proporții – mare sau deosebit de mare – determină gradul de gravitate a pericolului care amenință obiectul juridic special al infracțiunilor analizate. Din această cauză, valoarea socială și relațiile sociale alăturate afectate în rezultatul comiterii infracțiunii prevăzute la alin. (1) art. 259 CP RM, presupunând cauzarea daunelor în proporții mari, nu pot să coincidă cu valoarea socială și relațiile sociale aferente, care sunt afectate în rezultatul săvârșirii infracțiunii prevăzute la lit. h) alin. (2) art. 259 CP RM. Or, în cazul acestei din urmă infracțiuni, se cauzează daune în proporții deosebit de mari.

Așa cum s-a relevat anterior, regula este că obiectul juridic special decurge, rezultă, se desprinde din obiectul juridic generic. Informatica și telecomunicațiile reprezintă perechea de

valori sociale fundamentale, care sunt protejate contra infracțiunilor prevăzute în Capitolul XI din partea specială a Codului penal al Republicii Moldova. Ceea ce înseamnă că obiectul juridic special al infracțiunilor, prevăzute la art. 259 CP RM, trebuie să decurgă din relaţiile sociale din domeniul informaticii şi al telecomunicaţiilor.

Particularizând, este necesar să constatăm că denumirea art. 259 CP RM – „Accesul ilegal la informaţia computerizată" – sugerează că informatica este domeniul de relații sociale de care aparține obiectul juridic special al infracțiunilor, prevăzute la art. 259 CP RM. Această ipoteză este valabilă cu condiția că infracțiunile analizate sunt uniobiectuale. În ipoteza în care ele sunt biobiectuale, obiectul juridic principal trebuie este cel care se desprinde din relațiile sociale din domeniul informaticii.

Considerăm că infracțiunile, care sunt specificate în art. 259 CP RM, sunt biobiectuale. Despre aceasta ne vorbește structura faptei prejudiciabile specificate în acest articol. Astfel, fapta prejudiciabilă analizată include două componente:

1) acţiunea principală de acces ilegal la informaţia computerizată;

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

Astfel, acţiunea principală aduce atingere obiectului juridic principal al infracțiunilor prevăzute la art. 259 CP RM, pe când acţiunea adiacentă aduce atingere obiectului juridic secundar al acestor infracțiuni.

Cât privește obiectul juridic principal, acesta urmează a fi stabilit pe baza interpretării titlului art. 259 CP RM, precum și a acelei părți din dispoziția alin. (1) art. 259 CP RM în care este descrisă acțiunea principală: „accesul ilegal la informaţia computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică [...]."[2108] Din interpretarea acestor elemente ale art. 259 CP RM se poate deduce că, incriminând faptele reunite sub denumirea marginală de acces ilegal la informaţia computerizată, legiuitorul urmărește să stabilească un echilibru rezonabil între dreptul unor persoane de a accesa în mod liber informația computerizată și dreptul altor persoane de a nu permite accesul ilegal la o asemenea informație. Pe cale de consecință, obiectul juridic principal al infracțiunilor prevăzute la art. 259 CP RM îl formează relaţiile sociale cu privire la accesul autorizat sau permis la informaţia computerizată. Acest obiect este același pentru ambele infracțiuni specificate în art. 259 CP RM.

[2108] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

Obiectul juridic secundar al infracțiunilor prevăzute la art. 259 CP RM îl constituie „relaţiile sociale cu privire la integritatea, autenticitatea, disponibilitatea sau ireproductibilitatea informației computerizate ori funcționalitatea calculatoarelor, a sistemului sau a reţelei informatice”[2109], „apărate împotriva cauzării de:

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

2) daune în proporții deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2)).”[2110]

Astfel, datorită diferenței ce caracterizează urmările prejudiciabile ale infracțiunilor prevăzute la alin. (1) și lit. h) alin. (2) art. 259 CP RM, diferă obiectul juridic secundar al acestora.

În cazul infracțiunilor prevăzute la art. 259 CP RM, nici acțiunea principală, nici acțiunea adiacentă nu reprezintă de felul lor infracțiuni. În partea specială a Codului penal al Republicii Moldova nu există norme în care ar fi incriminate distinct fie accesul ilegal la informaţia computerizată, fie distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei ori dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice.

Concluzia noastră este următoarea: noțiunea de infracțiune biobiectuală se intersectează cu noțiunea de infracțiune complexă, fără însă a se echivala cu această noțiune. De aceea, infracțiunea biobiectuală, ca și infracțiunea complexă, reprezintă tipuri distincte de infracțiuni unice. Infracțiunile, prevăzute la art. 259 CP RM, sunt infracțiuni biobiectuale, însă nu sunt infracțiuni complexe.

În altă ordine de idei, sintagma „accesul ilegal la informaţia computerizată” din art. 259 CP RM indică o încălcare a ordinii stabilite de acces la informațiile din calculatoare, de pe suporturile materiale de informaţie, din sistemul informatic sau din reţeaua informatică. O astfel de încălcare face dificilă sau chiar imposibilă derularea relațiilor sociale dintre subiecții care folosesc, administrează sau controlează un sistem informatic, care desfăşoară cercetări ştiinţifice sau care efectuează orice altă operaţiune într-un sistem informatic. Având în vedere acest aspect, ar reieși că infracțiunile, prevăzute la art. 259 CP RM, au obiect imaterial (care constă în informația computerizată), nu și obiect material.

Însă, nu putem ignora o altă sintagmă din dispoziția art. 259 CP RM – „dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”.[2111] Această sintagmă se referă la acțiunea adiacentă și este relevantă (ca și sintagma „accesul ilegal la informaţia

[2109] STRÎMBEANU, Alexandru. Obiectul juridic special al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): reflecții, abordări și soluții. [citat 30.12.2022] Disponibil: În: SSRN Electronic Journal. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313472

[2110] Ibidem.

[2111] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

computerizată”) în vederea stabilirii entităților prin intermediul cărora este lezat obiectul juridic special al infracțiunilor ce sunt prevăzute de art. 259 CP RM. Din sintagma „dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”[2112] rezultă că – în afară de informația computerizată accesată ilegal (care constituie obiectul imaterial principal al infracțiunilor examinate) – entitățile, prin intermediul cărora este lezat obiectul juridic special al infracțiunilor ce sunt prevăzute de art. 259 CP RM, sunt reprezentate de:

– informația computerizată distrusă, deteriorată, modificată, blocată sau copiată (care formează obiectul imaterial secundar al infracțiunilor prevăzute la art. 259 CP RM);

– calculatoarele, sistemul informatic sau reţeaua informatică, a căror funcționare a fost dereglată (care formează obiectul material secundar al acestor infracțiuni).

Săvârșind accesul ilegal la informaţia computerizată, făptuitorul accesează anume o astfel de informație, fiind interesat de calitățile ei utile și intenționând să valorifice ilegal aceste calități. Suporturile, pe care se află informaţia computerizată, nu sunt neapărat influențate în mod nemijlocit în contextul săvârșirii acțiunii principale de acces ilegal la informația computerizată. Asemenea suporturi nu sunt neapărat influențate nici în cazul distrugerii, deteriorării, modificării, blocării sau copierii informației computerizate care formează obiectul imaterial secundar al infracțiunilor prevăzute la art. 259 CP RM.

Calculatoarele, sistemul informatic sau reţeaua informatică, a căror funcționare a fost dereglată (care formează obiectul material secundar al infracțiunilor prevăzute la art. 259 CP RM), sunt influențate nemijlocit în contextul săvârșirii doar a acțiunii adiacente prevăzute la art. 259 CP RM. Însă, chiar și în acest ultim caz, calculatoarele, sistemul informatic sau reţeaua informatică formează obiectul material secundar al infracțiunilor, prevăzute la art. 259 CP RM, nu pentru că au calitatea de suporturi de informație computerizată, ci pentru că făptuitorul le-a dereglat funcționarea. În acest mod, posesorul calculatoarelor, al sistemului informatic sau al reţelei informatice este lipsit de posibilitatea de a valorifica calitățile utile ale acestor entități și de a participa la relațiile sociale care implică buna funcționare a calculatoarelor, a sistemului informatic sau a reţelei informatice.

Fiind unul dintre tipurile informației, informația computerizată posedă toate caracteristicile informației în general, dar și anumite caracteristici particulare. În esență, informația reprezintă rezultatul perceperii obiectelor și fenomenelor din lumea înconjurătoare prin mesaje și simboluri care sunt transmise și recepționate în procesul cunoașterii. În art. 259 CP RM se pune accentul

[2112] Ibidem.

nu pe forma de percepere a informației computerizate, ci pe mediul în care se află informația la momentul săvârșirii infracțiunii. Informația computerizată este informația destinată prelucrării pe un calculator, fixată pe un suport care poate fi citit de un calculator sau transmis într-un mediu care face posibilă interacționarea în cadrul unui sistem informatic sau al unei rețele informatice.

În acest context, este necesar să precizăm că transmisia de date informatice[2113] (inclusiv a unei emisii electronice) – care nu sunt publice şi care sunt destinate unui sistem informatic, provin dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic – poate să nu constituie obiectul imaterial al infracțiunilor prevăzute la art. 259 CP RM. În conjunctura infracțiunii prevăzute la art. 260^1 CP RM, transmisia de date informatice (inclusiv a unei emisii electronice), care nu sunt publice şi care sunt destinate unui sistem informatic, provin dintr-un asemenea sistem sau se efectuează în cadrul unui sistem, informatic, este interceptată ilegal.

Din art. 260^1 CP RM (și anume din sintagma „se efectuează în cadrul unui sistem informatic”[2114]) rezultă că transmisia de date informatice (ca și orice altă informație computerizată,) poate fi localizată într-un sistem informatic. În această ipoteză, se poate susține că art. 260^1 CP RM este o normă specială față de art. 259 CP RM. Din art. 116 CP RM rezultă că aplicarea art. 260^1 CP RM exclude calificarea faptei în baza art. 259 CP RM. În celelalte ipoteze (la care se referă formularea „care sunt destinate unui sistem informatic, provin dintr-un asemenea sistem”[2115]) nu există o relație de concurență între art. 259 și 260^1 CP RM.

Informația computerizată, care constă în transmisia de date informatice localizată în reţeaua informatică, poate reprezenta obiectul imaterial al infracțiunilor prevăzute la art. 259 CP RM. Aceasta desigur dacă sunt îndeplinite condițiile cu privire la celelalte semne constitutive ale infracțiunilor în cauză.

În acest plan, este de luat în considerare definiția de la lit. б) art. 1 al Acordului de cooperare între statele membre ale Comunității Statelor Independente (în continuare – CSI) în combaterea infracțiunilor din sfera informațiilor informatice. În această normă, inițial, prin „informație computerizată” s-a înțeles „informația din memoria unui calculator, de pe suporturile electronice

---

[2113] După M. Dobrinoiu, prin „transmisie de date informatice” se înțelege „fluxul de pachete informatice (succesiunea de biţi „0” şi „1”, adică succesiunea de impulsuri electrice rezultată din variaţia controlată a tensiunii)”*, „care sunt transportate de la un echipament de calcul către altul sau în interiorul aceluiaşi sistem informatic şi spre care se îndreaptă interesul făptuitorului”*; „Se are în vedere, inclusiv, energia (emisia) electromagnetică ce radiază sau se găseşte în formă reziduală”* „ori necontrolată (necontrolabilă) în imediata vecinătate a echipamentelor electronice care alcătuiesc sistemul informatic vizat”.*

* DOBRINOIU, Maxim. Infracțiunea de interceptare ilegală a unei transmisii de date informatice. În: *Revista română de dreptul proprietății intelectuale*, 2006, nr. 2, pp. 68-85. ISSN 1584-7241.

[2114] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

[2115] Ibidem.

sau de pe alte suporturi materiale”[2116], „care este accesibilă perceperii de către un calculator sau care este transmisă prin canale de comunicare”.[2117] În această definiție, sintagma „sau care este transmisă prin canale de comunicare” poate să nu corespundă paradigmei din art. 259 CP RM, potrivit căreia informaţie computerizată trebuie considerată doar „informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau rețeaua informatică”.[2118]

Datele informatice trebuie privite ca informație reprezentată într-o formă adecvată efectuării de operațiuni prin mijloace informatice cu posibila implicare a unei persoane. Datele informatice nu pot fi percepute nemijlocit de către o persoană. Ca urmare, pentru a organiza interacțiunea dintre o persoană și un calculator, este necesară codificarea (convertirea informației de intrare într-o formă percepută de calculator) și decodificarea (convertirea datelor informatice într-o formă care poate fi percepută de om). Datele informatice, obiectul și subiectul acestora apar în contextul unei relații. Elementele unei astfel de relații sunt:

1) obiectul datelor informatice (adică fapte, noţiuni, fenomene, evenimente, însuşiri, indici, instrucţiuni etc.);

2) datele informatice propriu-zise;

3) subiectul care recepționează datele informatice.

Datele informatice comportă semnificație pentru subiectul care le recepționează. Fără subiectul receptor, datele informatice rămân a fi doar informație computerizată.

Considerăm oportună modificarea art. 259 CP RM. La concret, în dispoziția alineatului (1) al acestui articol: textul „informaţia computerizată, adică la informaţia din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau rețeaua informatică”[2119] trebuie substituită prin cuvintele „datele informatice”; cuvântul „informației” trebuie înlocuit prin cuvântul „datelor”. De asemenea, în dispoziția de la lit. g) alin. (2) art. 259 CP RM, sintagma „informaţiei protejată” trebuie substituită prin cuvintele „datelor informatice protejate”.

Pe lângă acestea, Capitolul XIII al părții speciale a Codului penal al Republicii Moldova trebuie completat cu art. 134^{25} în care ar fi formulată următoarea definiție: „Prin date informatice se înțelege orice reprezentare de fapte, informaţii sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcţii de către un sistem informatic”.

[2116] *Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации*. [citat 06.03.2022] Disponibil: https://docs.cntd.ru/document/902140948

[2117] Ibidem.

[2118] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

[2119] Ibidem.

În alt context, „din definiția de la lit. a) art. 1 din Convenția de la Budapesta rezultă următoarele trăsături caracteristice ale sistemului informatic”[2120]:

„1) este fie un dispozitiv izolat, fie un ansamblu de dispozitive interconectate ori aflate în legătură”[2121];

„2) asigură ori dintre care unul sau mai multe elemente asigură prelucrarea automată a datelor informatice”[2122];

„3) implică asigurarea prelucrării automate a datelor informatice prin executarea unui program informatic.”[2123]

Din definiția de la lit. a) art. 2 al Directivei 2013/40/UE ar reieși că „sistem informatic se consideră:

1) fie un dispozitiv, fie un grup de dispozitive interconectate sau omoloage, fie datele informatice stocate”[2124], „prelucrate, recuperate sau transmise de acest dispozitiv sau grup de dispozitive în vederea exploatării, a utilizării, a protecției și a întreținerii lor”[2125];

„2) în cazul în care constă dintr-un fie dintr-un dispozitiv, fie dintr-un grup de dispozitive interconectate sau omoloage”[2126], „atunci unul sau mai multe dintre acestea asigură prelucrarea automată a datelor informatice”[2127];

„3) implică asigurarea prelucrării automate a datelor informatice prin executarea unui program de calculator.”[2128]

O eventuală transpunere a definiției de la lit. a) art. 2 al Directivei 2013/40/UE în legislația Republicii Moldova ar fi vulnerabilă sub aspectul clarității și previzibilității legii penale. Or, interpretând dispoziția de la alin. (1) art. 259 CP RM, ar fi imposibil de înțeles ce înseamnă „dereglarea funcţionării datelor informatice stocate, prelucrate, recuperate sau transmise de sistemul informatic în vederea exploatării, a utilizării, a protecției și a întreținerii acestui sistem.”[2129]

Definiția noțiunii „sistem informatic” din art. 2 al Legii nr. 20/2009 – „orice dispozitiv izolat sau ansamblu de dispozitive interconectate ori aflate în legătură care asigură ori dintre care unul

---

[2120] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[2121] Ibidem.
[2122] Ibidem.
[2123] Ibidem.
[2124] Ibidem.
[2125] Ibidem.
[2126] Ibidem.
[2127] Ibidem.
[2128] Ibidem.
[2129] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

sau mai multe elemente asigură, prin executarea unui program, prelucrarea automată a datelor”[2130] – corespunde definiției de la lit. a) art. 1 din Convenția de la Budapesta și răspunde necesităților art. 259 CP RM. Ca urmare, este necesară completarea Codului penal al Republicii Moldova cu art. 134[26] „Sistem informatic” cu următorul conținut: *„Prin sistem informatic se înțelege sistemul definit astfel în Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice”*.[2131] În multitudinea de definiții normative și doctrinare ale noțiunii „sistem informatic”, această definiție ar avea rolul de reper de netăgăduit, care ar contribui la interpretarea și aplicarea art. 259 CP RM în corespundere cu principiul legalității.[2132]

Serverele (privite ca dispozitive), prin intermediul cărora se prestează serviciile de e-mail, Facebook, Flickr, LinkedIn, Instagram, Pinterest, Twitter etc., asigură prin executarea unui program prelucrarea automată a datelor informatice. Drept urmare, aceste servere reprezintă sisteme informatice.

Funcția unui suport (mijloc) de stocare a datelor informatice este de a asigura, prin executarea unui program, stocarea automată a datelor informatice. Nu oricare entitate, ce poate fi folosită ca suport (mijloc) de stocare a datelor informatice, poate cumula funcția de a asigura prin executarea unui program prelucrarea automată a datelor informatice. Doar în cazul cumulării celor două funcții, entitatea respectivă constituie un sistem informatic.[2133]

Sistemul informatic reprezintă nodul de prelucrare a datelor interconectate în scopul transportului de date, în timp ce ansamblul unor astfel de noduri constituie rețeaua informatică. Pe lângă aceasta, este necesar să precizăm: nodurile, care constituie rețeaua informatică, pot să se exprime nu doar în calculatoare. Se au în vedere orice sisteme informatice.

Având în vedere această relație dintre noțiunile „sistem informatic” și „rețea informatică”, considerăm inutilă prezența sintagmei „rețea informatică” în art. 259 CP RM.

[2130] Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.

[2131] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

[2132] Precizăm că propunerea, ca noțiunea „sistem informatic” să fie definită în Codul penal prin referire la Legea nr. 20/2009, are la bază următorul argument: eventuala modificare în Legea nr. 20/2009 a definiției noțiunii de „sistem informatic” nu ar avea ca efect necesitatea de a face aceeași modificare în definiția noțiunii de „sistem informatic” din Codul penal. În acest mod definiția respectivă din legea penală nu va depinde de fluctuațiile din Legea nr. 20/2009.

[2133] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

Precizăm că rețeaua de comunicații electronice reprezintă obiectul material nu al infracțiunilor prevăzute la art. 259 CP RM[2134], ci al infracțiunilor prevăzute la art. 261[1] CP RM sau al faptelor prevăzute la art. 246-252 CC RM.[2135] Accesul neautorizat la reţelele de comunicații electronice (de telecomunicaţii) intră sub incidența art. 261[1] CP RM sau a art. 252 CC RM.[2136] În cazul în care rețeaua de comunicații electronice oferă posibilitatea realizării unui schimb de date informatice, ea cumulează calitatea de rețea informatică. În acest caz, este posibil concursul ideal al faptelor infracționale specificate în art. 259 și 261[1] CP RM.[2137]

În calitate de obiect material secundar al infracțiunilor prevăzute la art. 259 CP RM, calculatorul se distinge prin următoarele caracteristici:

1) acesta include două părți principale: partea fizică (hardware); partea logică (software);

2) calculatorul procesează datele în conformitate cu un program (o secvență de comenzi care trebuie executate în privința datelor pentru a rezolva o problemă);

3) calculatorul funcționează datorită interacțiunii următoarelor subsisteme: intrare (input); control; procesare aritmetică şi logică; memorie şi ieşire (output);

4) calculatorul reprezintă un sistem.

Orice calculator este un sistem informatic. De aceea, este necesară excluderea textelor „din calculatoare," și „calculatoarelor," din dispoziția alin. (1) art. 259 CP RM.

În alt context, „nu avem niciun temei să nu utilizăm noțiunea „victima infracțiunii" în raport cu persoana fizică sau cu persoana juridică asupra căreia este săvârșită una dintre infracțiunile prevăzute la art. 259 CP RM."[2138]

Victimă a infracțiunilor, prevăzute la art. 259 CP RM, este persoana fizică sau persoana juridică care participă la relaţiile sociale cu privire la accesul autorizat sau permis la informaţia computerizată.[2139]

Indiferent dacă accesul la informaţia computerizată necesită autorizare în temeiul legii sau al unui contract ori permisiune – obligația de a asigura protecția acelei informaţii computerizate îi incumbă 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. Respectiv, titularul dreptului corelativ acestei obligații, în cazul în care se

---

[2134] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale", 2022, nr. 8, pp. 77-90. ISSN 1814-3199.
[2135] Ibidem.
[2136] Ibidem.
[2137] Ibidem.
[2138] BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale", 2022, nr. 8, pp. 111-120. ISSN 1814-3199.
[2139] Ibidem.

accesează ilegal informațiile care îi aparțin, are calitatea de victimă a infracțiunilor prevăzute la art. 259 CP RM. Ne referim la persoana care are dreptul la protecția informației computerizate împotriva accesului neautorizat sau nepermis la aceasta.[2140]

Interesează nu caracteristicile persoanei care deține dreptul la protecția sistemului informațional sau a produsului informatic împotriva distrugerii, deteriorării, modificării, blocării, copierii sau dereglării funcţionării, ci caracteristicile persoanei care deține dreptul la protecția informaţiilor computerizate, a calculatoarelor, a sistemului informatic sau a reţelei informatice împotriva distrugerii, deteriorării, modificării, blocării, copierii sau dereglării funcţionării. De dreptul la protecția informaţiilor computerizate împotriva distrugerii, deteriorării, modificării, blocării sau copierii beneficiază nu doar proprietarul unor astfel de informații, ci și alți posesori ai informaţiilor computerizate. În mod similar, de dreptul la protecția calculatorului, a sistemului informatic sau a reţelei informatice împotriva dereglării funcționării beneficiază nu doar proprietarul acestora, ci și alți posesori.[2141]

Dacă persoana, vizată în informația computerizată distrusă, deteriorată, modificată, blocată sau copiată, nu este nici măcar utilizator al unei astfel de informații, ea nu va putea fi considerată victimă a acestor infracțiuni.[2142]

Nu se exclude ca persoana, vizată în informația computerizată distrusă, deteriorată, modificată, blocată sau copiată, să fie participantă la relațiile sociale apărate de alte articole din Codul penal (altele decât art. 259 CP RM). Pentru această ipoteză poate fi valabilă soluția concursului de infracțiuni. Astfel, în afară de art. 259 CP RM, poate fi aplicat art. 177, 178, 204, 245^{10}, alin. (1) art. 245^{12} etc. din Codul penal. În această ipoteză, persoana, vizată în informația computerizată distrusă, deteriorată, modificată, blocată sau copiată, va fi victimă a infracțiunilor prevăzute la art. 177, 178, 204, 245^{10}, alin. (1) art. 245^{12} etc. din Codul penal. O astfel de persoană va cumula calitatea de victimă a uneia dintre infracțiunile prevăzute la art. 259 CP RM numai dacă va avea calitatea de participantă la relațiile sociale ocrotite de acest articol (de exemplu, va avea calitatea de utilizator al informației computerizate distruse, deteriorate, modificate, blocate sau copiate).[2143]

[2140] Ibidem.
[2141] Ibidem.
[2142] Ibidem.
[2143] Ibidem.

3.2. Rezultatele obținute în urma analizei de drept penal a laturii obiective a infracțiunilor prevăzute la art. 259 CP RM

Accesul la informația computerizată implică intrarea în posesia asupra informației computerizate care aparține victimei, însă nu neapărat folosirea și/sau dispunerea de această informație. Accesul la informația computerizată doar deschide calea pentru o eventuală folosire și/sau dispunere de respectiva informație. De fapt, așa cum se va putea vedea mai jos, folosirea și/sau dispunerea de informația computerizată se referă la următoarea etapă de executare a laturii obiective a infracțiunilor prevăzute la art. 259 CP RM. Este corect să afirmăm că folosirea și/sau dispunerea de informația computerizată reprezintă scopul acțiunii de acces la informația computerizată, scop care depășește cadrul acestei acțiuni. Această concluzie o confirmă implicit următoarea prevedere de la lit. d) alin. (2) art. 28 al Legii nr. 1069/2000: „În scopul asigurării protecţiei datelor şi evitării infracţiunilor ce ţin de domeniul informaticii, se interzice: [...] pătrunderea neautorizată şi cu intenţie în sistemele”[2144] „şi reţelele informatice publice sau private, *chiar neurmată de ascultarea, înregistrarea sau utilizarea în interese personale”*[2145] *„ori în interesele altor persoane a datelor culese, precum şi pentru obţinerea unui alt folos* (evid. ns.)”.[2146]

Accesul la informația computerizată poate fi precedat de accesul la sistemul informatic în care se află respectiva informație. Totodată, nu trebuie să uităm că, în cazul infracțiunilor prevăzute la art. 259 CP RM, accesul la informația computerizată poate fi precedat de accesul nu doar la sistemul informatic în care se află respectiva informație, ci și la calculatorul, la suportul material de informaţie ori la reţeaua informatică, în care sau pe care se află informația computerizată.

Considerăm că, pentru a defini noțiunea de acces la informația computerizată, care să corespundă exigențelor dispoziției art. 259 CP RM, este necesar, în primul rând, să luăm în calcul înțelesul noțiunii de informație computerizată: informația destinată prelucrării pe un calculator, fixată pe un suport care poate fi citit de un calculator sau transmis într-un mediu care face posibilă interacționarea în cadrul unui sistem informatic sau al unei rețele informatice.

Însă, aceasta nu este suficient. Din dispoziția de la alin. (1) art. 259 CP RM rezultă că, în momentul accesării informației computerizate, această informație se află într-un calculator, pe un suport material de informaţie, într-un sistem informatic sau într-o reţea informatică. Este clar că,

---

[2144] Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
[2145] Ibidem.
[2146] Ibidem.

pentru a accesa informația computerizată, este necesar mai întâi să fie accesat calculatorul, suportul material de informaţie, sistemul informatic sau reţeaua informatică, în care sau pe care se află respectiva informație. Așadar, condiția obligatorie pentru accesarea ilegală a informației computerizate, este ca, în prealabil, să fie comisă acțiunea de intruziune ilegală în calculatorul, în suportul material de informaţie, în sistemul informatic sau în reţeaua informatică, în care sau pe care se află respectiva informație.[2147] În anumite privințe, această ipoteză poate fi comparată cu cea care presupune sustragerea unui bun care se află într-o încăpere, într-un alt loc pentru depozitare sau într-o locuinţă: făptuitorul pătrunde în încăperea, în alt loc pentru depozitare sau în locuinţa în care se află bunul care aparține victimei, după care intră în posesia asupra acelui bun, pentru a-l putea folosi și/sau a dispune de acesta.

Ținând cont de acest aspect și de înțelesul noțiunii de informație computerizată, considerăm că, prin „acces la informația computerizată" în accepțiunea art. 259 CP RM trebuie de înțeles: obținerea posibilității de a recurge la informația computerizată, în vederea beneficierii de calitățile utile ale acesteia.

Interacțiunea făptuitorului cu partea fizică (materială) a unui sistem informatic doar precede accesarea acestuia, fără însă a se identifica cu accesul la sistemul informatic.[2148] Cu atât mai mult, interacțiunea făptuitorului cu partea fizică (materială) a unui sistem informatic nu poate fi confundată cu accesul la informația computerizată. Or, informația computerizată are, prin excelență, o natură imaterială, incorporală. Așa cum am menționat mai sus, intruziunea ilegală în calculatorul, în suportul material de informaţie, în sistemul informatic sau în reţeaua informatică, în care sau pe care se află respectiva informație, trebuie deosebită de accesul la informația computerizată. Or, accesul la informația computerizată este precedat de o astfel de intruziune, fără însă a o include. În concluzie, în cazul infracțiunilor prevăzute la art. 259 CP RM, accesul la informația computerizată presupune o interacțiune logică, nu fizică, cu o astfel de informație.

[2147] Subliniem că această acțiune trebuie privită ca situație-premisă, nu ca etapă în procesul de săvârșire a accesului ilegal la informația computerizată. De aceea, trebuie calificată ca pregătire, nu ca tentativă, intruziunea ilegală în calculatorul, în suportul material de informaţie, în sistemul informatic sau în reţeaua informatică, în care sau pe care se află informația computerizată, dacă, din cauze ce nu depind de voința făptuitorului, nu este săvârșit accesul ilegal la acea informație. Sub anumite aspecte, această ipoteză poate fi comparată cu omorul săvârșit cu premeditare (lit. a) alin. (2) art. 145 CP RM), care presupune că, înainte de a săvârși omorul propriu-zis, făptuitorul se pregătește, în mod inerent, de comiterea acestuia.

[2148] Precizăm că nu oricare interacțiune logică cu un sistem informatic presupune accesul la acesta. Așa cum se menționează în pct. 46 din Raportul explicativ la Convenția de la Budapesta, „noțiunea [de acces] nu include simpla expediere a unui mesaj de e-mail sau a unui fișier către acel sistem".* În pct. 48 din același Raport se explică: „Aplicarea unor instrumente tehnice specifice *poate avea ca rezultat un acces* (evid. ns.) în temeiul articolului 2"*, „cum ar fi accesul la o pagină web, direct sau prin link-uri hipertext, inclusiv deep-link-uri sau aplicarea de „cookie-uri" sau „boți" pentru a localiza și a prelua informații".* Acțiunile exemplificate au menirea de a „pregăti terenul" pentru accesarea sistemului informatic.

* *Explanatory Report to the Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/16800cce5b

Interacțiunea logică cu informația computerizată se exprimă în aceea că făptuitorul folosește un program informatic sau mai multe programe informatice care asigură prelucrarea acelei informații.

În acest context, precizăm că accesul ilegal la informația computerizată (în accepția art. 259 CP RM) trebuie deosebit de interceptarea ilegală a unei transmisii de date informatice (în sensul art. 260^1 CP RM). În ultimul caz, interacțiunea este, de asemenea, de ordin logic. La concret, are loc interceptarea ilegală a unei transmisii de date informatice (inclusiv a unei emisii electronice) care nu sunt publice şi care sunt, după caz:

1) destinate unui sistem informatic;

2) provin dintr-un asemenea sistem;

3) se efectuează în cadrul unui sistem informatic.[2149]

În ultimul caz, atunci când se interceptează ilegal transmisia datelor informatice (inclusiv a emisiei electronice) ce nu sunt publice, se aplică doar art. 260^1 CP RM. Infracțiunea, prevăzută la art. 260^1 CP RM, poate fi concepută doar în cazul unei transmisii de date informatice (inclusiv a unei emisii electronice). În cazul infracțiunilor prevăzute la art. 259 CP RM, se accesează ilegal informația computerizată din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică, nu informația computerizată transmisă între calculatoare, între suporţii materiali de informaţie, între sisteme informatice sau între reţele informatice.[2150]

Menținerea accesului ilegal la informația computerizată după retragerea ori expirarea autorizării este avută în vedere implicit în dispoziția art. 259 CP RM. Așa cum rezultă din dispoziția de la alin. (1) art. 259 CP RM, accesul ilegal la informaţia computerizată presupune, printre altele, lipsa autorizării. Aceasta presupune, printre altele, ipoteza când, inițial, făptuitorul a fost autorizat să acceseze informaţia computerizată. Odată consumată autorizarea, dacă făptuitorul continuă să acceseze cu intenție informaţia computerizată, el devine pasibil de răspundere în baza art. 259 CP RM. Într-o altă ipoteză, dacă făptuitorul a obținut accesul la informația computerizată în mod fortuit sau din eroare, acesta devine pasibil de răspundere în baza art. 259 CP RM dacă va continua să acceseze cu intenție informația computerizată. Desigur, în ambele ipoteze, art. 259 CP RM este aplicabil numai dacă sunt prezente toate celelalte condiții stabilite în cadrul acestui articol.

În cazul infracțiunilor prevăzute la art. 259 CP RM, ilegalitatea faptei prejudiciabile este reprezentată, printre altele, la nivelul acțiunii de acces la informația computerizată. Folosirea de

---

[2149] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

[2150] STRÎMBEANU, Alexandru. Noţiunea de acces la informaţia computerizată în accepţiunea art. 259 din Codul penal al Republicii Moldova. În: *Revista Institutului Naţional al Justiţiei*, 2022, nr. 3, pp. 16-22. ISSN 1857-2405.

către legiuitor a termenului „ilegal” nu este redundantă în raport cu această acțiune. Această afirmație este confirmată de sintagma „al unei persoane care nu este autorizată în temeiul legii sau al unui contract, 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”[2151], ce este utilizată în dispoziția de la alin. (1) art. 259 CP RM. Această sintagmă este nu altceva decât extensia termenului „ilegal” din această dispoziție, menită să concretizeze semantismul termenului „ilegal” în contextul particular al infracțiunilor prevăzute de art. 259 CP RM.

În afară de aceasta, dacă termenul „ilegal” nu ar fi folosit în art. 259 CP RM, atunci ar fi imposibil sau foarte dificil de delimitat infracțiunile prevăzute de acest articol de infracțiunile specificate în art. 261 CP RM. Ultimul dintre aceste articole prevede răspunderea pentru „încălcarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic, prevăzute în conformitate cu statutul informaţiei sau gradul ei de protecţie, dacă această acţiune a contribuit la însuşirea, denaturarea sau la distrugerea informaţiei ori a provocat alte urmări grave”.[2152] Observăm că infracțiunea, prevăzută la art. 261 CP RM, presupune accesul la informația computerizată. Mai mult, accesul în sensul art. 261 CP RM, ca și accesul în accepția art. 259 CP RM, poate fi urmat de însuşirea (copierea), denaturarea (modificarea) sau distrugerea informaţiei computerizate. Totuși, spre deosebire de accesul în accepția art. 259 CP RM, accesul în sensul art. 261 CP RM este legal. Temeiul aplicării art. 261 CP RM îl constituie încălcarea regulilor de colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei computerizate ori a regulilor de protecţie a sistemului informatic, în condițiile unui acces legal la informația computerizată. Așadar, tocmai caracterul legal/ilegal al accesului la informația computerizată ne permite să deosebim infracțiunea, prevăzută la art. 261 CP RM, de infracțiunile prevăzute la art. 259 CP RM.

În concluzie, nu în toate cazurile este de prisos să vorbim despre ilegalitate atunci când caracterizăm o infracțiune concretă prevăzută de partea specială a legii penale.

Accesul la informația computerizată este ilegal, dacă se realizează:

1) în lipsa autorizării în temeiul legii sau al unui contract;

2) cu depăşirea limitelor autorizării;

[2151] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2152] Ibidem.

3) fără 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”.[2153]

Lipsa autorizării de a accesa informația computerizată presupune lipsa împuternicirii de a o accesa, pe care o acordă proprietarul informației computerizate sau un alt posesor al acestei informații. Pentru aplicarea art. 259 CP RM, nu are importanță dacă autorizarea, care-i lipsește făptuitorului, are ca sursă o lege sau un contract. De asemenea, nu contează dacă:

1) făptuitorul nu a avut în genere autorizarea de a accesa informația computerizată;

2) făptuitorul a avut în trecut autorizarea de a accesa informația computerizată, însă, în momentul săvârșirii infracțiunii, nu o mai avea, întrucât fie termenul autorizării expirase, fie autorizarea a fost suspendată ori revocată;

3) făptuitorului urma să-i fie acordată autorizarea de a accesa informația computerizată, însă, în momentul săvârșirii infracțiunii, acesta încă nu o avea, întrucât termenul autorizării nu începuse să curgă. Astfel de circumstanțe pot fi luate în calcul, eventual, doar la individualizarea pedepsei.

Depășind limitele autorizării de a accesa informația computerizată, făptuitorul își arogă împuterniciri de a accesa: un volum mai mare de informație decât cel autorizat pentru statutul pe care-l deține; informație calitativ diferită de cea autorizată pentru statutul pe care-l deține. Astfel de circumstanțe nu are un impact asupra calificării faptei în corespundere cu art. 259 CP RM, însă pot fi avute în vedere în procesul de individualizare a pedepsei.

Nu are importanță dacă permisiunea de a accesa informația computerizată (pe care ar fi trebuit să o aibă făptuitorul, însă nu o are) are un caracter verbal sau scris. De asemenea, nu este relevant dacă:

a) făptuitorul a solicitat permisiunea de a accesa informația computerizată, după care a ignorat refuzul de a da curs unei asemenea solicitări;

b) făptuitorul nu a solicitat permisiunea de a accesa informația computerizată.

La fel, nu contează dacă:

a) făptuitorul nu a avut în genere permisiunea de a accesa informația computerizată;

b) făptuitorul a avut în trecut permisiunea de a accesa informația computerizată, însă, în momentul săvârșirii infracțiunii, nu o mai avea, întrucât fie termenul permisiunii expirase, fie permisiunea a fost suspendată ori revocată;

[2153] Ibidem.

c) făptuitorului urma să-i fie acordată permisiunea de a accesa informația computerizată, însă, în momentul săvârșirii infracțiunii, acesta încă nu o avea, întrucât termenul permisiunii nu începuse să curgă.

Astfel de circumstanțe pot fi luate în calcul, eventual, doar la individualizarea pedepsei.

La calificarea faptei urmează să fie stabilită, în baza prevederilor actelor normative, competența persoanei care a permis accesul făptuitorului la informația computerizată. Dacă o astfel de persoană nu are calitatea de victimă a infracțiunii și nu are competența de a permite accesul făptuitorului la informația computerizată, atunci în baza art. 259 CP RM va răspunde: a) doar ea – în cazul în care a acționat cu intenție, în timp ce persoana, care a obținut permisiunea lovită de nulitate, a acționat fără vinovăție sau din imprudență. În acest caz, persoana care a permis accesul făptuitorului la informația computerizată, va răspunde ca autor al infracțiunii; b) atât ea, cât și persoana care a obținut permisiunea lovită de nulitate – în cazul în care ambele aceste persoane au acționat cu intenție. În acest caz, persoana care a permis accesul făptuitorului la informația computerizată, va răspunde ca instigator sau organizator al infracțiunii. Bineînțeles, persoana care a obținut permisiunea lovită de nulitate, va răspunde ca autor al infracțiunii.

Pentru a stabili dacă accesul la informația computerizată a fost realizat în condiții de legalitate, este necesară luarea în considerare a reglementărilor legale și/sau a celor ce dezvoltă prevederile unor legi, care circumstanțiază temeiul și limitele obținerii posibilității de a recurge la informația computerizată, în vederea beneficierii de calitățile utile ale acesteia.

Este posibil ca două ori mai multe persoane să aibă drept de acces la informaţia computerizată care se află în același calculator, pe același suport material de informaţie, în același sistem informatic sau în aceeași rețea informatică. Într-un asemenea caz, se prezumă că toate aceste persoane:

1) sunt autorizate în temeiul legii sau al unui contract;

2) nu depășesc limitele autorizării;

3) au permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic.

Această prezumție nu funcționează în ipoteza în care:

a) pentru una sau mai multe dintre persoanele respective, este restricționat dreptul de acces la o anumită informaţie computerizată care se află în același calculator, pe același suport material de informaţie, în același sistem informatic sau în aceeași rețea informatică *și*

b) una sau unele dintre persoanele respective încalcă acea restricție, ceea ce echivalează cu accesarea ilegală a informației computerizate.

Recomandăm ca, în scopul dezaglomerării dispoziției de la alin. (1) art. 259 CP RM, textul „ , al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să folosească”[2154], „să administreze sau să controleze un sistem informatic ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic”[2155] să fie exclus din această dispoziție. Totodată, propunem ca art. 134[28] „Persoana care accesează ilegal datele informatice”, inspirat de modelul alin. (2) art. 35 al României nr. 161/2003, să completeze Capitolul XIII din partea generală a Codului penal al Republicii Moldova: *„Accesează ilegal datele informatice persoana care se află în una dintre următoarele situații: a) nu este autorizată, în temeiul legii sau al unui contract; b) depășește limitele autorizării; c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic”*.[2156]

În altă privință, dacă intenția făptuitorului se limitează la săvârșirea accesului ilegal la informaţia computerizată, iar această intenție se realizează, atunci lipsește temeiul aplicării art. 259 CP RM. În acest caz este lipsă latura obiectivă a infracțiunii în deplinătatea sa, motiv pentru care vorbim despre lipsa componenței de infracțiune. În alte cazuri, dacă intenția făptuitorul cuprinde atât ambele componente ale faptei prejudiciabile prevăzute la art. 259 CP RM, cât și urmările prejudiciabile prevăzute de acest articol, iar această intenție se realizează doar în raport cu acțiunea de accesul ilegal la informaţia computerizată, trebuie să vorbim despre tentativa la una dintre infracțiunile prevăzute la art. 259 CP RM. În situația dată, latura obiectivă a infracțiunii este prezentă, doar că ea se realizează în mod parțial.

Care trebuie să fie calificarea dacă accesul ilegal la informația computerizată precede săvârșirea unei infracțiuni (de exemplu, a uneia dintre infracțiunile prevăzute la art. 145, 177, 185^1, 185^2, 189 etc. din Codul penal)? Într-un asemenea caz, se va aplica doar art. 145, 177, 185^1, 185^2, 189 etc. din Codul penal. De regulă, accesul ilegal la informația computerizată urmează a fi considerată pregătire de una dintre infracțiunile prevăzute la aceste articole, deoarece presupune crearea intenţionată de condiţii pentru săvârşirea lor, atunci când, din cauze ce nu depind de voinţa făptuitorului, infracţiunea nu şi-a produs efectul.

[2154] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2155] Ibidem.
[2156] STRÎMBEANU, Alexandru. *Răspunderea penală pentru accesul ilegal la informaţia computerizată: Monografie*. Chișinău: Tipografia Centrală, 2023, p. 241. 430 p. ISBN 978-5-88554-178-7.

În anumite cazuri, accesul ilegal la informația computerizată *per se* poate forma conținutul unei fapte penale sau contravenționale. De exemplu, accesul ilegal la informația computerizată *per se* poate reprezenta un exemplu de folosire ilegală a situației de serviciu (exprimat în accesarea informației computerizate în calitate de persoană autorizată în virtutea funcției pe care o deține făptuitorul). Într-un asemenea caz (dacă, desigur, sunt întrunite toate celelalte condiții stabilite în art. 327, 335 sau 370 CP RM ori în art. 312 CC RM, se va aplica unul dintre aceste articole). Apreciind în ansamblu cele comise, faptele, care sunt prevăzute de art. 327, 335 sau 370 CP RM ori la art. 312 CC RM, vor forma concurs cu una dintre infracțiunile prevăzute la art. 145, 177, 185^1, 185^2, 189 etc. din Codul penal.

În cazuri de altă natură, vom fi în prezența concursului de infracțiuni dacă o anumită infracțiune este precedată, însoțită sau succedată nu pur și simplu de accesul ilegal la informația computerizată, ci de accesul ilegal la informaţia computerizată, „însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”[2157], dacă s-au produs daune în proporţii mari sau deosebit de mari. Într-un asemenea caz, una dintre infracțiunile, prevăzute la art. 259 CP RM, va forma concurs cu infracțiunea precedentă, însoțitoare sau succesoare.

Prezența art. 260^2 și 260^3 CP RM face inutilă prezența în art. 259 CP RM a sintagmei care se referă la acțiunea adiacentă din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM: „dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”[2158].[2159] Mai mult decât atât, prezența acestei sintagme în art. 259 CP RM constituie un factor care contribuie la reținerea neîntemeiată a concursului ideal dintre una din infracțiunile, prevăzute la art. 259 CP RM, și una din infracțiunile prevăzute la art. 260^2 sau 260^3 CP RM. Or, unii practicieni ar fi, probabil, tentați să aplice atât art. 259 CP RM, cât și art. 260^2 sau 260^3 CP RM în cazul accesului ilegal la informaţia computerizată, însoțit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care a cauzat daune în proporţii mari sau deosebit de mari.

În art. 259 CP RM sunt specificate șase modalități normative ale acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM.:

[2157] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2158] Ibidem.
[2159] Trebuie de menționat că renunțarea la această sintagmă este propusă în Proiectul de lege pentru modificarea unor acte normative (modificarea Codului penal și Codului contravențional), publicat de Ministerul Justiției.*
* *Proiectul de lege pentru modificarea unor acte normative (modificarea Codului penal și Codului contravențional) (533/MJ/2022)*. [citat 30.12.2022] Disponibil: https://cancelaria.gov.md/ro/content/privind-aprobarea-proiectului-de-lege-pentru-modificarea-unor-acte-normative-modificarea

1) distrugerea informației computerizate;

2) deteriorarea informației computerizate;

3) modificarea informației computerizate;

4) blocarea informației computerizate;

5) copierea informaţiei informației computerizate;

6) dereglarea funcţionării calculatoarelor, a sistemului informatic sau a reţelei informatice.

Modalitățile respective au un caracter alternativ. Prezența oricăreia dintre cele șase modalități este suficientă pentru constatarea prezenței acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM. Numărul de modalități normative ale acțiunii adiacente din cadrul faptei prejudiciabile, care este prevăzută de art. 259 CP RM, poate fi luat în calcul în procesul de individualizare a pedepsei.

Distrugerea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, care exclude restabilirea ei ulterioară, indiferent de mijloacele și procedeele aplicate.

Deteriorarea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, ce are ca efect pierderea în parte sau pentru un anumit timp a calităților utile ale acesteia. Spre deosebire de distrugerea informaţiei computerizate, deteriorarea informaţiei computerizate nu exclude restabilirea ei ulterioară.

Modificarea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, ce implică schimbarea conținutului, formei sau aspectului acesteia. Spre deosebire de distrugerea și deteriorarea informaţiei computerizate, modificarea informaţiei computerizate presupune afectarea nu a integrității acesteia, ci a autenticității informaţiei computerizate. Informația modificată este – sub aspect cantitativ sau calitativ – diferită față de informația inițială, cea dinaintea modificării. Modificarea informației computerizate presupune fie substituirea unei părți din informația inițială cu alta, fie completarea informației inițiale cu alta. De asemenea, făptuitorul poate: introduce părți ale unei informații computerizate în conținutul unei alte informații computerizate; schimba ordinea părților dintr-o informație computerizată, etc.

În alt context, este oare necesar ca, în ipoteza însușirii ilegale de criptomonede, pe lângă fie art. 196 CP RM sau art. 244 CPR, fie art. 260^6 CP RM sau art. 250 CPR, să fie aplicat art. 259

CP RM (care prevede răspunderea pentru accesul ilegal la informaţia computerizată) sau art. 360 CPR (în care este incriminat accesul ilegal la un sistem informatic)?

Menționăm că infracțiunile, prevăzute la art. 259 CP RM, implică în mod necesar, printre altele, modificarea informaţiei. De asemenea, ele presupun cauzarea de daune în proporţii mari sau deosebit de mari. Cât privește infracțiunile prevăzute la art. 260^6 CP RM, acestea implică în mod necesar, printre altele, modificarea datelor informatice. În afară de aceasta, la fel ca infracțiunile, prevăzute la art. 259 CP RM, ele presupun cauzarea de daune în proporţii mari sau deosebit de mari. Din acest punct de vedere, observăm o anumită afinitate între infracțiunile, prevăzute la art. 259 CP RM, și cele prevăzute la art. 260^6 CP RM.

Totuși, în art. 260^6 CP RM este menționat un scop special (și anume – „scopul de a obţine un beneficiu material pentru sine sau pentru altul”[2160]), care nu este specificat în art. 259 CP RM. În aceste condiții, apare necesitatea de a răspunde la următoarea întrebare: care trebuie să fie încadrarea juridică în ipoteza accesului ilegal la criptomonede al unei persoane, care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să efectueze o operaţiune într-un sistem informatic, dacă acest acces: a) este însoţit de modificarea informaţiei, b) este săvârșit în scopul de a obţine un beneficiu material pentru sine sau pentru altul *și* c) a cauzat daune în proporţii mari sau deosebit de mari?

Apreciem că în această ipoteză nu este admisibilă aplicarea atât a art. 259 CP RM, cât și a art. 260^6 CP RM. În caz contrar, ar fi sancționată dublu aceeași modificare a informaţiei și aceeași cauzare de daune în proporţii mari sau deosebit de mari. În aceste condiții, considerăm corectă aplicarea doar a art. 260^6 CP RM. Putem vorbi despre o absorbție a faptei de acces ilegal la informaţia computerizată de către fapta de fraudă informatică. Compararea sancțiunilor din art. 259 și 260^6 CP RM permite o astfel de absorbție. Mai mult, accesul ilegal la criptomonede „al unei persoane, care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării ori nu are permisiunea persoanei competente”[2161] să efectueze o operaţiune într-un sistem informatic, trebuie privit ca act de pregătire de frauda informatică. Întrucât acest act are ca finalitate comiterea fraudei informatice, el își pierde relevanța juridică în procesul de săvârșire a fraudei informatice. (de făcut referire la Revista de Drept Penal)

Blocarea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra

[2160] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2161] Ibidem.

informaţiei computerizate, ce are ca efect restricționarea totală sau parțială a accesului victimei la informaţia computerizată. Spre deosebire de distrugerea și deteriorarea informaţiei computerizate, blocarea presupune că informaţia computerizată rămâne intactă. Durata și amploarea blocării informaţiei computerizate pot fi luate în considerare la individualizarea pedepsei.

Copierea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune reproducerea informaţiei computerizate într-un alt calculator, pe un alt suport material de informaţie, într-un alt sistem informatic sau într-o altă reţea informatică. Spre deosebire de blocarea informaţiei computerizate, copierea informaţiei computerizate nu exclude beneficierea în continuare de către victimă de informaţia computerizată.

În anumite cazuri, copierea informației computerizate (dacă produce daune în proporții mari sau deosebit de mari și *dacă nu este precedată de accesul ilegal la acea informație*), apare ca modalitate faptică a unor infracțiuni care presupun reproducerea anumitor informații (de exemplu, a infracțiunii prevăzute la lit. a) alin. (1) art. 185^1 CP RM). În asemenea cazuri, nu este necesară aplicarea art. 259 CP RM, întrucât nu sunt întrunite toate condițiile care ar permite aplicarea acestui articol. Dacă sunt prezente toate condițiile cerute de lit. a) alin. (1) art. 185^1 CP RM, atunci se aplică această normă.

În cazuri de altă natură, copierea informației computerizate (dacă produce daune în proporții mari sau deosebit de mari și *dacă este precedată de accesul ilegal la acea informație*), nu poate fi percepută ca modalitate faptică a infracțiunii care este prevăzută de lit. a) alin. (1) art. 185^1 CP RM. În cazul de față se aplică, după situație, lit. a) alin. (1) art. 185^1 CP RM sau art. 259 CP RM. La concret, conform principiului subsidiarității, trebuie să se aplice doar acea normă care prevede pedeapsa mai aspră.[2162]

Dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra calculatoarelor, a sistemului sau a reţelei informatice, care implică scoaterea din funcțiune – permanentă sau temporară – a acestora. Durata de scoatere

[2162] Cu privire la acest principiu, C.G. Feșteu afirmă: „Subsidiaritatea se regăsește în cadrul relației dintre două sau mai multe norme de incriminare”*, „subordonând aplicarea unei norme penale de neaplicarea unei norme mai grave (de regulă) sau de o altă normă determinată”*; „[...] În mod normal, analiza pe baza criteriului subsidiarității începe de la infracțiunea mai gravă corespunzând faptei materiale, care după ce este verificată”*, „nu mai lasă loc de aplicare normei subsidiare, de o gravitate mai redusă, astfel realizându-se alegerea normei”.*

* FEȘTEU, Cristina Georgiana. Concursul de calificări (I). În: *Penalmente relevant*, 2016, nr. 1, pp. 67-88. ISSN 2501-1367.

din funcțiune a calculatoarelor, a sistemului sau a reţelei informatice, poate fi luată în considerare la individualizarea pedepsei.

În alt context, formularea „distrugerea, deteriorarea modificarea [...] informaţiei, [...] dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”[2163] (care este folosită în dispoziția de la alin. (1) art. 259 CP RM din momentul adoptării Codului penal în vigoare și care nu a fost afectată de adoptarea Legii nr. 278/2008) are un caracter eliptic, concentrând în ea descrierea nu numai a faptei prejudiciabile, dar și a urmărilor prejudiciabile, precum și a legăturii cauzale.

Poziția față de structura laturii obiective a faptelor infracționale, ce sunt prevăzute de art. 259 CP RM, trebuie diferențiată în funcție de modalitățile normative ale acțiunii adiacente din cadrul faptei prejudiciabile.

Ținând cont de specificul infracțiunilor prevăzute la art. 259 CP RM, apreciem că, doar în cazurile de distrugere, deteriorare sau modificare a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, *verbum regens* vizează atât fapta prejudiciabilă, cât și urmările prejudiciabile. Or, în prezența acestor patru modalități normative, se produc anumite metamorfoze la nivelul obiectului material sau imaterial al infracțiunilor prevăzute la art. 259 CP RM. De aceea, în aceste patru cazuri, rezultatul, necesar consumării infracțiunii, constă, în primul rând, în distrugerea, deteriorarea sau modificarea informaţiei, ori în dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice. În al doilea rând, un astfel de rezultat se exprimă în daunele în proporții mari. La o privire *in corpore*, în cazurile analizate, urmările prejudiciabile constau în distrugerea, deteriorarea sau modificarea informaţiei, ori dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor în proporţii mari.

În opinia noastră, acest punct de vedere este reflectat, într-o oarecare măsură, în alin. (1) și (1^1) art. 126 CP RM: „(1) Se consideră proporţii mari valoarea bunurilor sustrase, dobândite, primite, fabricate, *distruse* (evid. ns.), utilizate, transportate, păstrate, comercializate, trecute peste frontiera vamală”[2164], „*valoarea pagubei pricinuite* (evid. ns.) de o persoană sau de un grup de persoane, care depăşeşte 20 de salarii medii lunare pe economie prognozate”[2165], „stabilite prin hotărârea de Guvern în vigoare la momentul săvârșirii faptei”[2166]; „(1^1) Se consideră proporţii deosebit de mari valoarea bunurilor sustrase, dobândite, primite, fabricate, *distruse*

[2163] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2164] Ibidem.
[2165] Ibidem.
[2166] Ibidem.

(evid. ns.), utilizate, transportate, păstrate, comercializate, trecute peste frontiera vamală”[2167], „*valoarea pagubei pricinuite* (evid. ns.) de o persoană sau de un grup de persoane, care depăşeşte 40 de salarii medii lunare pe economie prognozate”[2168], „stabilite prin hotărârea de Guvern în vigoare la momentul săvârșirii faptei”.[2169]

Totodată, în cazurile de blocare sau copiere a informaţiei, *verbum regens* vizează exclusiv fapta prejudiciabilă. Considerăm că, în prezența acestor două modalități normative, nu se produc metamorfoze la nivelul obiectului material sau imaterial al infracțiunilor prevăzute la art. 259 CP RM. În aceste cazuri, rezultatul, necesar consumării infracțiunii, constă doar în daunele în proporții mari.

În consecință, latura obiectivă a infracţiunilor prevăzute la art. 259 CP RM are, în prima sa variantă, următoarea structură:

1) fapta prejudiciabilă care constă în acţiunea principală de acces ilegal la informaţia computerizată, succedată de acţiunea adiacentă de distrugere, deteriorare sau modificare a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice;

2) urmările prejudiciabile, și anume – distrugerea, deteriorarea sau modificarea informaţiei, ori dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor în proporţii mari (în cazul infracțiunii prevăzute la alin. (1)) ori a daunelor în proporţii deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2));

3) legătura cauzală dintre fapta prejudiciabilă şi urmările prejudiciabile.

Într-o altă variantă, latura obiectivă a infracţiunilor prevăzute la art. 259 CP RM are structura următoare:

1) fapta prejudiciabilă care constă în acţiunea principală de acces ilegal la informaţia computerizată, succedată de acţiunea adiacentă de blocare sau copiere a informaţiei;

2) urmările prejudiciabile, și anume – daunele în proporţii mari (în cazul infracțiunii prevăzute la alin. (1)) sau daunele în proporţii deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2));

3) legătura cauzală dintre fapta prejudiciabilă şi urmările prejudiciabile.

Cât privește noțiunile „distrugerea informației computerizate”, „deteriorarea informației computerizate”, „modificarea informației computerizate” și „dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”, acestea au fost definite și analizate

[2167] Ibidem.
[2168] Ibidem.
[2169] Ibidem.

anterior, în procesul examinării acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM. De aceea, fără a ne repeta, facem referire la explicațiile respective.

În cele ce urmează, prezentăm poziția noastră cu privire la oportunitatea specificării urmărilor prejudiciabile în art. 259 CP RM.

Considerăm că excluderea textului „însoțită de distrugerea, deteriorarea, modificarea, blocarea sau copierea informațiilor și perturbarea funcționării calculatoarelor, a unui sistem informatic sau a unei rețele de calculatoare”[2170] din alin. (1) art. 259 CP RM este oportună. Această excludere ar fi compensată datorită existenței în Codul penal a art. 260^2 și 260^3. În eventualitatea în care textul „însoțită de distrugerea, deteriorarea, modificarea, blocarea sau copierea informațiilor și perturbarea funcționării calculatoarelor, a unui sistem informatic sau a unei rețele de calculatoare”[2171] ar fi exclus din alin. (1) art. 259 CP RM, accesul ilegal la informaţia computerizată ar putea forma concurs cu una dintre infracțiunile prevăzute la art. 260^2 sau 260^3 CP RM. Deci, ordinea de drept ar continua să fie apărată la fel de eficient.

În acest context, este necesar să menționăm că, rezultatul adoptării Legii nr. 278 din 18.12.2008 pentru modificarea şi completarea Codului penal al Republicii Moldova[2172], printre altele:

1) a fost modificat art. 260 CP RM;

2) Codul penal al Republicii Moldova a fost completat cu art. 260^1-260^6.

În acest mod, Codul penal al Republicii Moldova a fost adus în concordanță cu prevederile art. 3-8 din Convenția de la Budapesta.

Totodată, prin aceeași lege, art. 259 CP RM nu a fost adus în concordanță cu prevederile art. 2 al Convenției de la Budapesta. Or, art. 2 al Convenției de la Budapesta nu conține recomandarea ca accesul ilegal la informaţia computerizată să fie incriminat dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice. Actuala dispoziție a alin. (1) art. 259 CP RM reprezintă o „adaptare originală” a dispoziției de la alin. 1 art. 272 CP FR („Accesul ilegal la informația computerizată protejată legal, dacă această faptă a dus la distrugerea, blocarea, modificarea sau copierea informației computerizate”[2173]). Aici este

[2170] Ibidem.
[2171] Ibidem.
[2172] Legea 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, 98.
[2173] Уголовный кодекс Российской Федерации. În: *Собрание законодательства Российской Федерации*, 1996, № 25.

important de menționat că Federația Rusă nu este parte la Convenția de la Budapesta.[2174] De aceea, păstrarea dispoziției actuale a alin. (1) art. 259 CP RM vine în discordanță cu angajamentele asumate de către Republica Moldova la semnarea și ratificarea Convenției de la Budapesta.

Mai sus am menționat că alin. (1) art. 259 CP RM reprezintă o „adaptare originală" a dispoziției de la alin. 1 art. 272 CP FR. Ne referim la sintagma „dacă este însoţit de" din alin. (1) art. 259 CP RM. Doar în alin. (1) art. 259 CP RM este consacrată concepția, conform căreia acțiunea principală de acces ilegal la informaţia computerizată este însoţită de acțiunea adiacentă de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice. În realitate, accesul ilegal la informaţia computerizată nu poate însoţi nici distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, nici dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice. O astfel de însoțire ar presupune simultaneitatea comiterii accesului ilegal la informaţia computerizată și a comiterii distrugerii, deteriorării, modificării, blocării sau copierii informaţiei, ori a dereglării funcţionării calculatoarelor, a sistemului sau a reţelei informatice.

Supra am menționat că acțiunea principală de acces la informația computerizată doar deschide calea pentru o eventuală folosire și dispunere de această informație. Însăși folosirea și/sau dispunerea de informația computerizată se referă la următoarea etapă de executare a laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, și anume – la acțiunea adiacentă din cadrul faptei prejudiciabile.[2175] Ne dăm seama că – pentru ca informația computerizată să fie distrusă, deteriorată, modificată, blocată sau copiată, ori pentru ca funcţionarea calculatoarelor, a sistemului sau a reţelei informatice să fie dereglată – este necesar ca, în prealabil, făptuitorul să acceseze ilegal informaţia computerizată. Fără a ține seama de această consecutivitate condiționată de însăși natura lucrurilor, legiuitorul moldovean a consacrat în alin. (1) art. 259 CP RM o consecutivitate care sfidează logica elementară.

În altă privință, excluderea sintagmelor „şi dacă a cauzat daune în proporţii mari" din alin. (1) art. 259 CP RM, precum și excluderea lit. h) „în proporţii deosebit de mari" din alin. (2) art. 259 CP RM ar fi compensată, de asemenea, prin existența în Codul penal a art. 260^2 și 260^3. Or, art. 260^2 CP RM prevede răspunderea pentru „modificarea, ştergerea sau deteriorarea intenţionată a datelor informatice ţinute într-un sistem informatic ori restricţionarea ilegală a accesului la aceste

[2174] A se vedea în acest sens: *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*. [citat 18.12.2020] Disponibil: https://www.coe.int/en/web/cybercrime/parties-observers

[2175] Prin această săvârșire etapizată a faptei prejudiciabile, infracțiunile analizate amintesc de infracțiunile prevăzute la art. 238 CP RM.

date”[2176], „transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, comercializarea sau punerea la dispoziţie”[2177], „sub orice formă, a datelor informatice cu acces limitat, *dacă aceste acţiuni au cauzat daune în proporţii mari* (evid. ns.)”. La rândul său, art. 260^2 CP RM prevede răspunderea pentru „perturbarea funcţionării unui sistem informatic prin introducerea, transmiterea, modificarea, ştergerea sau deteriorarea datelor informatice sau prin restricţionarea accesului la aceste date”[2178], dacă aceste acţiuni au cauzat „daune în proporţii mari” (alin. (1)) ori „daune în proporţii deosebit de mari” (lit. d) alin. (2)).

În art. 2 al Convenției de la Budapesta nu se recomandă ca incriminarea faptei de acces ilegal al sistemului informatic să fie condiționată de producerea unor urmări grave. O astfel de recomandare se face în art. 4 al Convenției de la Budapesta pentru o altă faptă, și anume – cea de afectare a integrităţii datelor. Această abordare trebuie respectată de către legiuitorul moldovean. Este necesar ca în art. 259 CP RM să fie prevăzută răspunderea pentru o infracțiune formală, a cărei consumare să nu depindă de producerea unei urmări prejudiciabile.

Totodată, renunțarea la specificarea urmărilor prejudiciabile în art. 259 CP RM nu trebuie să influențeze negativ asupra diferențierii răspunderii juridice pentru accesul ilegal la informația computerizată. Această diferențiere poate fi făcută în baza unui alt criteriu care, de altfel, este propus în art. 2 al Convenției de la Budapesta: „Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern”[2179], „accesarea intenţionată şi fără drept a ansamblului ori a unei părţi a unui sistem informatic”[2180]; „O parte poate condiţiona o astfel de incriminare de comiterea încălcării respective *prin violarea măsurilor de securitate* (evid. ns.) [...]”.[2181]

Din această prevedere desprindem că accesul ilegal la informaţia computerizată este suficient de periculoasă sub aspect social pentru a fi incriminată. O astfel de acțiune ar putea fi incriminată doar cu condiția că n-ar constitui un „caz minor”. Dezvoltând ideea, ținem să menționăm că, potrivit art. 3 „Accesarea ilegală a sistemelor informatice” din Directiva 2013/40/UE, „statele membre adoptă măsurile necesare pentru a garanta că accesarea cu intenție și fără drept a unui sistem informatic”[2182] „ori a unei părți a acestuia *este incriminată atunci când este săvârșită prin*

[2176] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2177] Ibidem.
[2178] Ibidem.
[2179] *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
[2180] Ibidem.
[2181] Ibidem.
[2182] *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en

încălcarea unei măsuri de securitate (evid. ns.), cel puțin atunci când nu reprezintă un caz minor”.[2183]

Într-un Raport al Comisiei Europene, Regatul Belgiei, Republica Bulgaria, Republica Franceză, Republica Croația, Marele Ducat de Luxemburg, Republica Malta, Republica Portugheză, România, Republica Slovenia și Marea Britanie sunt criticate pentru că violarea măsurilor de securitate nu este o condiție obligatorie în articolele din legile penale ale acestor state, care sunt corespondente cu art. 259 CP RM, așa cum cere art. 3 din Directiva 2013/40/UE. Din contra, alte state – Republica Cipriotă, Grecia, Republica Slovacă, Republica Austria, Republica Cehă, Republica Federală a Germaniei, Republica Estonia, Regatul Spaniei, Republica Finlanda, Ungaria, Republica Italia, Republica Lituania, Republica Letonia, Regatul Țărilor de Jos și Regatul Suediei – sunt prezentate ca exemple de urmat.[2184] În afară de aceasta, în Recomandarea Comitetului de Miniştri al Consiliului Europei nr. R(89)9 referitoare la criminalitatea în legătură cu utilizarea calculatorului, se sugerează incriminarea „accesului ilegal la un sistem computerizat sau la o rețea computerizată prin încălcarea măsurilor de securitate”.[2185] În acest context, nu este de prisos de menționat că, în conformitate cu art. 176[1] CP RM din 1961, „încălcarea sistemului de protecţie”[2186] constituia condiția indispensabilă pentru incriminarea accesului ilegal la informaţia computerizată.

În consecință, apreciem că trebuie abrogată prevederea de la lit. c) alin. (2) art. 259 CP RM („cu violarea sistemelor de protecţie”). Totodată, dispoziția de la alin. (1) art. 259 CP RM trebuie completată cu sintagma „prin violarea măsurilor de securitate”.

Astfel, violarea măsurilor de securitate trebuie să devină condiția obligatorie pentru existența variantei-tip a faptei prevăzute la art. 259 CP RM. Prin stabilirea acestei condiții, incriminarea accesului ilegal la informația computerizată ar corespunde principiului proporționalității incriminării. Violarea măsurilor de securitate ar asigura acel grad minim necesar de pericol social care ar justifica intervenția legii penale.

Pe această cale va fi asigurată respectarea următoarei teze din Manifestul referitor la politica penală europeană se menționează: „Decizia-cadru referitoare la atacurile privind sistemele

---

[2183] Ibidem.

[2184] *Raport al Comisiei către Parlamentul European și Consiliu de evaluare a gradului în care statele membre au adoptat măsurile necesare pentru a se conforma Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017DC0474&from=GA

[2185] *Recommendation No. R. (89) 9 of the Committee of the Ministers to Member States on Computer-related Crime*. [citat 18.12.2020] Disponibil: http://www.cm.coe.int/ta/rec/1989/ 89r9.htm

[2186] Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.

informatice[2187] stabileşte obligaţii de incriminare pentru accesarea ilegală a sistemelor informatice [...]”[2188]; „Pentru a nu extinde prea mult sfera faptelor sancţionabile penal aceasta exceptează de la aplicarea unei sancţiuni penale aşa-numitele cazuri uşoare”[2189] ; „Mai mult, în ceea ce priveşte hacking-ul introducerea unei sancţiuni penale doar pentru tentativă este lăsată la latitudinea statelor membre”[2190], „deşi în celelalte cazuri pedepsirea tentativei este obligatorie”[2191]; „Ar putea exista dubii cu privire la caracterul suficient al acestor paşi raportat la evitarea unei incriminări mult prea extinse. [...]”.[2192]

În afară de aceasta, propunerea, pe care o facem, ar fi consonantă cu ideea exprimată de V. Stati, referitoare la inițiativa de a substitui în alin. (1) art. 259 CP RM sintagma „daune în proporţii mari” prin sintagma „daune considerabile”, formulată în Proiectul de lege pentru modificarea unor acte normative (modificarea Codului penal și Codului contravențional)[2193]: „Înțelegem intenția autorilor Proiectului de a trasa – în alin. (1) art. 259 [...] CP RM – o limită care ar permite delimitarea manifestărilor de ilicit penal”[2194] „de manifestările care nu posedă gradul suficient de pericol social pentru a fi considerate infracțiuni”[2195]; „Însă, în afară de sintagme de genul „daune (în proporții) considerabile”, chiar nu mai există alte căi de a asigura o astfel de delimitare?”[2196]; „[...] O posibilă soluție la problema, pe care am învederat-o, transpare chiar din art. 2 „Accesarea ilegală” al Convenției de la Budapesta [...]”[2197]; „Din criteriile propuse în [acest articol] poate fi ales unul sau câteva care ar permite delimitarea manifestărilor de ilicit penal”[2198] „de manifestările care nu posedă gradul suficient de pericol social pentru a fi considerate infracțiuni”[2199]; „Dacă fapta nu va corespunde unui asemenea criteriu / unor

---

[2187] Se are în vedere Decizia-cadru 2005/222/JAI a Consiliului din 24.02.2005 privind atacurile împotriva sistemelor informatice*, care a fost înlocuită prin Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului.**

* https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32005F0222&from=ro

** https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=RO

[2188] *Manifest referitor la politica penală europeană*. [citat 18.12.2020] Disponibil: https://www.zis-online.com/dat/artikel/2009_12_387.pdf

[2189] Ibidem.

[2190] Ibidem.

[2191] Ibidem.

[2192] Ibidem.

[2193] *Proiectul de lege pentru modificarea unor acte normative (modificarea Codului penal și Codului contravențional) (533/MJ/2022)*. [citat 30.12.2022] Disponibil: https://cancelaria.gov.md/ro/content/privind-aprobarea-proiectului-de-lege-pentru-modificarea-unor-acte-normative-modificarea

[2194] STATI, Vitalie. Despre „interesul public”, „daunele considerabile” și nu numai: analiza unui proiect de amendare a Codului penal al Republicii Moldova. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4188261

[2195] Ibidem.

[2196] Ibidem.

[2197] Ibidem.

[2198] Ibidem.

[2199] Ibidem.

asemenea criterii, poate fi stabilită răspunderea contravențională pentru manifestările care nu posedă gradul suficient de pericol social pentru a fi considerate infracțiuni”.[2200]

În lipsa violării măsurilor de securitate, accesul ilegal la informaţia computerizată ar trebui sancționat contravențional într-un articol care ar fi inclus în Capitolul XIV „Contravenţii în domeniul comunicaţiilor electronice și al comunicațiilor poștale” din Codul contravențional. La concret, recomandăm ca acest capitol să fie completat cu art. 246[1] „Accesul ilegal la datele informatice” cu următorul conținut: „Accesul ilegal la datele informatice, dacă fapta nu constituie infracţiune, se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 120 la 180 de unităţi convenţionale aplicată persoanei juridice”.[2201]

În altă ordine de idei, nu este oportună completarea art. 259 CP RM cu un alineat aparte în care s-ar prevedea răspunderea pentru tentativa de infracțiune. Art. 25, 27 și alin. (3) art. 81 CP RM sunt suficiente pentru a sancționa tentativa la infracțiunile prevăzute la art. 259 CP RM și pentru a individualiza pedeapsa pentru aceste infracțiuni. Nu este necesară prezența în partea specială a Codului penal a unor norme care ar dubla art. 25, 27 și alin. (3) art. 81 CP RM, și, astfel, ar dezorienta practicienii.

Mai mult, parag. 3 art. 11 al Convenției de la Budapesta lasă la discreția statelor semnatare să decidă asupra unei eventuale incriminări distincte a tentativei de infracțiune. Din acest punct de vedere nu constituie o încălcare a acestei Convenții omisiunea de a completa art. 259 CP RM cu un alineat aparte în care s-ar prevedea răspunderea pentru tentativa de infracțiune.

În cazul infracțiunilor prevăzute la art. 259 CP RM, tentativa este posibilă în următoarele cazuri:

1) se încearcă săvârșirea accesului ilegal la informaţia computerizată, însă, din cauze care nu depind de voința făptuitorului nu este comis în întregime acest acces și nu este săvârșită în genere nici distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, nici dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice;

2) este săvârșit în întregime accesul ilegal la informaţia computerizată, însă, din cauze care nu depind de voința făptuitorului, nu este comisă în genere nici distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, nici dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice;

[2200] Ibidem.

[2201] STRÎMBEANU, Alexandru. *Răspunderea penală pentru accesul ilegal la informaţia computerizată: Monografie*. Chișinău: Tipografia Centrală, 2023, p. 391. 430 p. ISBN 978-5-88554-178-7.

3) este săvârșit în întregime accesul ilegal la informaţia computerizată, se încearcă săvârșirea distrugerii, deteriorării, modificării, blocării sau copierii informaţiei, ori a dereglării funcţionării calculatoarelor, a sistemului sau a reţelei informatice, însă, din cauze ce nu depind de voința făptuitorului, nu este comisă în întregime nici distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, nici dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice;

4) sunt săvârșite în întregime atât accesul ilegal la informaţia computerizată, cât și distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, însă, din cauze care nu depind de voința făptuitorului, nu se produc daunele în proporţii mari sau daunele în proporții deosebit de mari.

Având în vedere posibilitatea erorii de fapt fie cu privire la anumite semne constitutive ale infracțiunilor prevăzute la art. 259 CP RM, fie cu privire la anumite circumstanțe agravante prevăzute de acest articol, semnalăm posibilitatea tentativei în alte câteva cazuri:

1) făptuitorul intenționează să săvârșească infracțiunea ce este prevăzută de alin. (1) art. 259 CP RM cu violarea sistemelor de protecţie, însă, din cauze ce nu depind de voința lui, nu realizează această intenție. În acest caz, trebuie aplicate art. 27 și lit. c) alin. (2) art. 259 CP RM;

2) făptuitorul intenționează să săvârșească infracțiunea ce este prevăzută de alin. (1) art. 259 CP RM cu conectarea la canalele de telecomunicaţii, însă, din cauze care nu depind de voința lui, nu realizează această intenție. În acest caz, trebuie aplicate art. 27 și lit. d) alin. (2) art. 259 CP RM;

3) făptuitorul intenționează să săvârșească infracțiunea ce este prevăzută de alin. (1) art. 259 CP RM cu folosirea unor mijloace tehnice speciale, însă, din cauze ce nu depind de voința lui, nu realizează această intenție. În acest caz, trebuie aplicate art. 27 și lit. e) alin. (2) art. 259 CP RM;

4) făptuitorul intenționează să săvârșească infracțiunea ce este prevăzută de alin. (1) art. 259 CP RM în privinţa informaţiei protejate de lege, însă, din cauze independente de voința lui, nu realizează această intenție. În acest caz, trebuie aplicate art. 27 și lit. g) alin. (2) art. 259 CP RM;

5) făptuitorul intenționează să cauzeze daune în proporţii deosebit de mari, însă, din cauze independente de voința lui, cauzează daune în proporţii mari sau daune de o mărime mai redusă. În acest caz, trebuie aplicate art. 27 și lit. h) alin. (2) art. 259 CP RM.

Nu se exclude îmbinarea condițiilor de tentativă din primele patru categorii specificate mai sus cu condițiile de tentativă din ultimele cinci categorii specificate mai sus. Într-un asemenea caz, în prezența aceleiași intenții infracționale, bineînțeles, tentativa trebuie reținută o singură dată. Nu putem vorbi despre „tentativa la tentativă” sau despre „dublă tentativă”. Numărul și specificul condițiilor de tentativă pot fi luate în considerare la individualizarea pedepsei.

Art. 260 CP RM stabilește răspunderea pentru „producerea, importul, comercializarea sau punerea la dispoziţie, sub orice altă formă, în mod ilegal”[2202], „a mijloacelor tehnice sau produselor program, concepute sau adaptate”[2203], în scopul săvârşirii uneia dintre infracţiunile prevăzute la art. 237, 259, 260^1-260^3, 260^5 şi 260^6”.[2204] La fel, art. 260^4 CP RM prevede răspunderea pentru „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”.[2205] Observăm că săvârșirea infracțiunilor prevăzute la art. 259 CP RM se numără printre scopurile de comitere a infracțiunilor prevăzute la art. 260 și 260^4 CP RM. În acest context, infracțiunile, prevăzute la art. 260 și 260^4 CP RM, pot fi considerate exemple de pregătire *sui generis* de infracțiunile prevăzute la art. 259 CP RM.

În ceea ce privește prima variantă a laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, urmările prejudiciabile – exprimate în distrugere, deteriorare sau modificare a informaţiei, ori în dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor în proporţii mari (în cazul infracțiunii prevăzute la alin. (1)) ori a daunelor în proporţii deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2)) – trebuie să se afle într-un raport de cauzalitate cu fapta prejudiciabilă care constă în acţiunea principală de acces ilegal la informaţia computerizată, succedată de acţiunea adiacentă de distrugere, deteriorare sau modificare a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice.

În ceea ce privește variantă secundă a laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, urmările prejudiciabile – exprimate în daunele în proporţii mari (în cazul infracțiunii prevăzute la alin. (1)) ori în daunele în proporţii deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2)) – trebuie să se afle într-un raport de cauzalitate cu fapta prejudiciabilă care constă în acţiunea principală de acces ilegal la informaţia computerizată, succedată de acţiunea adiacentă de blocare sau copiere a informaţiei.

Considerăm că, în contextul infracțiunilor prevăzute la art. 259 CP RM, acțiunea principală de acces ilegal la informația computerizată nu are potențialitatea de a cauza daune în proporții mari sau deosebit de mari. Această acțiune presupune oferă făptuitorului posibilitatea de a folosi

[2202] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2203] Ibidem.
[2204] Ibidem.
[2205] Ibidem.

și a dispune de informația computerizată. Posibilitatea în cauză se poate transforma în realitate doar în momentul săvârșirii acțiunii adiacente de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei, de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice. De aceea, daunele în proporții mari sau deosebit de mari trebuie raportate exclusiv la acțiunea adiacentă prevăzută de art. 259 CP RM.

Nu se exclude ca accesul ilegal la informația computerizată *per se* să reprezinte modalitatea de pregătire de unele infracțiuni care implică producerea de daune în proporții mari sau deosebit de mari (de exemplu, a infracțiunilor prevăzute la art. 245^3, alin. (3) art. 245^{10}, alin. (1) sau (3) art. 245^{12}, art. 260^6 etc. din Codul penal). În asemenea cazuri, daunele în proporții mari sau deosebit de mari sunt legate cauzal nu de accesul ilegal la informația computerizată, ci de faptele descrise ca *verbum regens* în art. 245^3, alin. (3) art. 245^{10}, alin. (1) sau (3) art. 245^{12}, art. 260^6 etc. din Codul penal.

Indiferent de varianta sub care se prezintă latura obiectivă a infracțiunilor prevăzute la art. 259 CP RM, fapta prejudiciabilă trebuie să preceadă urmările prejudiciabile. Dacă este invers – urmările prejudiciabile sunt prezente înainte de săvârșirea faptei prejudiciabile – atunci lipsește temeiul aplicării art. 259 CP RM. De asemenea, acțiunea principală trebuie să preceadă acțiunea adiacentă. Dacă este invers – acțiunea adiacentă este comisă înainte de săvârșirea acțiunii principale – atunci lipsește temeiul aplicării art. 259 CP RM.

În afară de aceasta, fapta prejudiciabilă, prevăzută la art. 259 CP RM, trebuie să reprezinte cauza indispensabilă a survenirii urmărilor prejudiciabile specificate în acest articol. Este posibil ca această cauză să fie însoțită de alte cauze, însă aceste alte cauze nu pot fi suficiente pentru a determina producerea urmărilor prejudiciabile prevăzute la art. 259 CP RM. Cu alte cuvinte, în lipsa faptei prejudiciabile, prevăzute la art. 259 CP RM, aceste urmări nu au cum să survină. Dacă ele totuși survin, atunci nu din cauza săvârșirii faptei prejudiciabile prevăzute la art. 259 CP RM. În asemenea condiții, lipsește temeiul aplicării acestui articol.

Modificarea sau deteriorarea datelor informatice ţinute într-un sistem informatic ori restricţionarea ilegală a accesului la aceste date, care produce daune în proporţii mari, nu trebuie să fie antecedentă în plan cauzal față de acțiunea de acces ilegal la informația computerizată. În caz contrar, se va aplica nu art. 260^2 CP RM, dar art. 259 CP RM.

Perturbarea funcţionării unui sistem informatic prin modificarea sau deteriorarea datelor informatice sau prin restricţionarea accesului la aceste date, care produce daune în proporţii mari sau deosebit de mari, nu trebuie să fie antecedentă în plan cauzal față de acțiunea de acces ilegal la informația computerizată. În caz contrar, se va aplica nu art. 260^3 CP RM, dar art. 259 CP RM.

Pentru a fi aplicat art. 261 CP RM, denaturarea sau distrugerea informaţiei computerizate, care produce daune în proporţii mari sau deosebit de mari, trebuie să fie antecedentă în plan cauzal față de acțiunea sau inacțiunea de încălcare a regulilor de „colectare, prelucrare, păstrare, difuzare, repartizare a informaţiei ori a regulilor de protecţie a sistemului informatic, prevăzute în conformitate cu statutul informaţiei sau gradul ei de protecţie”.[2206] Dacă însă denaturarea sau distrugerea informaţiei computerizate, care produce daune în proporţii mari sau deosebit de mari, este antecedentă în plan cauzal față de acțiunea de acces ilegal la informația computerizată, atunci se va aplica art. 259 CP RM.

3.3. Rezultatele obținute în urma analizei de drept penal a laturii subiective a infracțiunilor prevăzute la art. 259 CP RM

În art. 259 CP RM nu este indicată forma de vinovăție – intenția sau imprudența. Prin aceasta art. 259 CP RM se deosebește de art. 145, 150, 151, 152, 157, 166^1 sau alte articole din Codul penal, în care este specificată una dintre aceste forme.

Semantismul noțiunii „acces ilegal la informaţia computerizată” ce se referă la acțiunea principală din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, denotă că această acțiune poate fi săvârșită doar cu intenție. În mod firesc, dacă acțiunea principală este săvârșită cu intenție, atunci acțiunea adiacentă, care o însoțește, trebuie să fie săvârșită, de asemenea, cu intenție.

Infracțiunile, prevăzute la art. 259 CP RM, pot fi săvârșite doar cu intenție. Conform art. 17 CP RM, „se consideră că infracțiunea a fost săvârșită cu intenție dacă persoana care a săvârșit-o își dădea seama de caracterul prejudiciabil al acțiunii sau inacțiunii sale”[2207], „a prevăzut urmările ei prejudiciabile, le-a dorit sau admitea, în mod conștient, survenirea acestor urmări”.[2208] Atrage atenția partea finală a acestei definiții: „le-a dorit sau admitea, în mod conștient, survenirea acestor urmări”.[2209] Conjuncția „sau” din această parte denotă că intenția cunoaște două tipuri care se diferențiază în funcție de voința (factorul volitiv) care se manifestă în raport cu urmările prejudiciabile. Astfel, intenția este directă dacă făptuitorul a dorit survenirea urmărilor prejudiciabile; intenția este indirectă dacă făptuitorul admitea, în mod conștient, survenirea acestor urmări.

[2206] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2207] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2208] Ibidem.
[2209] Ibidem.

Infracţiunile, prevăzute la art. 259 CP RM, pot fi comise cu intenţie directă sau cu intenție indirectă. Într-adevăr, deoarece infracțiunile prevăzute la art. 259 CP RM sunt infracțiuni materiale, regula este că subiectul acestor infracțiuni manifestă intenție directă sau indirectă. Singura excepție la această regulă este cea de la lit. f) alin. (2) art. 259 CP RM. În acest caz, întrucât făptuitorul urmărește un scop special, intenția poate fi doar directă.

În concluzie, se poate susține: în cazul infracțiunilor, prevăzute la art. 259 CP RM (cu excepția lit. f) alin. (2)), făptuitorul îşi dă seama de caracterul prejudiciabil al acțiunii de acces ilegal la informaţia computerizată, precum și al acțiunii de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei, de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, prevede urmările prejudiciabile care constau fie în distrugerea, deteriorarea sau modificarea informaţiei ori în dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor în proporţii mari sau deosebit de mari, fie în daunele în proporţii mari sau deosebit de mari, și dorește ori admite, în mod conștient, survenirea unor astfel de urmări. În ipoteza prevăzută la lit. f) alin. (2) art. 259 CP RM, făptuitorul îşi dă seama de caracterul prejudiciabil al acțiunii de acces ilegal la informaţia computerizată cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice, în scopul săvârşirii uneia dintre infracţiunile prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6 CP RM, precum și al acțiunii de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei, de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, prevede urmările prejudiciabile care constau fie în distrugerea, deteriorarea sau modificarea informaţiei ori în dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor în proporţii mari, fie în daunele în proporţii mari, și dorește survenirea acestor urmări.

Accesul din imprudență sau fără vinovăție la informaţia computerizată este posibil, însă nu trebuie calificat în baza art. 259 CP RM. Intenția de acces la informaţia computerizată poate fi demonstrată prin: depunerea de către făptuitor a unor eforturi de recurgere la parole, coduri sau alte asemenea mijloace necesare violării sistemelor de protecție; ignorarea de către făptuitor a mesajelor de avertizare care apar pe ecranul calculatorului; sfidarea interdicțiilor verbale de accesare a informației computerizate, etc. În cazurile în care există dubii privind forma de vinovăție, se va lua în considerare: numărul și repetabilitatea solicitărilor de acces la informaţia computerizată; perseverenţa făptuitorului în accesarea informaţiei computerizate; cunoştinţele, abilitățile și experiența făptuitorului în ceea ce privește domeniul informatic, etc.

Recomandăm completarea art. 6 CP RM cu alineatul (3) care are avea următoarea dispoziție: „Fapta săvârșită din imprudență constituie infracțiune numai atunci când o prevede în mod

expres norma din partea specială din prezentul cod”.[2210] În afară de aceasta, trebuie excluse referirile la intenție din toate normele părții speciale a Codului penal al Republicii Moldova, în care se menționează această formă de vinovăție.

În altă privință, mai corect este să vorbim despre semne principale și semne secundare ale laturii subiective a infracțiunii, nu despre semne obligatorii și semne facultative ale laturii subiective a infracțiunii. Vinovăția este semnul principal al laturii subiective a infracțiunii, iar motivul, scopul și emoțiile reprezintă semnele secundare ale acesteia. Are caracter obligatoriu orice semn secundar al laturii subiective a infracțiunii, în lipsa căruia fapta nu poate fi considerată infracțiune.

Motivul infracțiunii este cel care ne ajută să găsim răspunsul la întrebarea „De ce a fost săvârșită infracțiunea?”. Scopul infracțiunii ne ajută să găsim răspunsul la întrebarea „Pentru ce a fost săvârșită infracțiunea?”. Pentru cineva poate părea că aceste două întrebări au același conținut. Însă, realitatea este alta. Atunci când întrebăm de ce a fost săvârșită infracțiunea, stabilim imboldul lăuntric care l-a determinat pe făptuitor să ajungă la concluzia că infracțiunea trebuie săvârșită. Atunci când întrebăm pentru ce a fost săvârșită infracțiunea, stabilim obiectivul pe care făptuitorul urmărește să-l realizeze prin comiterea infracțiunii. Astfel, dacă motivul infracțiunii se află la originea acesteia, atunci scopul infracțiunii reprezintă vectorul și, totodată, finalitatea proiectată a acesteia.[2211]

Trebuie de precizat că să aplică doar art. 260^6 CP RM în cazul când accesul ilegal la informația computerizată este urmat de introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă aceste acţiuni au cauzat daune în proporţii mari sau deosebit de mari. În acest caz, este prezent interesul material. Totodată, acest motiv apare nu în contextul uneia dintre infracțiunile prevăzute la art. 259 CP RM. Accesul ilegal la informația computerizată *per se* constituie etapa de pregătire de una dintre infracțiunile prevăzute la art. 260^6 CP RM.

Aceasta nu înseamnă că, în cazul infracțiunilor prevăzute la art. 259 CP RM, interesul material nu este posibil în genere. În cazul acestor infracțiuni, acest motiv poate presupune, de exemplu, năzuința făptuitorului de a obține un câștig material din distribuirea contra plată a informației computerizate accesate și copiate ilegal.

[2210] STRÎMBEANU, Alexandru. *Răspunderea penală pentru accesul ilegal la informaţia computerizată: Monografie*. Chişinău: Tipografia Centrală, 2023, p. 390. 430 p. ISBN 978-5-88554-178-7.

[2211] STRÎMBEANU, Alexandru. Elementele constitutive subiective ale infracțiunilor de acces ilegal la informația computerizată (art. 259 din Codul penal al Republicii Moldova). [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313475

Important este ca, indiferent de motivul care-l determină pe făptuitor să săvârșească una dintre infracțiunile prevăzute la art. 259 CP RM, motivul să apară până la momentul comiterii infracțiunii. Pentru existența infracțiunii, nu este obligatoriu ca motivul să fie realizat, obiectivizat. Or, ca semn al laturii subiective, motivul infracțiunii trebuie să caracterizeze conștiința și voința făptuitorului.

Cât privește scopul infracțiunii, acesta este prezent și în alte cazuri decât cel prevăzut la lit. f) alin. (2) art. 259 CP RM. În asemenea cazuri, scopul infracțiunii nu este special și poate fi luat în considerare doar la individualizarea pedepsei. Dacă vorbim despre alte cazuri decât cel prevăzut la lit. f) alin. (2) art. 259 CP RM, atunci este important ca scopul infracțiunii să presupună săvârşirea altor infracțiuni decât cele „prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6”.

Starea emoțională a făptuitorului (de exemplu, starea de afect a acestuia) nu este indicată în art. 259 CP RM. Deci, o asemenea stare nu poate influența calificarea faptei în baza art. 259 CP RM.

3.4. Rezultatele obținute în urma analizei de drept penal a subiectului infracțiunilor prevăzute la art. 259 CP RM

Este necesar ca subiectul - persoană fizică al infracţiunilor, ce sunt prevăzute de art. 259 CP RM, să îndeplinească condițiile următoare:

1) să fie responsabil;

2) la momentul săvârșirii infracţiunii să fi atins vârsta de 16 ani.

Absența oricăreia dintre aceste condiții echivalează cu lipsa subiectului infracţiunii și, în ultimă instanță, a temeiului de aplicare a art. 259 CP RM.

Condiția, legată de responsabilitatea subiectului infracţiunilor prevăzute la art. 259 CP RM, rezultă din art. 22 CP RM. Din art. 22 CP RM derivă că responsabilitatea posedă următoarele caracteristici:

1) este o stare psihologică a persoanei;

2) presupune că persoana are: a) capacitatea de a înţelege caracterul prejudiciabil al faptei şi b) capacitatea de a-şi manifesta voinţa şi a-şi dirija acţiunile.

În alin. (1) art. 23 CP RM sunt menționate cauzele iresponsabilității: boală psihică cronică; tulburarea psihică temporară; altă stare patologică. În fine, în acord cu aceeași normă, persoana care, în timpul săvârşirii unei fapte prejudiciabile, se afla în stare de iresponsabilitate, nu este pasibilă de răspundere penală. În raport cu o astfel de persoană, „în baza hotărârii instanţei de

judecată, pot fi aplicate măsuri de constrângere cu caracter medical”[2212], prevăzute de art. 99 CP RM: a) „internarea într-o instituţie psihiatrică cu supraveghere obişnuită”[2213]; b) „internarea într-o instituţie psihiatrică cu supraveghere riguroasă”.[2214]

În acord cu alin. (2) art. 23 CP RM, nu este pasibilă de pedeapsă persoana care îndeplinește următoarele condiții:

1) „a săvârşit infracţiunea în stare de responsabilitate”[2215];

2) „înainte de pronunţarea sentinţei de către instanţa de judecată s-a îmbolnăvit de o boală psihică”[2216] „care a lipsit-o de posibilitatea de a-şi da seama de acţiunile ori inacţiunile sale sau de a le dirija”.[2217]

În raport cu o astfel de persoană, în temeiul hotărârii instanţei de judecată, pot fi aplicate măsuri de constrângere cu caracter medical, prevăzute de art. 99 CP RM. După însănătoşirea unei astfel de persoane, ea poate fi supusă pedepsei.

O a treia stare psihologică cu relevanță penală, alta decât responsabilitatea și iresponsabilitatea, este responsabilitatea redusă. R. Berdilo susține: „Responsabilitatea redusă, ca și responsabilitatea și iresponsabilitatea, este un tip aparte de măsură a capacității persoanei de a-şi da seama de acţiunea sau inacţiunea sa ori de a o dirija”.[2218]

Din art. 23^1 CP RM rezultă următoarele caracteristici ale persoanei cu responsabilitate redusă:

1) „a săvârşit o infracţiune ca urmare a unei tulburări psihice”[2219];

2) „această tulburare psihică a fost constatată prin expertiza medicală efectuată în modul stabilit”[2220];

3) „din cauza acestei stări, persoana respectivă: a) nu-şi putea da seama pe deplin de caracterul şi legalitatea faptelor sale”[2221] „sau b) nu le putea dirija pe deplin”[2222].

Așa cum s-a relevat mai sus, în conformitate cu lit. d) alin. (1) art. 76 CP RM, comiterea faptei de către o persoană ce are o responsabilitate redusă se consideră circumstanță atenuantă care se ia în calcul la stabilirea pedepsei.

[2212] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2213] Ibidem.
[2214] Ibidem.
[2215] Ibidem.
[2216] Ibidem.
[2217] Ibidem.
[2218] BERDILO, Rodica. Responsabilitatea redusă și starea emoțională a subiectului infracțiunilor prevăzute la art. 146, 147 și 156 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 3, pp. 150-159. ISSN 1814-3199.
[2219] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2220] Ibidem.
[2221] Ibidem.
[2222] Ibidem.

În alt context, analiza alin. (3) art. 21 CP RM denotă că persoana juridică poate avea calitatea de subiect al faptelor infracționale, ce sunt prevăzute de art. 259 CP RM, dacă această persoană nu a îndeplinit sau a îndeplinit necorespunzător dispozițiile directe ale legii ce stabilesc îndatoriri sau interdicții privind accesul la informația computerizată. În plus, din alin. (3) art. 21 CP RM rezultă că persoana juridică poate avea calitatea de subiect al infracțiunilor, prevăzute la art. 259 CP RM, dacă: a) accesul ilegal la informația computerizată a fost săvârșit în interesul persoanei juridice respective de către o persoană fizică împuternicită cu funcții de conducere, care a acționat independent sau ca parte a unui organ al persoanei juridice; b) accesul ilegal la informația computerizată a fost admis sau autorizat, sau aprobat, sau utilizat de către persoana împuternicită cu funcții de conducere; c) accesul ilegal la informația computerizată a fost săvârșit datorită lipsei de supraveghere și control din partea persoanei împuternicite cu funcții de conducere.

Pentru a înțelege mai bine condițiile ce caracterizează aceste trei ipoteze, legiuitorul definește în alin. (3^1) art. 21 CP RM noțiunea de persoană împuternicită cu funcții de conducere. Astfel, se disting trei categorii de funcții de conducere pe care le exercită persoana respectivă: a) funcția de reprezentare a persoanei juridice; b) funcția de luare a deciziilor în numele persoanei juridice; c) funcția de exercitare a controlului în cadrul persoanei juridice.

În alt context, în cadrul analizei laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, am afirmat că această sintagmă este nu altceva decât extensia termenului „ilegal” din această dispoziție, menită să concretizeze semantismul termenului „ilegal” în contextul particular al infracțiunilor prevăzute de art. 259 CP RM. Mai mult, în cadrul aceleiași analize, am examinat următoarele trei ipoteze:

1) lipsa de autorizare în temeiul legii sau al unui contract de a accesa informația computerizată;

2) depășirea limitelor de autorizare de a accesa informația computerizată;

3) lipsa permisiunii persoanei competente de a folosi, a administra sau a controla un sistem informatic ori a desfăşura cercetări ştiinţifice sau a efectua orice altă operaţiune într-un sistem informatic.

Ca urmare, nu considerăm necesar să ne repetăm. Calitatea specială a subiectului infracțiunilor, prevăzute la art. 259 CP RM, poate fi lesne stabilită prin raportare la analiza celor trei ipoteze enunțate mai sus.

Subiecți ai infracțiunilor, prevăzute la art. 259 CP RM, pot fi persoanele care *au dreptul de acces* anume la un calculator, la un suport material de informaţie, la un sistem informatic sau la o rețea informatică. În același timp, asemenea persoane *nu trebuie să aibă dreptul de acces* la

informația computerizată din calculatorul, de pe suportul material de informaţie, din sistemul informatic sau din reţeaua informatică la care au acces legal.

Revenind la persoanele, care au drept de acces la un calculator, la un suport material de informaţie, la un sistem informatic sau la o rețea informatică, trebuie să vorbim despre folosirea situației de serviciu de către unele dintre aceste persoane.

În contextul analizei laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, am menționat: în anumite cazuri, accesul ilegal la informația computerizată *per se* poate forma conținutul unei fapte penale sau contravenționale. De exemplu, accesul ilegal la informația computerizată *per se* poate reprezenta un exemplu de folosire ilegală a situației de serviciu (exprimat în accesarea informației computerizate în calitate de persoană autorizată în virtutea funcției pe care o deține făptuitorul). Într-un asemenea caz (dacă, desigur, sunt întrunite toate celelalte condiții stabilite în art. 327, 335 sau 370 CP RM ori în art. 312 CC RM), se va aplica unul dintre aceste articole. Apreciind în ansamblu cele comise, faptele, prevăzute la art. 327, 335 sau 370 CP RM ori la art. 312 CC RM, vor forma concurs cu una dintre infracțiunile prevăzute la art. 145, 177, 185^1, 185^2, 189 etc. din Codul penal.

Însă, este posibilă o altă ipoteză. În legătură cu această ipoteză, nu poate fi ignorată următoarea întrebare: care trebuie să fie calificarea dacă situația de serviciu este folosită ilegal pentru a accesa ilegal informaţia computerizată și pentru a distruge, deteriora, modifica, bloca sau copia informaţia, ori pentru a deregla funcţionarea calculatoarelor, a sistemului sau a reţelei informatice, şi dacă s-au cauzat daune în proporţii mari sau deosebit de mari?

Considerăm că, într-o asemenea ipoteză, trebuie aplicate art. 259 CP RM și art. 312 CC RM. Este posibil concursul infracțiunilor prevăzute la art. 259 CP RM, pe de o parte, și al infracțiunilor prevăzute la art. 327, 335 sau 370 CP RM, pe de altă parte, numai dacă abuzul de putere sau abuzul de serviciu produce daunele prevăzute de art. 327, 335 sau 370 CP RM. Contează ca aceste daune să fie altele decât daunele produse de infracțiunile prevăzute la art. 259 CP RM.

Soluțiile de calificare, prezentate mai sus, condiționează inutilitatea unei eventuale completări a art. 259 CP RM cu o dispoziție în care ar fi stabilită circumstanța agravantă „cu folosirea situației de serviciu”.

3.5. Rezultatele obținute în urma analizei de drept penal a circumstanțelor agravante ale infracțiunilor prevăzute la art. 259 CP RM

Infracțiunile prevăzute la art. 259 CP RM, au o componență specială.

Astfel, chiar în dispoziția de la alin. (1) art. 259 CP RM este reliefată calitatea specială a subiectului infracțiunilor de acces ilegal la informația computerizată: „[...] al unei persoane care nu este autorizată în temeiul legii sau al unui contract”[2223], „depăşeşte limitele autorizării ori nu are permisiunea persoanei competente să folosească”[2224], „să administreze sau să controleze un sistem informatic ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic [...]”.[2225] Pe această cale, legiuitorul sugerează că subiectul infracțiunilor, prevăzute la art. 259 CP RM, posedă calitatea specială de persoană care nu are dreptul de acces la informația computerizată dintr-un calculator, de pe un suport material de informaţie, dintr-un sistem informatic sau dintr-o reţea informatică.

Fără doar și poate, persoanele, care nu dețin calitatea specială reliefată în alin. (1) art. 259 CP RM, nu pot leza obiectul juridic al infracțiunilor prevăzute de acest articol. Amintim că obiectul juridic principal al acestor infracțiuni îl formează relaţiile sociale cu privire la accesul autorizat sau permis la informaţia computerizată. Dacă o persoană are dreptul de acces la informația computerizată dintr-un calculator, de pe un suport material de informaţie, dintr-un sistem informatic sau dintr-o reţea informatică, atunci fapta acesteia nu poate să aducă atingere relaţiilor sociale cu privire la accesul autorizat sau permis la respectiva informaţie computerizată.

În afară de aceasta, persoanele, care nu posedă calitatea specială reliefată în alin. (1) art. 259 CP RM, nu pot realiza nemijlocit latura obiectivă a infracțiunilor prevăzute de acest articol. În cadrul analizei laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, am afirmat că sintagma „[...] al unei persoane care nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării”[2226] „ori nu are permisiunea persoanei competente să folosească, să administreze sau să controleze un sistem informatic”[2227] „ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic [...]” este extensia termenului „ilegal” din dispoziția de la alin. (1) art. 259 CP RM, menită să concretizeze semantismul termenului „ilegal” în contextul particular al infracțiunilor prevăzute de art. 259 CP RM. Dacă o persoană are dreptul de acces la informația computerizată dintr-un calculator, de pe un suport

[2223] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2224] Ibidem.
[2225] Ibidem.
[2226] Ibidem.
[2227] Ibidem.

material de informaţie, dintr-un sistem informatic sau dintr-o reţea informatică, atunci nu poate avea un caracter ilegal accesul acestei persoane la respectiva informație computerizată dintr-un calculator, de pe un suport material de informaţie, dintr-un sistem informatic sau dintr-o reţea informatică.

Nu în ultimul rând, persoanele, care nu posedă calitatea specială reliefată în alin. (1) art. 259 CP RM, nu pot avea atitudinea psihică specifică infracțiunilor prevăzute de acest articol. Cu această ocazie, amintim că, în cazul infracțiunilor, prevăzute la art. 259 CP RM (cu excepția lit. f) alin. (2)), făptuitorul este conștient de caracterul prejudiciabil al acțiunii de acces ilegal la informaţia computerizată, precum și al acțiunii de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei, de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, prevede urmările prejudiciabile care constau fie în distrugerea, deteriorarea sau modificarea informaţiei ori în dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor în proporţii mari sau deosebit de mari, fie în daunele în proporţii mari sau deosebit de mari, și dorește sau admite, în mod conștient, survenirea acestor urmări. În ipoteza prevăzută la lit. f) alin. (2) art. 259 CP RM, făptuitorul îşi dă seama de caracterul prejudiciabil al acțiunii de acces ilegal la informaţia computerizată cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice, în scopul săvârşirii uneia dintre infracţiunile prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6 CP RM, precum și al acțiunii de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei, de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, prevede urmările prejudiciabile care constau fie în distrugerea, deteriorarea sau modificarea informaţiei ori în dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor în proporţii mari, fie în daunele în proporţii mari, și dorește survenirea acestor urmări.

În mod cert, nu poate manifesta o astfel de atitudine psihică acea persoană care are dreptul de acces la informația computerizată dintr-un calculator, de pe un suport material de informaţie, dintr-un sistem informatic sau dintr-o reţea informatică.

În concluzie, accesul ilegal la informaţia computerizată, care este săvârșit de două ori mai multe persoane (lit. b) alin. (2) art. 259 CP RM), presupune ipoteza exclusivă a prezenței a cel puțin doi coautori care au cu toții calitatea specială reliefată în alineatul (1) al acestui articol. Persoanele, care nu sunt pasibile de răspundere penală (din cauza vârstei, iresponsabilității etc.), nu se au în vedere în dispoziția de la lit. b) alin. (2) art. 259 CP RM.

Săvârșirea infracțiunii de către un grup criminal organizat nu este specificată în art. 259 CP RM ca circumstanță agravantă. De aceea, în cazul săvârșirii uneia dintre infracțiunile prevăzute de acest articol de către un grup criminal organizat, se va aplica lit. b) alin. (2) art. 259 CP RM.

Or, atât argumentul logic *a minore ad maius* (care denotă o deducție de la mai mic la mai mare), cât și interpretarea sistemică a art. 41, 43 și 46 CP RM, duc spre concluzia că orice grup criminal organizat constituie o reuniune, o asociere a două ori mai multor persoane care îndeplinesc condițiile stabilite în alin. (6) art. 42 CP RM. În ipoteza prevăzută la lit. b) alin. (2) art. 259 CP RM atestăm nu simplamente o pluralitate de făptuitori, dar o participaţie care presupune săvârşirea infracțiunii prin participarea împreună, cu rol de coautori, a două ori mai multor persoane, fiecare realizând latura obiectivă a infracţiunii. O astfel de participație este prezentă în cazul oricărui grup criminal organizat. Or, în cazul grupului criminal organizat, în afară de prezența a doi sau mai mulți coautori, este necesară îndeplinirea altor condiții: 1) caracterul stabil al grupului; 2) organizarea în prealabil a membrilor grupului pentru a comite una sau mai multe infracţiuni.[2228]

În alt context, ipoteza, care este prevăzută la lit. b) alin. (2) art. 259 CP RM, nu exclude prezența unor participanți secundari (organizator, instigator, complice). Această posibilitate rezultă din analiza art. 45 CP RM. Potrivit alineatului (1) al acestui articol, „infracţiunea se consideră săvârşită cu participaţie complexă dacă la săvârşirea ei participanţii au contribuit în calitate de autor, organizator, instigator sau complice”.[2229] Totodată, conform lit. b) alin. (2) art. 45 CP RM, „latura obiectivă a infracţiunii cu participaţie complexă poate fi realizată [...] de doi sau mai mulţi autori”.[2230] Rezultă că latura obiectivă a infracţiunii cu participaţie complexă poate fi executată de către doi sau mai mulţi coautori, iar la această executare să-și aducă contribuția un organizator sau mai mulți organizatori, un instigator sau mai mulți instigatori, un complice sau mai mulți complici.

Din dispoziția de la lit. a) alin. (2) art. 45 CP RM rezultă că latura obiectivă a infracţiunii cu participaţie complexă poate fi realizată de către un singur autor. Dacă infracțiunea este săvârșită de către un singur autor, iar alte persoane apar în rolul de organizator, instigator sau complice, atunci lipsește temeiul aplicării lit. b) alin. (2) art. 259 CP RM.

Infracțiunea, prevăzută la art. 260 CP RM, poate fi considerată exemplu de complicitate *sui generis*, printre altele, la oricare dintre infracțiunile prevăzute la art. 259 CP RM. Or, din dispoziția art. 260 CP RM se desprinde că scopul infracțiunii, prevăzute de acest articol, poate consta în săvârşirea uneia dintre infracţiunile prevăzute la art. 259 CP RM. Nu se exclude ca, în

[2228] Din considerente asemănătoare, în situația săvârșirii uneia dintre infracțiunile prevăzute de art. 259 CP RM de către o organizație criminală, se va aplica lit. b) alin. (2) art. 259 CP RM.
[2229] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2230] Ibidem.

această ipoteză, cel, care comite una dintre infracţiunile, prevăzute la art. 259 CP RM, să nu fie autorul infracțiunii prevăzute la art. 260 CP RM.

În mod similar, oricare dintre infracțiunile, care sunt prevăzute în art. 260^4 CP RM, poate fi considerată exemplu de complicitate *sui generis*, printre altele, la oricare dintre infracțiunile prevăzute la art. 259 CP RM. Or, din dispoziția art. 260^4 CP RM se desprinde că scopul infracțiunii, prevăzute de acest articol, poate consta în săvârşirea uneia dintre infracţiunile prevăzute la art. 259 CP RM. Nu se exclude ca, în această ipoteză, cel, care comite una dintre infracţiunile, ce sunt specificate în art. 259 CP RM, să nu fie autorul infracțiunii prevăzute la art. 260^4 CP RM.

În consecință, se poate afirma că art. 260 și 260^4 CP RM constituie rezultatul unei transpuneri indirecte a prevederilor alin. (1) art. 8 din Directiva 2013/40/UE și a alin. 1 art. 11 al Convenției de la Budapesta.

În alt context, în Codul penal al Republicii Moldova nu găsim definiția noțiunii „sisteme de protecție", care se utilizează la lit. c) alin. (2) art. 259 CP RM. Din acest motiv suntem nevoiți să căutăm sensul acestei noțiuni în alte surse normative. Interpretarea acestor surse normative ne determină să afirmăm că în art. 259 CP RM sintagma „cu violarea sistemelor de protecţie" trebuie înlocuită prin sintagma „prin violarea măsurilor de securitate". În afară de aceasta, adaptând definiția noțiunii „măsuri de securitate" din art. 2 al Legii nr. 20/2009 la necesitățile art. 259 CP RM, recomandăm completarea Capitolului XIII din partea generală a Codului penal al Republicii Moldova cu art. 134^{27} ce ar urma să aibă următorul conținut: „Prin măsuri de securitate, în sensul art. 259, se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la informația computerizată este restricţionată sau interzisă pentru anumite categorii de utilizatori".[2231]

În sensul lit. c) alin. (2) art. 259 CP RM, prin „protecție" se are în vedere protecția împotriva accesului ilegal la informația computerizată, nu protecția împotriva accesului ilegal la: 1) calculatorul, suportul material de informaţie, sistemul sau reţeaua informatică, care conțin informația computerizată ce poate fi accesată ilegal; 2) încăperea, alt loc pentru depozitare sau locuința în care se află calculatorul, suportul material de informaţie, sistemul sau reţeaua informatică, care conțin informația computerizată ce poate fi accesată ilegal.

În accepțiunea lit. c) alin. (2) art. 259 CP RM, au relevanță măsurile de securitate împotriva accesului ilegal nu la sistemul informatic, ci la informația computerizată din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică.

[2231] STRÎMBEANU, Alexandru. *Răspunderea penală pentru accesul ilegal la informaţia computerizată: Monografie*. Chișinău: Tipografia Centrală, 2023, p. 390. 430 p. ISBN 978-5-88554-178-7.

În altă privință, sintagma „canalele de telecomunicaţii”, care este folosită la lit. d) alin. (2) art. 259 CP RM, nu este nici clară, nici previzibilă. Noțiunea „canale de telecomunicaţii” nu este definită nici în Codul penal al Republicii Moldova, nici în legislația extrapenală a Republicii Moldova. Există o probabilitate mare că la lit. d) alin. (2) art. 259 CP RM, prin „canalele de telecomunicaţii” se înțelege „reţeaua de comunicaţii electronice” în sensul art. 2 al Legii nr. 241/2007.[2232]

Dispoziția de la lit. d) alin. (2) art. 259 CP RM este aplicabilă, dacă noțiunea „rețea informatică” se intersectează cu noțiunea „rețea de comunicații electronice” (adică în ipoteza în care rețeaua de comunicații electronice oferă posibilitatea realizării unui schimb de date informatice). *Per a contrario,* dacă noțiunea „rețea informatică” nu se intersectează cu noțiunea „rețea de comunicații electronice”, atunci se aplică art. 259 CP RM (cu excepția lit. d) alin. (2)).

Concursul ideal al infracțiunilor prevăzute la lit. d) alin. (2) art. 259 și art. 261^1 CP RM prezintă dezavantajul luării în considerare la calificare de două ori a calității de rețea de comunicații electronice. Drept urmare, propunem abrogarea lit. d) alin. (2) art. 259 CP RM. Efectul unei asemenea abrogări va consta în reținerea la calificare o singură dată a calității de rețea de comunicații electronice.

În alt context, noțiunea „mijloace tehnice speciale” este definită în Hotărârea Guvernului nr. 100/2009. În Anexa nr. 2 la acest act normativ sunt specificate, între altele, mijloacele tehnice speciale destinate pentru obţinerea accesului neautorizat la informaţiile stocate în sistemele informaţionale şi pe alte mijloace tehnice de păstrare a informaţiei. Anume acest tip de mijloace tehnice speciale își găsește relevanța în ipoteza prevăzută la lit. e) alin. (2) art. 259 CP RM.

În contextul analizei laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, am susținut că fapta infracțională, ce este prevăzută la art. 260 CP RM, poate fi considerată un exemplu de pregătire *sui generis* de infracțiunile prevăzute la art. 259 CP RM. Aceasta înseamnă că aplicarea art. 260 CP RM exclude aplicarea art. 26 și 259 CP RM.

Atunci când este vorba de o altă persoană decât cea care comite una dintre infracțiunile prevăzute la art. 259 CP RM, infracțiunea, prevăzută la art. 260 CP RM, poate fi considerat un exemplu de complicitate *sui generis* la una dintre infracțiunile prevăzute la art. 259 CP RM. Aceasta înseamnă că aplicarea art. 260 CP RM exclude aplicarea alin. (5) art. 42 și art. 259 CP RM.

[2232] Legea comunicațiilor electronice: nr. 241 din 15.11.2007. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 51-54, 155.

În context, apare următoare întrebare: care este relația dintre pregătirea sau complicitatea la infracțiunea prevăzută la lit. e) alin. (2) art. 259 CP RM, pe de o parte, și infracțiunea prevăzută la art. 260 CP RM / art. 301^1 CP RM sau art. 261 din Codul contravențional, pe de altă parte?

Pentru a fi considerat mijloc tehnic special, mijlocul tehnic trebuie să îndeplinească condițiile stabilite în Hotărârea Guvernului nr. 100/2009. În același timp, din art. 260 CP RM, nu rezultă clar dacă noțiunea „mijloc tehnic" include sensul de „mijloc tehnic special" sau nu. Nu este clar nici care dintre următoarele norme este generală și care specială: 1) art. 260 CP RM sau 2) art. 301^1 CP RM ori art. 261 CC RM. În aceste condiții, aplicăm principiul subsidiarității și alegem art. 260 CP RM. Or, acest articol stabilește un regim sancționator mai aspru în comparație cu art. 301^1 CP RM și cu art. 261 CC RM.

Firește, nu se admite aplicarea concomitentă atât a art. 260 CP RM, cât și a art. 301^1 CP RM sau a art. 261 CC RM. În caz contrar, calitatea de de mijloc tehnic special va fi reținută de două ori la calificare. Ceea ce ar fi inechitabil.

În alt context, ipoteza, descrisă la lit. f) alin. (2) art. 259 CP RM, presupune următoarele: acțiunea principală de acces ilegal la informaţia computerizată este urmată de acțiunea terțiară de utilizare ilegală a calculatorului, sistemului sau reţelei informatice, iar, ulterior, succedată de acțiunea adiacentă de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, prin care se cauzează daune în proporţii mari. În plus, acțiunea terțiară sus-menționată are scopul special de săvârşire a uneia dintre infracţiunile ce sunt prevăzute de alin. (1) art. 259, art. 260^1-260^3, 260^5 şi 260^6 CP RM. În acest caz, întrucât făptuitorul urmărește un scop special, intenția poate fi doar directă.

Recomandăm abrogarea dispoziției de la lit. f) alin. (2) art. 259 CP RM. Primul argument este că această circumstanță agravantă presupune sancționarea dublă a aceleiași fapte în cazul în care scopul special, care este menționat la lit. f) alin. (2) art. 259 CP RM, își găsește realizarea. Or, în afară de aceea că se aplică alin. (1) art. 259, art. 260^1-260^3, 260^5 şi 260^6 CP RM, se agravează răspunderea în baza lit. f) alin. (2) art. 259 CP RM. În acest mod, este supraevaluat pericolul social al celor săvârșite.[2233]

Alt argument constă în incoerența prevederii de la lit. f) alin. (2) art. 259 CP RM. Or, scopul, menționat în această normă, presupune săvârșirea, între altele, a infracțiunilor care sunt prevăzute de art. 260^2, 260^3, 260^5 și 260^6 CP RM. Aceste articole prevăd răspunderea, printre

[2233] STRÎMBEANU, Alexandru. Circumstanțele agravante ale infracțiunilor de acces ilegal la informația computerizată (art. 259 din Codul penal al Republicii Moldova). În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4331505

altele, pentru: „modificarea sau deteriorarea intenţionată a datelor informatice ţinute într-un sistem informatic ori restricţionarea ilegală a accesului la aceste date, dacă aceste acţiuni au cauzat daune în proporţii mari”[2234] (art. 260^2 CP RM); „perturbarea funcţionării unui sistem informatic prin modificarea sau deteriorarea datelor informatice sau prin restricţionarea accesului la aceste date, dacă aceste acţiuni au cauzat daune în proporţii mari”[2235] (art. 260^3 CP RM); „modificarea ilegală a datelor informatice ori restricţionarea ilegală a accesului la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice”[2236] (art. 260^5 CP RM); „modificarea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă aceste acţiuni au cauzat daune în proporţii mari”[2237] (art. 260^6 CP RM).

În același timp, în art. 259 CP RM, ca acțiune adiacentă este specificată, între altele, deteriorarea, modificarea sau blocarea informaţiei computerizate, ori dereglarea funcţionării sistemului informatic, care cauzează daune în proporţii mari. În acest fel există riscul ca, în cazul realizării scopului menționat la lit. f) alin. (2) art. 259 CP RM, să fie sancționată dublu aceeași deteriorare, modificare sau blocare a informaţiei computerizate, ori dereglare a funcţionării sistemului informatic, care cauzează daune în proporţii mari.

Cel mai greu este de înțeles ce are în vedere legiuitorul în una dintre subipotezele indicate la lit. f) alin. (2) art. 259 CP RM: infracțiunea, ce este specificată în alin. (1) art. 259 CP RM, este săvârșită în scopul comiterii unei infracțiuni prevăzute, de asemenea, la alin. (1) art. 259 CP RM. O astfel de intenție de săvârșire repetată a două infracțiuni, prevăzute de aceeași normă, ar presupune următoarele: accesul ilegal la informaţia computerizată, succedat de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, ori de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care a cauzat daune în proporţii mari, se comite în scopul accesului ilegal la informaţia computerizată, care să fie succedat de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, ori de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, și care ar cauza daune în proporţii mari.

Nu este limpede de ce ar fi necesar ca o asemenea construcție să fie statuată în art. 259 CP RM. Dacă, după o infracțiune prevăzută la alin. (1) art. 259 CP RM, este săvârșită o altă

[2234] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
[2235] Ibidem.
[2236] Ibidem.
[2237] Ibidem.

infracțiune prevăzută la aceeași normă, ar fi suficient să vorbim despre concursul real dintre două infracțiuni care este prevăzută de alin. (1) art. 259 CP RM.

În altă ordine de idei, o informație computerizată este protejată de lege atunci când există cel puțin o lege care conține prevederi care stabilesc statutul de informație protejată de lege. Dacă nu poate fi identificată o astfel de lege, rezultă că informația computerizată nu este protejată de lege. Într-un asemenea caz, lipsește temeiul de invocare a lit. g) alin. (2) art. 259 CP RM.

Având în vedere regula stabilită în alin. (2) art. 3 CP RM, nu putem considera legi în sensul lit. g) alin. (2) art. 259 CP RM: hotărârile Parlamentului; decretele Preşedintelui Republicii Moldova; hotărârile şi ordonanţele Guvernului; actele normative ale autorităţilor administraţiei publice centrale de specialitate; actele normative ale autorităţilor publice autonome; actele normative ale autorităţilor unităţilor teritoriale autonome cu statut juridic special; actele normative ale autorităţilor administraţiei publice locale, etc.[2238] Astfel de acte normative nu pot fi considerate legi nici măcar în cazul în care sunt adoptate în temeiul unor legi.

În alt context, lista de caracteristici protejate, care sunt specificate în alin. (1) art. 134^{21} CP RM, are un caracter exhaustiv, limitativ. Alte caracteristici (de exemplu, statutul de migrant sau de azilant al victimei) nu pot sta la baza motivelor de prejudecată în accepțiunea art. 134^{21} CP RM.

Din analiza alin. (1) art. 134^{21} CP RM rezultă că infracțiunea, prevăzută la lit. g^1) alin. (2) art. 259 CP RM, poate fi săvârșită nu doar în privința persoanei care posedă una dintre caracteristicile protejate specificate în alin. (1) art. 134^{21} CP RM. Această infracțiune poate fi comisă, de asemenea, în privința bunurilor persoanei respective ori a bunurilor asociate cu aceasta. Mai mult decât atât, infracțiunea, prevăzută la lit. g^1) alin. (2) art. 259 CP RM, poate fi săvârșită chiar și în privința persoanei ce acordă suport, asistență, ajutor, sprijin persoanelor care posedă asemenea caracteristici protejate ori doar se asociază cu acestea. După cum rezultă din alin. (1) art. 134^{21} CP RM, nu importă dacă această asociere are un caracter real sau doar este percepută de către făptuitor ca având un caracter real.

Din interpretarea alin. (2) art. 134^{21} CP RM desprindem că, pentru aplicarea lit. g^1) alin. (2) art. 259 CP RM, nu este suficient ca accesul ilegal la informația computerizată să fie comis asupra unei persoane care este, spre exemplu, de o altă rasă decât făptuitorul. Într-un asemenea caz, săvârșirea infracțiunii poate fi determinată nu de motivele de prejudecată, dar de motive de alt gen (de exemplu, de interesul material, de răzbunare, de gelozie etc.). Va exista un temei

[2238] STRÎMBEANU, Alexandru. Victima secundară a infracțiunilor prevăzute la art. 259 din Codul penal. În: *Conferința științifică națională cu participare internațională dedicată aniversării a 75-a a Universității de Stat din Moldova „Integrare prin cercetare și inovare" (10-11 noiembrie 2021)*. Chișinău: CEP USM, 2021, pp. 6-8. ISBN 978-9975-152-48-8.

suficient pentru aplicarea lit. g^1) alin. (2) art. 259 CP RM dacă accesul ilegal la informația computerizată a fost comis anume datorită faptului că victima era, de exemplu, de o altă rasă decât făptuitorul. În alți termeni, făptuitorul nu ar fi săvârșit accesul ilegal la informația computerizată dacă victima nu ar fi fost, de exemplu, de o altă rasă decât făptuitorul.

În fine, din interpretarea alin. (3) art. 134^{21} CP RM desprindem că motivele de alt gen (de exemplu: interesul material; răzbunare; gelozie, etc.) pot fi prezente în ipoteza prevăzută la lit. g^1) alin. (2) art. 259 CP RM. Însă, într-un asemenea caz, este obligatoriu ca, pe lângă astfel de motive, să fie prezente motivele de prejudecată. Nu se cere ca motivele de prejudecată să reprezinte motivul dominant, prioritar al infracțiunii. Acestea pot avea chiar și un caracter secundar, subsidiar. Important este ca motivele de prejudecată să-l ghideze pe făptuitor chiar și parțial. Numărul de motive ale infracțiunii, precum și ponderea acestora poate fi avută în vedere în procesul de individualizare a pedepsei stabilite în alin. (2) art. 259 CP RM.

În finalul acestui studiu, vom vorbi despre oportunitatea agravării răspunderii în cazul săvârșirii infracțiunilor, ce sunt prevăzute de art. 259 CP RM, fie asupra unui sistem informatic care este parte integrantă a infrastructurii critice, fie în privința informației sensibile privind protecția infrastructurilor critice. Necesitatea stringentă a unei asemenea completări este dictată de războiul de agresiune dus de Federația Rusă împotriva Ucrainei (care are efecte colaterale asupra Republicii Moldova), precum și de războiul hibrid purtat de către Federația Rusă, printre altele, împotriva Republicii Moldova.

Urmare acestui fapt, propunem completarea alin. (2) art. 259 CP RM cu lit. i) cu următorul conținut: „asupra unui sistem informatic care este parte integrantă a infrastructurii critice”. De asemenea, în scopul perfecționării art. 259 CP RM, propunem completarea alin. (2) art. 259 CP RM cu lit. j) cu următorul conținut: „în privința informației sensibile privind protecția infrastructurilor critice”.

Pentru ca aceste recomandări *de lege ferenda* să aibă efectul scontat, considerăm necesară completarea Capitolului XIII din partea generală a Codului penal al Republicii Moldova cu două articole în care ar fi definite noțiunile „infrastructură critică” și „date informatice[2239] sensibile privind protecția infrastructurilor critice”. Aceste definiții vor avea ca model definițiile aceloraşi noțiuni din Directiva 2008/114/CE, desigur cu operarea ajustărilor corespunzătoare.

La concret, recomandăm completarea Capitolului XIII din partea generală a Codului penal al Republicii Moldova cu următoarele două articole:

[2239] Propunem folosirea sintagmei „date informatice” în locul termenului „informații” pentru a dovedi consecvență și a fi în concordanță cu propunerea de substituire în art. 259 CP RM a sintagmei „informație computerizată” prin sintagma „date informatice”, pe care am făcut-o *supra*.

„Articolul 134[29]. Infrastructură critică

Prin infrastructură critică, în sensul art. 259, se înțelege un element, un sistem sau o componentă a acestuia, aflat pe teritoriul Republicii Moldova, care este esențial pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor, și a căror perturbare sau distrugere ar avea un impact semnificativ pentru Republica Moldova ca urmare a incapacității de a menține respectivele funcții”[2240];

„Articolul 134[30]. Date informatice sensibile privind protecția infrastructurilor critice

Prin date informatice sensibile privind protecția infrastructurilor critice, în sensul art. 259, se înțelege datele informatice cu privire la o infrastructură critică ce ar putea fi utilizate, în cazul divulgării, în scopul planificării și al realizării unor acțiuni care să determine perturbarea sau distrugerea instalațiilor unor infrastructuri critice”.[2241]

3.6. Sinteza problematicii tratate și a rezultatelor obținute în Capitolul 3

Considerăm necesară formularea anumitor concluzii după ce am prezentat rezultatele obținute în urma analizei de drept penal a infracțiunilor ce sunt specificate în art. 259 CP RM:

1) relațiile sociale cu privire la securitatea datelor informatice şi a comunicaţiilor electronice prezintă suficientă semnificație sub aspect axiologic, astfel încât să fie pasibile de apărare penală;

2) nu este admisibilă confundarea noțiunilor „securitatea informațională” și „securitatea informatică (cibernetică)”;

3) în accepția art. 259 CP RM, informația computerizată este informația destinată prelucrării pe un calculator, fixată pe un suport care poate fi citit de un calculator sau transmis într-un mediu care face posibilă interacționarea în cadrul unui sistem informatic sau al unei rețele informatice;

4) datele informatice trebuie privite ca informație reprezentată într-o formă adecvată efectuării de operațiuni prin mijloace informatice cu posibila implicare a unei persoane;

5) programele informatice, datele informatice, procedurile, procesele de folosire, personalul şi utilizatorii nu pot să reprezinte părți ale unui sistem informatic;

6) nu oricare entitate, ce poate fi folosită ca suport (mijloc) de stocare a datelor informatice, poate cumula funcția de a asigura prin executarea unui program prelucrarea automată a datelor

[2240] STRÎMBEANU, Alexandru. *Răspunderea penală pentru accesul ilegal la informaţia computerizată: Monografie*. Chișinău: Tipografia Centrală, 2023, p. 382. 430 p. ISBN 978-5-88554-178-7.
[2241] Ibidem, p. 382.

informatice. Doar în cazul cumulării celor două funcții, entitatea respectivă constituie un sistem informatic;

7) sistemul informatic reprezintă nodul de prelucrare a datelor interconectate în scopul transportului de date, în timp ce ansamblul unor astfel de noduri constituie rețeaua informatică;

8) noțiunea de sistem informațional nu trebuie confundată cu noțiunea de sistem informatic în accepția art. 259 CP RM. Relația dintre noțiunile „sistem informatic" și „sistem informațional" este o relație de tip „parte – întreg";

9) victimă a infracțiunilor, care sunt prevăzute de art. 259 CP RM, este persoana fizică sau persoana juridică care participă la relaţiile sociale cu privire la accesul autorizat sau permis la informaţia computerizată;

10) prin „acces la informația computerizată" în accepțiunea art. 259 CP RM trebuie de înțeles: obținerea posibilității de a recurge la informația computerizată, în vederea beneficierii de calitățile utile ale acesteia;

11) în cazul infracțiunilor ce sunt prevăzute de art. 259 CP RM, accesul la informația computerizată presupune o interacțiune logică, nu fizică, cu o astfel de informație. Interacțiunea logică cu informația computerizată se exprimă în aceea că făptuitorul folosește un program informatic sau mai multe programe informatice care asigură prelucrarea acelei informații;

12) acțiunea de intruziune ilegală în calculatorul, în suportul material de informaţie, în sistemul informatic sau în reţeaua informatică, în care sau pe care se află respectiva informație, trebuie privită ca situație-premisă, nu ca etapă în procesul de săvârșire a accesului ilegal la informația computerizată. De aceea, trebuie calificată ca pregătire, nu ca tentativă, intruziunea ilegală în calculatorul, în suportul material de informaţie, în sistemul informatic sau în reţeaua informatică, în care sau pe care se află informația computerizată, dacă, din cauze care nu depind de voința făptuitorului, nu este săvârșit accesul ilegal la acea informație;

13) folosirea și/sau dispunerea de informația computerizată reprezintă scopul acțiunii de acces la informația computerizată, scop care depășește cadrul acestei acțiuni;

14) infracțiunea, prevăzută la art. 260^1 CP RM, poate fi concepută doar în cazul unei transmisii de date informatice (inclusiv a unei emisii electronice). În cazul infracțiunilor care sunt prevăzute de art. 259 CP RM, se accesează ilegal informația computerizată din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică, nu informația computerizată transmisă între calculatoare, între suporţii materiali de informaţie, între sisteme informatice sau între reţele informatice;

15) accesul la informația computerizată este ilegal, dacă se realizează: a) în lipsa autorizării în temeiul legii sau al unui contract; b) cu depăşirea limitelor autorizării; c) fără 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;

16) menținerea accesului ilegal la informația computerizată după retragerea ori expirarea autorizării este avută în vedere implicit în dispoziția art. 259 CP RM;

17) lipsa autorizării de a accesa informația computerizată presupune lipsa împuternicirii de a o accesa, pe care o acordă proprietarul informației computerizate sau un alt posesor al acestei informații;

18) depășirea limitelor autorizării de a accesa informația computerizată presupune că făptuitorul deține autorizarea de a accesa informația computerizată, însă acesta nu se conformează autorizării respective, arogându-și împuterniciri care nu i-au fost acordate;

19) pentru a considera accesul la informația computerizată ilegal, nu este relevant dacă: a) făptuitorul a solicitat permisiunea de a accesa informația computerizată, după care a ignorat refuzul de a da curs unei asemenea solicitări; b) făptuitorul nu a solicitat permisiunea de a accesa informația computerizată;

20) accesul legal la informația computerizată presupune prezența nu doar a unor scopuri legitime, ci și a tuturor celorlalte condiții care asigură respectarea legalității;

21) art. 259 CP RM se aplică în ipoteza în care: a) pentru una sau mai multe persoane – care au drept de acces la informaţia computerizată care se află în același calculator, pe același suport material de informaţie, în același sistem informatic sau în aceeași rețea informatică – este restricționat dreptul de acces la o anumită informaţie computerizată de acest gen *și* b) una sau unele dintre persoanele respective încalcă acea restricție;

22) în contextul infracțiunilor ce sunt prevăzute de art. 259 CP RM, acțiunea principală de acces ilegal la informația computerizată nu are potențialitatea de a cauza daune în proporții mari sau deosebit de mari. De aceea, daunele în proporții mari sau deosebit de mari trebuie raportate exclusiv la acțiunea adiacentă prevăzută de art. 259 CP RM;

23) indiferent de varianta sub care se prezintă latura obiectivă a infracțiunilor ce sunt prevăzute de art. 259 CP RM, fapta prejudiciabilă trebuie să preceadă urmările prejudiciabile. Dacă este invers – urmările prejudiciabile sunt prezente înainte de săvârșirea faptei prejudiciabile – atunci lipsește temeiul aplicării art. 259 CP RM. De asemenea, acțiunea principală trebuie să preceadă acțiunea adiacentă. Dacă este invers – acțiunea adiacentă este comisă înainte de săvârșirea acțiunii principale – atunci lipsește temeiul aplicării art. 259 CP RM;

24) infracțiunile, care sunt prevăzute de art. 260 și 260^4 CP RM, pot fi considerate exemple de pregătire sau de complicitate *sui generis* la oricare dintre infracțiunile prevăzute la art. 259 CP RM;

25) infracțiunile, prevăzute la art. 259 CP RM, sunt săvârșite cu intenție directă sau indirectă;

26) se aplică doar art. 260^6 CP RM în acea ipoteză în care accesul ilegal la informația computerizată este urmat de introducerea, modificarea sau ştergerea datelor informatice, restricţionarea accesului la aceste date ori împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă aceste acţiuni au cauzat daune în proporţii mari sau deosebit de mari;

27) în conformitate cu lit. d) alin. (1) art. 76 CP RM, comiterea faptei de o persoană ce are o responsabilitate redusă se consideră circumstanță atenuantă care se ia în calcul la stabilirea pedepsei. Anume în această postură, starea de afect poate fi luată în considerare la individualizarea pedepsei care se aplică pentru infracțiunile prevăzute la art. 259 CP RM;

28) subiecți ai infracțiunilor, prevăzute la art. 259 CP RM, pot fi persoanele care au dreptul de acces la un calculator, la un suport material de informaţie, la un sistem informatic sau la o rețea informatică. Asemenea persoane nu trebuie să aibă dreptul de acces la informația computerizată din calculatorul, de pe suportul material de informaţie, din sistemul informatic sau din reţeaua informatică la care au acces legal;

29) subiecți ai infracțiunilor, prevăzute la art. 259 CP RM, pot fi, de asemenea, persoanele care nu au un dreptul de acces la un calculator, la un suport material de informaţie, la un sistem informatic sau la o rețea informatică. Desigur, astfel de persoane nu au nici dreptul de acces la informația computerizată;

30) infracțiunile prevăzute la art. 259 CP RM au nu doar un subiect special. Ele au o componență specială;

31) în cazul săvârșirii uneia din infracțiunile ce sunt prevăzute de acest articol de către un grup criminal organizat sau de către o organizație criminală, se va aplica lit. b) alin. (2) art. 259 CP RM;

32) prin sisteme de protecție, în sensul lit. c) alin. (2) art. 259 CP RM, se înţelege procedurile, dispozitivele sau programele informatice specializate cu ajutorul cărora accesul la informația computerizată este restricţionată sau interzisă pentru anumite categorii de utilizatori;

33) în sensul lit. c) alin. (2) art. 259 CP RM, prin „protecție" se are în vedere protecția împotriva accesului ilegal la informația computerizată, nu protecția împotriva accesului ilegal la: a) calculatorul, suportul material de informaţie, sistemul sau reţeaua informatică, care conțin informația computerizată ce poate fi accesată ilegal; b) încăperea, alt loc pentru depozitare sau locuința în care se află calculatorul, suportul material de informaţie, sistemul sau reţeaua informatică, care conțin informația computerizată ce poate fi accesată ilegal;

34) prevederea de la lit. d) alin. (2) art. 259 CP RM este aplicabilă, dacă noțiunea „rețea informatică” se intersectează cu noțiunea „rețea de comunicații electronice”. Din contra, dacă noțiunea „rețea informatică” nu se intersectează cu noțiunea „rețea de comunicații electronice”, atunci se aplică art. 259 CP RM (cu excepția lit. d) alin. (2));

35) aplicarea art. 260 CP RM exclude aplicarea art. 26 și 259 CP RM (în cazul în care infracțiunea, prevăzută la art. 260 CP RM, reprezintă un exemplu de pregătire *sui generis* de infracțiunile prevăzute la art. 259 CP RM). Aplicarea art. 260 CP RM exclude aplicarea alin. (5) art. 42 și art. 259 CP RM (în cazul în care infracțiunea, prevăzută la art. 260 CP RM, constituie un exemplu de complicitate *sui generis* la una dintre infracțiunile prevăzute la art. 259 CP RM. În ambele aceste cazuri nu se admite aplicarea concomitentă atât a art. 260 CP RM, cât și a art. 301^1 CP RM sau a art. 261 CC RM;

36) circumstanța agravantă, prevăzută la lit. f) alin. (2) art. 259 CP RM, presupune sancționarea dublă a aceleiași fapte în cazul în care scopul special, menționat în această normă, își găsește realizarea;

37) în situația când se accesează ilegal informaţia computerizată protejată de lege (iar această informație se referă la viaţa personală a victimei, constituind un secret personal sau familial al acesteia), informația dată fiind distrusă, deteriorată, modificată, blocată sau copiată, aceeași persoană poate apărea atât ca victimă a infracțiunii care este prevăzută de lit. g) alin. (2) art. 259 CP RM, cât și ca victimă a uneia dintre infracţiunile prevăzute la alin. (1) sau (1^1) art. 177 CP RM;

38) lista de caracteristici protejate, care sunt specificate în alin. (1) art. 134^{21} CP RM, are un caracter limitativ. Alte caracteristici (de exemplu, statutul de migrant sau de azilant al victimei) nu pot sta la baza motivelor de prejudecată în accepțiunea art. 134^{21} CP RM;

39) va exista un temei suficient pentru aplicarea lit. g^1) alin. (2) art. 259 CP RM dacă accesul ilegal la informația computerizată a fost comis anume datorită faptului că victima era, de exemplu, de o altă rasă decât făptuitorul. În alți termeni, făptuitorul nu ar fi săvârșit accesul ilegal la informația computerizată dacă victima nu ar fi fost, de exemplu, de o altă rasă decât făptuitorul.

CONCLUZII ȘI RECOMANDĂRI

Rezultatele, pe care le-am obținut în cadrul prezentei teze, constau în următoarele: 1) au fost investigate viziunile doctrinare cu privire la răspunderea pentru infracțiunile prevăzute la art. 259 CP RM [268, pp. 133-142; 269, pp. 114-127; 275, pp. 19-65]; 2) a fost utilizat potențialul, de care dispun reglementările naționale cu privire la accesul la informaţia computerizată, în procesul de interpretare a acestui articol [265, pp. 13-16; 275, pp. 76-81]; 3) a fost identificat gradul de compatibilitate dintre art. 259 CP RM și reglementările de sorginte internațională privind interzicerea accesului ilegal la informaţia computerizată [266; 275, pp. 65-76]; 4) a fost studiată experienţa pozitivă a altor state în planul prevenirii și combaterii prin mijloace penale a accesului ilegal la informaţia computerizată [261; 275, pp. 81-97]; 5) au fost stabilite valorile sociale apărate împotriva infracţiunilor prevăzute la art. 259 CP RM [271-274; 275, pp. 101-138]; 6) au fost relevate caracteristicile obiectului material sau imaterial al infracţiunilor prevăzute de acest articol [18, pp. 77-90; 262, pp. 231-242; 263, pp. 69-71; 275, pp. 138-194]; 7) au fost examinate trăsăturile particularizante ce caracterizează victima infracţiunilor prevăzute la art. 259 CP RM [19, pp. 111-120; 275, pp. 194-211; 276, pp. 6-8]; 8) au fost stabilite conţinutul și structura faptei prejudiciabile prevăzute de acest articol [270, pp. 16-22; 275, pp. 211-267]; 9) au fost relevate urmările prejudiciabile şi legătura cauzală în cazul infracţiunilor prevăzute la art. 259 CP RM [275, pp. 267-303]; 10) a fost pertractate latura subiectivă și subiectul infracţiunilor prevăzute de acest articol [267; 275, pp. 307-331]; 11) au fost analizate circumstanțele care agravează răspunderea pentru infracţiunile prevăzute la art. 259 CP RM [264; 275, pp. 331-375]; 12) a fost efectuată delimitarea infracțiunilor, care sunt prevăzute la art. 259 CP RM, de alte infracțiuni [267; 275, pp. 154-155, 217-218, 247-248, 251, 254, 257-259]; 13) au fost investigate vulnerabilitățile ce caracterizează practica de aplicare a art. 259 CP RM, urmând formularea de soluții [267; 275, pp. 219, 220, 291, 295, 297, 339, 343]; 14) au fost analizate neajunsurile de natură tehnico-legislativă de care suferă dispoziţia art. 259 CP RM, urmând formularea de recomandări *de lege ferenda* [18, pp. 77-90; 19, pp. 111-120; 263, pp. 69-71; 267; 275, pp. 163, 182, 241, 349, 382, 390-391].

Problema ştiinţifică importantă, soluţionată în urma obținerii rezultatelor descrise, se exprimă în fundamentarea concepției de interpretare a art. 259 CP RM și de calificare a infracțiunilor în baza acestui articol fără a fi încălcat principiul legalității, această fundamentare având ca efect identificarea erorilor de aplicare a art. 259 CP RM și a defectelor ce

caracterizează dispoziția acestui articol, astfel fiind creată baza teoretică necesară pentru a perfecționa practica de aplicare a art. 259 CP RM și pentru a îmbunătăți calitatea acestui articol.

I. Concluzii:

Problema ştiinţifică importantă a fost demonstrată prin ***concluziile*** care au fost elaborate în baza ipotezei de cercetare, după cum urmează:

1. Incriminând faptele reunite sub denumirea marginală de acces ilegal la informaţia computerizată, legiuitorul urmărește să stabilească un echilibru rezonabil între dreptul unor persoane de a accesa în mod liber informația computerizată și dreptul altor persoane de a nu permite accesul ilegal la o asemenea informație. Dreptul la informație este un drept prevăzut de art. 34 din Constituție. Dreptul de a accesa în mod liber informația computerizată nu este decât o versiune a acestui drept constituțional. Din alin. (2) art. 54 al Constituției reiese că dreptul la informație poate fi restrâns. Important este ca această restrângere: a) să fie prevăzută de lege; b) să corespundă normelor unanim recunoscute ale dreptului internaţional; c) să fie necesară în interesele securităţii naţionale, integrităţii teritoriale, bunăstării economice a ţării, ordinii publice, în scopul prevenirii tulburărilor în masă şi infracţiunilor, protejării drepturilor, libertăţilor şi demnităţii altor persoane, împiedicării divulgării informaţiilor confidenţiale sau garantării autorităţii şi imparţialităţii justiţiei. Restrângerea dreptului de a accesa în mod liber informația computerizată, prevăzută de art. 259 CP RM, îndeplinește aceste trei condiții. Această restrângere se bazează pe lege și are drept scop protejarea interesului legitim al unei persoane, al societății sau al statului. Aceasta rezultă din descrierea subiectului infracțiunii, care se face în alin. (1) art. 259 CP RM: „persoană care nu este autorizată în temeiul legii sau al unui contract, 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”[2242] *(a se vedea: Capitolul 3, Subcapitolul 3.1)*.

2. Infracțiunile, prevăzute la art. 259 CP RM, sunt infracțiuni biobiectuale, însă nu sunt infracțiuni complexe. Infracțiunile, prevăzute la art. 259 CP RM, sunt biobiectuale. Despre aceasta ne vorbește structura faptei prejudiciabile prevăzute de acest articol. Astfel, fapta prejudiciabilă analizată include două componente: a) acţiunea principală de acces ilegal la informaţia computerizată; b) acţiunea adiacentă de distrugere, deteriorare, modificare, blocare sau copiere a informaţiei ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice. Obiectul juridic principal al infracțiunilor prevăzute la art. 259 CP RM îl formează

[2242] Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.

relaţiile sociale cu privire la accesul autorizat sau permis la informaţia computerizată. Acest obiect este același pentru ambele infracțiuni specificate în art. 259 CP RM. Obiectul juridic secundar al infracțiunilor prevăzute la art. 259 CP RM îl constituie relaţiile sociale cu privire la integritatea, autenticitatea, disponibilitatea sau ireproductibilitatea informației computerizate ori funcționalitatea calculatoarelor, a sistemului sau a reţelei informatice, apărate împotriva cauzării de: a) daune în proporții mari (în cazul infracțiunii prevăzute la alin. (1)); b) daune în proporții deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2)). În cazul infracțiunilor prevăzute la art. 259 CP RM, nici acțiunea principală, nici acțiunea adiacentă nu reprezintă de felul lor infracțiuni. În partea specială a Codului penal al Republicii Moldova nu există norme în care ar fi incriminate distinct fie accesul ilegal la informaţia computerizată, fie distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei ori dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice. Deci, infracțiunile, prevăzute la art. 259 CP RM, sunt infracțiuni biobiectuale, însă nu sunt infracțiuni complexe. *(a se vedea: Capitolul 2, Subcapitolul 2.1; Capitolul 3, Subcapitolul 3.1)*.

3. În cazul infracțiunilor prevăzute la art. 259 CP RM, obiectul imaterial principal îl reprezintă informația computerizată. În cazul aceloraşi infracțiuni, informația computerizată distrusă, deteriorată, modificată, blocată sau copiată constituie obiectul imaterial secundar; calculatoarele, sistemul informatic sau reţeaua informatică, a căror funcționare a fost dereglată formează obiectul material secundar. Sintagma „accesul ilegal la informaţia computerizată” din dispoziția art. 259 CP RM indică o încălcare a ordinii stabilite de acces la informațiile din calculatoare, de pe suporturile materiale de informaţie, din sistemul informatic sau din reţeaua informatică. O astfel de încălcare face dificilă sau chiar imposibilă derularea relațiilor sociale dintre subiecții care folosesc, administrează sau controlează un sistem informatic, care desfăşoară cercetări ştiinţifice sau care efectuează orice altă operaţiune într-un sistem informatic. Având în vedere acest aspect, ar reieși că infracțiunile, prevăzute la art. 259 CP RM, au obiect imaterial (care constă în informația computerizată), nu și obiect material. Însă, nu putem ignora o altă sintagmă din dispoziția art. 259 CP RM – „dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”.[2243] Această sintagmă se referă la acțiunea adiacentă și este relevantă (ca și sintagma „accesul ilegal la informaţia computerizată”) în vederea stabilirii entităților prin intermediul cărora este lezat obiectul juridic special al infracțiunilor care sunt prevăzute de art. 259 CP RM. Din sintagma „dacă este însoţit

[2243] Ibidem.

de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”[2244] rezultă că – în afară de informația computerizată accesată ilegal (care constituie obiectul imaterial principal al infracțiunilor examinate) – entitățile, prin intermediul cărora este lezat obiectul juridic special al infracțiunilor care sunt prevăzute de art. 259 CP RM, sunt reprezentate de: a) informația computerizată distrusă, deteriorată, modificată, blocată sau copiată (care formează obiectul imaterial secundar al infracțiunilor prevăzute la art. 259 CP RM); b) calculatoarele, sistemul informatic sau reţeaua informatică, a căror funcționare a fost dereglată (care formează obiectul material secundar al acestor infracțiuni) *(a se vedea: Capitolul 3, Subcapitolul 3.1)*.

4. Poziția față de structura laturii obiective a infracțiunilor, prevăzute la art. 259 CP RM, trebuie diferențiată în funcție de modalitățile normative ale acțiunii adiacente din cadrul faptei prejudiciabile. Ținând cont de specificul infracțiunilor prevăzute la art. 259 CP RM, apreciem că, doar în cazurile de distrugere, deteriorare sau modificare a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice, verbum regens vizează atât fapta prejudiciabilă, cât și urmările prejudiciabile. Or, în prezența acestor patru modalități normative, se produc anumite metamorfoze la nivelul obiectului material sau imaterial al infracțiunilor prevăzute la art. 259 CP RM. De aceea, în aceste patru cazuri, rezultatul, necesar consumării infracțiunii, constă, în primul rând, în distrugerea, deteriorarea sau modificarea informaţiei, ori în dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice. În al doilea rând, un astfel de rezultat se exprimă în daunele în proporții mari. La o privire *in corpore*, în cazurile analizate, urmările prejudiciabile constau în distrugerea, deteriorarea sau modificarea informaţiei, ori dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor în proporţii mari. Pe cale de consecință, latura obiectivă a infracţiunilor prevăzute la art. 259 CP RM are, în prima sa variantă, următoarea structură: a) fapta prejudiciabilă care constă în acţiunea principală de acces ilegal la informaţia computerizată, succedată de acţiunea adiacentă de distrugere, deteriorare sau modificare a informaţiei, ori de dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice; b) urmările prejudiciabile, și anume – distrugerea, deteriorarea sau modificarea informaţiei, ori dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, care îmbracă forma daunelor în proporţii mari (în cazul infracțiunii prevăzute la alin. (1)) ori a daunelor în proporţii deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2)); c) legătura cauzală dintre fapta prejudiciabilă şi urmările prejudiciabile. Într-o altă variantă, latura obiectivă a infracţiunilor

[2244] Ibidem.

prevăzute la art. 259 CP RM are următoarea structură: a) fapta prejudiciabilă care constă în acţiunea principală de acces ilegal la informaţia computerizată, succedată de acţiunea adiacentă de blocare sau copiere a informaţiei; b) urmările prejudiciabile, și anume – daunele în proporţii mari (în cazul infracțiunii prevăzute la alin. (1)) sau daunele în proporţii deosebit de mari (în cazul infracțiunii prevăzute la lit. h) alin. (2)); c) legătura de cauzalitate dintre fapta prejudiciabilă şi urmările prejudiciabile. *(a se vedea: Capitolul 3, Subcapitolul 3.2).*

5. Datorită structurii nereușite a laturii obiective a infracțiunilor prevăzute la art. 259 CP RM, lipsește posibilitatea de apărare penală eficientă a relaţiilor sociale cu privire la accesul autorizat sau permis la informaţia computerizată. În art. 259 CP RM este incriminat nu pur și simplu accesul ilegal la informaţia computerizată, ci accesul ilegal la informaţia computerizată însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, dacă, în rezultat, s-au produs daune în proporţii mari / deosebit de mari. Doar în unele cazuri, accesul ilegal la informația computerizată *per se* poate forma conținutul unor fapte penale sau contravenționale (de exemplu, al faptelor prevăzute la art. 327, 335 sau 370 CP RM ori în art. 312 CC RM). În celelalte cazuri, dacă intenția făptuitorului se limitează la săvârșirea accesului ilegal la informaţia computerizată, iar această intenție se realizează, atunci lipsește temeiul aplicării art. 259 CP RM. În acest caz, este lipsă latura obiectivă a infracțiunii în deplinătatea sa, motiv pentru care vorbim despre lipsa componenței de infracțiune. Necesitatea de revizuire a structurii actuale a laturii obiective a infracțiunilor, prevăzute la art. 259 CP RM, este determinată nu doar de această stare de lucruri. Un alt argument constă în prezența art. 260^2 și 260^3 CP RM, ceea ce face inutilă prezența în art. 259 CP RM a sintagmei care se referă la acțiunea adiacentă din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM: „dacă este însoţit de distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice”.[2245] *(a se vedea: Capitolul 2, Subcapitolul 2.2; Capitolul 3, Subcapitolul 3.2).*

6. Este oportună agravarea răspunderii în cazul săvârșirii infracțiunilor, prevăzute la art. 259 CP RM, fie asupra unui sistem informatic care este parte integrantă a infrastructurii critice, fie în privința informației sensibile privind protecția infrastructurilor critice. Analiza art. 259 CP RM demonstrează că acest articol nu este ajustat la exigențele sociale curente, fiind lipsite de apărare penală relațiile sociale care apar și se dezvoltă în legătură cu: a) sistemele informatice care sunt părți integrante ale infrastructurii

[2245] Ibidem.

critice; b) datele informatice sensibile privind protecția infrastructurilor critice. Necesitatea stringentă a unei asemenea completări este dictată de războiul de agresiune dus de Federația Rusă împotriva Ucrainei (care are efecte colaterale asupra Republicii Moldova), precum și de războiul hibrid purtat de către Federația Rusă, printre altele, împotriva Republicii Moldova. De asemenea, necesitatea de a suplini lacuna respectivă este sugerată în Decizia (PESC) 2019/797 a Consiliului din 17.05.2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre. Toate acestea confirmă că este oportună completarea Capitolului XIII din partea generală a Codului penal al Republicii Moldova cu două articole în care ar fi definite noțiunile „infrastructură critică" și „date informatice sensibile privind protecția infrastructurilor critice". Aceste definiții vor avea ca model definițiile aceloraşi noțiuni din Directiva 2008/114/CE, desigur cu operarea ajustărilor corespunzătoare. În afară de aceasta, este oportună agravarea răspunderii pentru infracțiunile prevăzute la art. 259 CP RM, în cazul în care acestea sunt săvârșite fie asupra unui sistem informatic care este parte integrantă a infrastructurii critice, fie în privința datelor informatice sensibile privind protecția infrastructurilor critice. *(a se vedea: Capitolul 2, Subcapitolul 2.5; Capitolul 3, Subcapitolul 3.5).*

Descrierea contribuţiilor personale cu sublinierea semnificaţiei teoretice şi valorii practice a acesteia. Contribuţiile personale constau în investigarea temeinică şi complexă a elementelor constitutive și a circumstanțelor agravante ale infracțiunilor prevăzute la art. 259 CP RM. Reprezentând componenţa de bază / agravată a infracţiunilor respective, aceste elemente constitutive și circumstanțe agravante constituie temeiul juridic al răspunderii penale în baza art. 259 CP RM.

La contribuţii personale pot fi raportate: demonstrarea necesității de a distinge noțiunea „securitatea informațională" de noțiunea „securitatea informatică (cibernetică), noțiunea „sistem informațional" de noțiunea „sistem informatic", noțiunea „sistem informatic" de noțiunea „rețea informatică" etc.; propunerea de definiții pentru fiecare dintre noțiunile care se referă la obiectul material (imaterial) al infracțiunilor prevăzute la art. 259 CP RM, cu luarea în considerare a normelor etrapenale de referință; argumentarea necesității de a distinge două variante alternative ale laturii obiective a infracţiunilor prevăzute la art. 259 CP RM, în funcție de specificul modalităților normative ale acțiunii adiacente; stabilirea corelației dintre infracțiunile, prevăzute la art. 259 CP RM, și alte infracțiuni prevăzute în Capitolul XI din partea specială a Codului penal al Republicii Moldova; caracterizarea detaliată a circumstanțelor agravante ale infracțiunilor prevăzute la art. 259 CP RM, cu luarea în considerare a normelor etrapenale de referință, etc.

În ceea ce privește patrimoniul doctrinar anterior, constatăm că nu sunt prea multe studii științifice consacrate analizei de drept penal a infracțiunilor prevăzute la art. 259 CP RM. Se caracterizează prin insuficiență sau prin anumite contradicții investigarea de către penaliștii autohtoni a elementelor constitutive și a circumstanțelor agravante ale acestor infracțiuni (și anume, a aspectelor legate de: conținutul obiectului juridic generic al infracţiunilor prevăzute la art. 259 CP RM; structura obiectului juridic special al acestor infracţiuni; înțelesul noțiunilor „informație computerizată", „sistem informatic", „rețea informatică" și „calculator"; structura laturii obiective a infracţiunilor prevăzute la art. 259 CP RM etc.).

Baza legală şi empirică a prezentului studiu o constituie: a) prevederile art. 259 CP RM; b) alte norme din Capitolul XI al părții speciale a Codului penal al Republicii Moldova; c) anumite norme din partea generală şi din partea specială a Codului penal al Republicii Moldova, necesare fie interpretării sistemice a art. 259 CP RM, fie examinării infracțiunilor prevăzute de acest articol prin prisma participației, a etapelor activității infracționale sau a altor asemenea instituții; d) prevederile din legislația extrapenală care complinesc art. 259 CP RM și, astfel, contribuie la interpretarea acestuia; e) practica de aplicare a art. 259 CP RM; f) normele din legile penale ale altor state, care sunt corespondente cu art. 259 CP RM; g) normele care constituie precedente istorice în raport cu art. 259 CP RM. *Baza ştiinţifică* a prezentului studiu este reprezentată de lucrările doctrinarilor autohtoni, precum și de cele ale doctrinarilor de peste hotare.

Semnificația teoretică a tezei rezidă în: a) redimensionarea apărării penale a relaţiilor sociale cu privire la accesul autorizat sau permis la informaţia computerizată; b) acumularea unui amplu material teoretic şi practic indispensabil pentru dezvoltarea anumitor direcţii complexe și actuale de cercetare a infracţiunilor ce sunt prevăzute de art. 259 CP RM; c) caracterizarea detaliată a elementelor constitutive și a circumstanțelor agravante ale infracțiunilor prevăzute la art. 259 CP RM; d) identificarea neajunsurilor ce caracterizează dispoziția art. 259 CP RM și practica de aplicare a acestei dispoziții.

Valoarea practică a tezei constă în următoarele: a) interpretarea din perspective noi a prevederilor art. 259 CP RM contribuie la dezvoltarea discuţiei ştiinţifice privind stabilirea temeiului juridic al răspunderii penale pentru faptele incriminate în acest articol; b) analiza de drept comparat și analiza istorică a reglementărilor privind răspunderea pentru accesul ilegal la informația computerizată comportă o semnificaţie cognitivă în vederea perceperii esenței juridice şi sociale a infracţiunilor prevăzute la art. 259 CP RM; c) interpretarea conceptelor, utilizate în art. 259 CP RM, este utilă în planul interpretării acestui articol în corespundere cu principiul legalității și al asigurării unei practici uniforme de aplicare a art. 259 CP RM, fiind astfel redusă posibilitatea interpretării extensive defavorabile şi a aplicării prin analogie a art. 259 CP RM; d)

stabilirea defectelor, ce caracterizează dispoziția art. 259 CP RM, poate fi valorificată în procesul de perfecționare a acestei dispoziții, pentru a fi sporită claritatea și previzibilitatea art. 259 CP RM, pentru a fi armonizate prevederile acestui articol cu dispozițiile Convenției de la Budapesta și pentru a fi ajustate prevederile art. 259 CP RM la exigențele sociale curente.

Date privind aprobarea rezultatelor. Concluziile principale ale tezei se regăsesc în 19 publicaţii ştiinţifice. Rezultatele, obținute în urma studiului efectuat, au fost prezentate și aprobate la mai multe foruri științifice, cu caracter național și internațional, care s-au desfășurat în perioada anilor 2020-2022.

Indicarea limitelor rezultatelor obţinute, cu stabilirea problemelor rămase nerezolvate. Limitele rezultatelor obţinute sunt condiționate de: a) efectuarea unei analize cu predilecție de drept penal a infracţiunilor prevăzute la art. 259 CP RM; b) analiza empirică a practicii judiciare autohtone și a celei din România; c) analiza sistemică a infracţiunilor, prevăzute la art. 259 CP RM, luând în considerare reglementările cu caracter complinitor din legislația extrapenală de referință. Întrucât toate obiectivele tezei au fost realizate, nu se poate vorbi despre probleme rămase nerezolvate. În schimb, pot fi trasate direcţii viitoare de cercetare legate de tema abordată, care vor fi creionate *infra*.

II. Recomandări:

1) completarea art. 6 CP RM cu alineatul (3) care ar avea următoarea dispoziție: *„Fapta săvârșită din imprudență constituie infracțiune numai atunci când o prevede în mod expres norma din partea specială din prezentul cod”*;

2) excluderea referirilor la intenție din toate normele din partea specială a Codului penal al Republicii Moldova, în care se menționează această formă de vinovăție;

3) completarea Capitolului XIII din partea generală a Codului penal al Republicii Moldova cu următoarele articole:

„Articolul 134[25]. Date informatice

Prin date informatice se înțelege orice reprezentare de fapte, informaţii sau concepte sub o formă adecvată prelucrării într-un sistem informatic, inclusiv un program capabil să determine executarea unei funcţii de către un sistem informatic”[2246];

„Articolul 134[26]. Sistem informatic

Prin sistem informatic se înțelege sistemul definit astfel în Legea nr. 20/2009 privind prevenirea şi combaterea criminalităţii informatice”[2247];

[2246] STRÎMBEANU, Alexandru. *Răspunderea penală pentru accesul ilegal la informaţia computerizată: Monografie*. Chișinău: Tipografia Centrală, 2023, p. 390. 430 p. ISBN 978-5-88554-178-7.
[2247] Ibidem, p. 390.

„Articolul 134[27]. Măsuri de securitate

Prin măsuri de securitate, în sensul art. 259, se înţelege folosirea unor proceduri, dispozitive sau programe informatice specializate cu ajutorul cărora accesul la informația computerizată este restricţionată sau interzisă pentru anumite categorii de utilizatori”[2248];

„Articolul 134[28]. Persoana care accesează ilegal datele informatice

Accesează ilegal datele informatice persoana care se află în una dintre următoarele situații:

a) nu este autorizată, în temeiul legii sau al unui contract;

b) depășește limitele autorizării;

c) nu are permisiunea, din partea persoanei fizice sau juridice competente, potrivit legii, să o acorde, de a folosi, administra sau controla un sistem informatic ori de a desfășura cercetări științifice sau de a efectua orice altă operațiune într-un sistem informatic”[2249];

„Articolul 134[29]. Infrastructură critică

Prin infrastructură critică, în sensul art. 259, se înțelege un element, un sistem sau o componentă a acestuia, aflat pe teritoriul Republicii Moldova, care este esențial pentru menținerea funcțiilor societale vitale, a sănătății, siguranței, securității, bunăstării sociale sau economice a persoanelor, și a căror perturbare sau distrugere ar avea un impact semnificativ pentru Republica Moldova ca urmare a incapacității de a menține respectivele funcții”[2250];

„Articolul 134[30]. Date informatice sensibile privind protecția infrastructurilor critice

Prin date informatice sensibile privind protecția infrastructurilor critice, în sensul art. 259, se înțelege datele informatice cu privire la o infrastructură critică ce ar putea fi utilizate, în cazul divulgării, în scopul planificării și al realizării unor acțiuni care să determine perturbarea sau distrugerea instalațiilor unor infrastructuri critice”[2251];

4) modificarea titlului Capitolului XI al părții speciale a Codului penal din „Infracţiuni informatice şi infracţiuni în domeniul telecomunicaţiilor” în *„Infracţiuni contra securității datelor informatice şi a comunicaţiilor electronice”*[2252];

5) modificarea titlului și a dispoziției art. 259 CP RM, după cum urmează:

„Articolul 259. Accesul ilegal la datele informatice

(1) Accesul ilegal la datele informatice prin violarea măsurilor de securitate [...]

(2) Aceeaşi acţiune săvârşită:

b) de două sau mai multe persoane;

[2248] Ibidem, p. 390.
[2249] Ibidem, p. 390-391.
[2250] Ibidem, p. 391.
[2251] Ibidem, p. 391.
[2252] Ibidem, p. 391.

e) cu folosirea unor mijloace tehnice speciale;

g) în privinţa datelor informatice protejate prin lege;

g[1]) din motive de prejudecată;

i) asupra unui sistem informatic care este parte integrantă a infrastructurii critice;

j) în privința datelor informatice sensibile privind protecția infrastructurilor critice [...]"[2253];

6) completarea Codului contravențional al Republicii Moldova cu un articol nou:

„Articolul 246[1]. Accesul ilegal la datele informatice

Accesul ilegal la datele informatice, dacă fapta nu constituie infracţiune,

se sancţionează cu amendă de la 30 la 60 de unităţi convenţionale aplicată persoanei fizice, cu amendă de la 120 la 180 de unităţi convenţionale aplicată persoanei juridice".[2254]

Sugestii privind potenţialele direcţii viitoare de cercetare legate de tema abordată: 1) elaborarea unui proiect de hotărâre a Plenului Curții Supreme de Justiție cu privire la aplicarea în practică de către instanțele judecătorești a art. 259 CP RM; 2) analiza aprofundată a unor instituții ale părții generale a dreptului penal (etapele activității infracționale, participația, cauzele care înlătură caracterul penal al faptei etc.) în contextul aplicării art. 259 CP RM; 3) elucidarea conotaţiilor de ordin criminologic și procesual penal ale infracțiunilor prevăzute la art. 259 CP RM.

Propuneri de utilizare a rezultatelor obţinute în domeniile socio-cultural şi economic: în procesul de creaţie legislativă (în scopul înlăturării neajunsurilor ce caracterizează dispoziția art. 259 CP RM, al sporirii gradului de claritate și previzibilitate a art. 259 CP RM, al armonizării acestui articol cu dispozițiile Convenției de la Budapesta și al ajustării art. 259 CP RM la exigențele sociale curente), în procesul educaţional (în scopul de sporire a nivelului de cunoștințe și deprinderi ale studenţilor de la facultăţile de drept din instituţiile de învăţământ superior, a audienţilor și beneficiarilor de instruire continuă din cadrul Institutului Naţional al Justiţiei) şi în activitatea ştiinţifică de perspectivă (în scopul dezvoltării discuției științifice privind răspunderea pentru infracțiunile prevăzute la art. 259 CP RM).

[2253] Ibidem, p. 391.
[2254] Ibidem, p. 391.

BIBLIOGRAFIE

A. Surse în limba română

1. ABRIHAN, Raluca. *Tendințe în securitate IT: România, peste medie la minare ilicită de criptomonede, atacuri phishing şi ransomware*. [citat 05.09.2020] Disponibil: https://www.startupcafe.ro/smart-tech/tendinte-securitate-it-atac-minare-ilegalacriptomonede-microsoft.htm
2. *Acordul de asociere între Uniunea Europeană și Comunitatea Europeană a Energiei Atomice și statele membre ale acestora, pe de o parte, și Republica Moldova, pe de altă parte*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:22014A0830(01)&from=RO
3. ALECU, Gheorghe. *Instituţii de drept penal: partea generală şi partea specială*. Constanţa: Ovidius University Press, 2010. 635 p. ISBN 978-973-614-579-7.
4. ANGHEL, Traian. *Dicționar de informatică*. București: Corint Books, 2017. 447 p. ISBN 978-606-793-178-5.
5. BACINSCHI, Serghei. Răspunderea penală pentru accesul ilegal la informaţia computerizată protejată de lege. În: *Probleme actuale privind protecţia şi securitatea persoanelor implicate în procesul penal (Materialele conferinţei ştiinţifico-practice internaţionale, 21 martie 2013)*. Chişinău: Academia „Ştefan cel Mare" a MAI, 2013, pp. 229-236. ISBN 978-9975-4407-2-1.
6. BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui Alexei BARBĂNEAGRĂ. Chişinău: Arc, 2003. 836 p. ISBN 9975-61-291-1.
7. BARBĂNEAGRĂ, Alexei et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009. 860 p. ISBN 978-9975-105-20-0.
8. BARBĂNEAGRĂ, Alexei et al. *Codul penal comentat şi adnotat*. Chişinău: Cartier, 2005. 656 p. ISBN 9975-29-338-X.
9. BERDILO, Rodica. *Răspunderea penală pentru omorul săvârșit în stare de afect*. Chișinău: Tipografia Centrală, 2021. 399 p. ISBN 978-9975-104-94-4.
10. BERDILO, Rodica. Responsabilitatea redusă și starea emoțională a subiectului infracțiunilor prevăzute la art. 146, 147 și 156 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale"*, 2021, nr. 3, pp. 150-159. ISSN 1814-3199.
11. BERDILO, Rodica. Victima omorului săvârșit în stare de afect. În: *Revista Institutului Naţional al Justiţiei*, 2021, nr. 1, pp. 33-38. ISSN 1857-2405.
12. BODORONCEA, Georgina et al. *Codul penal: comentariu pe articole*. Bucureşti: C.H. Beck, 2014. 902 p. ISBN 978-606-18-0408-5.
13. BORODAC, Alexandru, BUJOR, Valeriu, BRÎNZA, Serghei. *Drept penal. Partea generală*. Chișinău: Știința, 1994. 368 p. ISBN 5-376-01847-4.
14. BORODAC, Alexandru. *Manual de drept penal. Partea specială*. Chişinău: Tipografia Centrală, 2004. 622 p. ISBN 9975-9788-7-8.
15. BOROI, Alexandru, GORUNESCU, Mirela, POPESCU, Mihaela. *Dicționar de drept penal*. București: All Beck, 2004. 417 p. ISBN 973-655-425-X.
16. BOTNARENCO, Dorin. Unele reflecții privind noțiunea „contrară legii" din dispoziția art. 307 CP RM. În: *Conferință științifică națională cu participare internațională „Integrare prin cercetare și inovare". Științe juridice și economice. Rezumate ale comunicărilor. Vol. I*. Chișinău: CEP USM, 2020, pp. 144-148. ISBN 978-9975-152-48-8.
17. BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Sistemul informatic și rețeaua informatică: obiecte materiale ale infracțiunilor prevăzute la art.259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale"*, 2022, nr. 8, pp. 77-90. ISSN 1814-3199.

18. BOTNARENCO, Mihaela, STRÎMBEANU, Alexandru. Victima infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 111-120. ISSN 1814-3199.
19. BOTNARU, Stela, ȘAVGA, Alina, GRAMA, Mariana, GROSU, Vladimir. *Drept penal. Partea generală*. Chișinău: Cartier, 2005. 624 p. ISBN 9975-79-318-5.
20. BOTNARU, Stela. *Iresponsabilitatea – cauză care înlătură vinovăţia făptuitorului: definitivarea conceptului*. În: *Revista Naţională de Drept*, 2014, nr. 2, pp. 33-37. ISSN 1811-0770.
21. BOȚIAN, Elisabeta. Mobilul și scopul. De la concepte filosofice la noțiuni ale dreptului penal. În: *Acta Universitatis Lucian Blaga*, 2021, nr. 1, pp. 107-120. ISSN 1582-4608.
22. BRAGARU, Tudor, BRICEAG, Valentin, MALCOCI, Viorel, GALAICU, Valeriu. Securitatea informației vis-a-vis de securitatea informațională. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe exacte şi economice”*, 2019, nr. 2, pp. 38-47. ISSN 1814-3199.
23. BRÎNZA, Cristian. Categoriile obiectului material sau imaterial al infracțiunilor de luare de mită și de dare de mită. În: *Conferinţa ştiinţifică naţională cu participare internaţională „Infracţiunea – Răspunderea penală – Pedeapsa. Drept şi Criminologie”, 25-26 martie 2021*. Chişinău: CEP USM, 2021, pp. 308-318. ISBN 978-9975-158-12-1.
24. BRÎNZA, Cristian. Obiectul material sau imaterial al infracțiunilor de luare de mită și de dare de mită: considerații introductive. În: Conferinţa ştiinţifică naţională cu participare internaţională „Infracţiunea – Răspunderea penală – Pedeapsa. Drept și Criminologie”, 25-26 martie 2021. Chişinău: CEP USM, 2021, pp. 300-307. ISBN 978-9975-158-12-1.
25. BRÎNZA, Cristian. *Răspunderea penală pentru luarea de mită și darea de mită*: tz. de doct. în drept. Chișinău, 2021. 351 p.
26. BRÎNZA, Serghei et al. *Drept penal. Partea specială*. Chișinău: Cartier, 2005. 804 p. ISBN 9975-79-324-X.
27. BRÎNZA, Serghei, MAREȘ, Mihai. Îmbogățirea ilicită – o analiză comparativă a legislațiilor din Republica Moldova și din România. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2020, nr. 8, pp. 3-16. ISSN 1814-3199.
28. BRÎNZA, Serghei, STATI, Vitalie. „Sexting”, „sextorsion”, „revenge porn”: fenomene reflectate în Codul penal al Republicii Moldova? În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 3, pp. 3-17. ISSN 1814-3199.
29. BRÎNZA, Serghei, STATI, Vitalie. *Drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2011. 1324 p. ISBN 978-9975-53-028-7.
30. BRÎNZA, Serghei, STATI, Vitalie. Rațiunea și efectele adoptării Legii nr. 111/2022. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2022, nr. 8, pp. 3-15. ISSN 1814-3199.
31. BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. I*. Chișinău: Tipografia Centrală, 2015. 1328 p. ISBN 978-9975-53-469-7.
32. BRÎNZA, Serghei, STATI, Vitalie. *Tratat de drept penal. Partea specială. Vol. II*. Chișinău: Tipografia Centrală, 2015. 1300 p. ISBN 978-9975-53-470-3.
33. BRÎNZA, Serghei, STRÎMBEANU, Alexandru. Unele aspecte ale laturii obiective a infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2023, nr. 3, pp. 3-15. ISSN 1814-3199.
34. BRÎNZA, Serghei. Infracțiunea de omor simplu în legea penală a Republicii Moldova. În: *Jurnalul de Studii Juridice*, 2010, număr special, pp. 15-29. ISSN 1841-6195.
35. BRÎNZA, Serghei. Justificarea publică a sinuciderii: caracteristici definitorii. În: *Conferință științifică națională cu participare internațională „Integrare prin cercetare și inovare”. Științe juridice și economice. Rezumate ale comunicărilor. Vol. I*. Chișinău: CEP USM, 2020, pp. 9-12. ISBN 978-9975-152-48-8.

36. BRÎNZA, Serghei. *Obiectul infracţiunilor contra patrimoniului*. Chișinău: Tipografia Centrală, 2005. 675 p. ISBN 9975-70-414-X.
37. BUJOR, Valeriu. Unele aspecte vizând elaborarea normelor de drept penal. În: *Legea și Viața*, 2009, nr. 8, pp. 8-10. ISSN 1810-309X.
38. BUTCULESCU, Claudiu Ramon. Rolul clarificator al doctrinei pentru comunicarea juridică. În: *Impactul transformărilor socio-economice și tehnologice la nivel național, european și mondial*, 2015, nr. 6, pp. 23-28. ISSN 2393-3240.
39. CAZACICOV, Andrei. Latura subiectivă a infracţiunii de creare sau conducere a unei organizaţii criminale. În: *Revista Naţională de Drept*, 2021, nr. 2, pp. 118-127. ISSN 1811-0770.
40. CHIRPAT, Nicolae, CERBU, Olga. Metode de utilizare a instrumentelor de securitate a informaţiei. În: *Teoria şi practica administrării publice (20 mai 2013, Chişinău)*. Chișinău: Academia de Administrare Publică, 2013, pp. 462-464. ISBN 978-9975-4241-5-8.
41. Codul audiovizualului al Republicii Moldova: nr. 260 din 27.07.2006. În: *Monitorul Oficial al Republicii Moldova*, 2006, nr. 131-133, 679.
42. Codul civil al Republicii Moldova: nr. 1107 din 06.06.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 82-86, 661.
43. Codul contravențional al Republicii Moldova: nr. 218 din 24.10.2008. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 3-6, 15.
44. Codul de procedură penală al Republicii Moldova: nr. 122 din 14.03.2003. În: *Monitorul Oficial al Republicii Moldova*, 2003, nr. 104-110, 447.
45. Codul de procedură penală al României: nr. 135 din 01.07.2010. În: *Monitorul Oficial al României*, 2010, nr. 486.
46. Codul funciar al Republicii Moldova: nr. 828 din 25.12.1991. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 107, 817.
47. *Codul penal al Greciei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Grecia-RO.html
48. *Codul penal al Marelui Ducat de Luxemburg*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Luxemburg-RO.html
49. *Codul penal al Regatului Belgiei*. [citat 04.07.2022] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html
50. *Codul penal al Regatului Danemarcei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Danemarca-RO.html
51. *Codul penal al Regatului Spaniei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Spania-RO.html
52. *Codul penal al Regatului Suediei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Suedia-RO.html
53. *Codul penal al Regatului Ţărilor de Jos (Olanda)*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Olanda-RO.html
54. *Codul penal al Republicii Austria*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Austria-RO.html
55. *Codul penal al Republicii Bulgaria*. [citat 07.03.2022] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Bulgaria-RO.html
56. *Codul penal al Republicii Cehe*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Cehia-RO.html
57. *Codul penal al Republicii Cipriote*. [citat 11.07.2022] Disponibil: https://codexpenal.just.ro/laws/Cod-Penal-Cipru-RO.html
58. *Codul penal al Republicii Croaţia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Croatia-RO.html

59. *Codul penal al Republicii Estonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Estonia-RO.html
60. *Codul penal al Republicii Federale Germania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Germania-RO.html
61. *Codul penal al Republicii Finlanda*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Finlanda-RO.html
62. *Codul penal al Republicii Franceze*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Franta-RO.html
63. *Codul penal al Republicii Italia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Italia-RO.html
64. *Codul penal al Republicii Letonia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Letonia-RO.html
65. *Codul penal al Republicii Lituania*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Lituania-RO.html
66. *Codul penal al Republicii Malta*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Malta-RO.html
67. Codul penal al Republicii Moldova: nr. 41 din 24.03.1961. În: *Veştile Sovietului Suprem al R.S.S. Moldoveneşti*, 1961, nr. 10, 41.
68. Codul penal al Republicii Moldova: nr. 985 din 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 128-129, 1012.
69. *Codul penal al Republicii Polone*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Polonia-RO.html
70. *Codul penal al Republicii Portugheze*. [citat 18.12.2020] Disponibil https://codexpenal.just.ro/laws/Cod-Penal-Portugalia-RO.html
71. *Codul penal al Republicii Slovace*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovacia-RO.html
72. *Codul penal al Republicii Slovenia*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Slovenia-RO.html
73. Codul penal al României din 21.06.1968. În: *Buletinul Oficial*, 1968, nr. 79-79 bis
74. Codul penal al României: nr. 286 din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510
75. Codul penal al României: nr. 301 din 28.06.2004. În: *Monitorul Oficial al României*, 2004, nr. 575.
76. *Codul penal al Ungariei*. [citat 18.12.2020] Disponibil: codexpenal.just.ro/laws/Cod-Penal-Ungaria-RO.html
77. Codul serviciilor media audiovizuale al Republicii Moldova: nr. 174 din 08.11.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 462-466, 766.
78. COMAN, Vasile. *Accesarea contului de e-mail și de Facebook. Noțiunea de date informatice. Forma agravată prevăzută de art. 360 alin. (3) CP*. [citat 06.03.2022] Disponibil: https://www.universuljuridic.ro/accesarea-contului-de-e-mail-si-de-facebook-notiunea-de-date-informatice-forma-agravata-prevazuta-de-art-360-alin-3-cp/
79. COMAN, Vasile. *Accesul prin „încălcarea măsurilor de securitate" prevăzută de art. 42 alin. (3) din Legea nr. 161/2003. Condiții de apreciere*. [citat 30.12.2022] Disponibil: https://www.universuljuridic.ro/accesul-prin-incalcarea-masurilor-de-securitate-prevazuta-de-art-42-alin-3-din-legea-nr-161-2003-conditii-de-apreciere/
80. COMAN, Vasile. *Infracțiuni privind criminalitatea în cyberspațiu: practică judiciară recentă adnotată. Vol. I*. București: Universul Juridic, 2020. 486 p. ISBN 978-606-39-0627-5.
81. *Comisia Europeană pentru Democrație prin Lege (Comisia de la Veneția). Republica Moldova. Proiect de Aviz Comun al Comisiei de la Veneția și al Direcției Generale*

Drepturile Omului și Statul de Drept (DGI) a Consiliului Europei pe marginea Proiectului de Lege nr. 161 pentru modificarea și completarea legislației moldovenești din domeniul criminalității informatice. [citat 18.12.2020] Disponibil: https://www.parlament.md/LinkClick.aspx?fileticket=IbGsshOB2Ys%3D&tabid=90&language=ro-RO
82. Constituția Republicii Moldova. În: *Monitorul Oficial al Republicii Moldova*, 1994, nr. 1, 140.
83. COPEȚCHI, Stanislav, HADÎRCĂ, Igor. Calificarea infracţiunilor după latura subiectivă. În*: Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2015, nr. 11, pp. 61-68. ISSN 1814-3199.
84. COPEȚCHI, Stanislav, HADÎRCĂ, Igor. *Calificarea infracțiunilor: Note de curs*. Chișinău: Tipografia Centrală, 2015. 352 p. ISBN 978-9975-53-547-2.
85. COPEȚCHI, Stanislav. Corespondenţa electronică: obiect imaterial al infracţiunii prevăzute la art. 178 CP RM? În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2017, nr. 8, pp. 116-122. ISSN 1814-3199.
86. COPEȚCHI, Stanislav. Infracţiunile informatice potrivit legii penale moldave: studiu de drept comparat și propuneri *de lege ferenda*. În: *Realități și perspective ale învățământului juridic național. Culegerea materialelor științifice elaborate în baza comunicărilor de la Conferinţa ştiinţifică naţională cu participare internaţională, organizată cu ocazia a 60 de ani de la înființarea Facultății de Drept (USM, 01-02 octombrie 2019, Chişinău). Vol. II*. Chișinău: CEP USM, 2020, pp. 29-40. ISBN 978-9975-149-88-4.
87. COPEŢCHI, Stanislav. Încadrarea infracţiunilor săvârşite în participaţie: aspecte discutabile. În: *Revista Institutului Naţional al Justiţiei*, 2020, nr. 4, pp. 35-42. ISSN 1857-2405.
88. COPEȚCHI, Stanislav. Semnele secundare ale laturii subiective: aspecte teoretico-practice şi legislative. În: *Conferinţa ştiinţifică naţională cu participare internaţională „Infracţiunea – Răspunderea penală – Pedeapsa. Drept şi Criminologie” (25-26 martie 2021, Chişinău)*. Chișinău: CEP USM, 2021, pp. 76-85. ISBN 978-9975-158-12-1.
89. CRIJANOVSCHI, Sergiu. Accesul ilegal la informaţia computerizată în practica judiciară a Republicii Moldova și a României. În: *Conferința „Integrare prin cercetare și inovare” (Chișinău, Moldova, 28-29 septembrie). Vol. 1*. Chișinău: CEP USM, 2016, pp. 250-253. ISBN 978-9975-71-815-8.
90. DASCĂLU, Beatrice Daiana. Subiecții infracțiunii de violență în familie. În: *Legea și Viața*, 2017, nr. 4, pp. 43-45. ISSN 2587-4373.
91. *Decizia (PESC) 2019/797 a Consiliului din 17.05.2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32019D0797&from=RO
92. *Decizia Colegiului penal al CSJ din 05.08.2020. Dosarul nr. 1ra-1508/2020*. [citat 11.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=16547
93. *Decizia Colegiului penal al CSJ din 07.11.2018. Dosarul nr. 1ra-1891/2018*. [citat 11.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=12288
94. *Decizia Colegiului penal al CSJ din 25.06.2014. Dosarul nr. 1ra-1113/2014*. [citat 11.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=2653
95. *Decizia Colegiului penal al Curții de Apel Bălți din 24.03.2021. Dosarul nr. 1a-568/2020*. [citat 18.12.2020] Disponibil: https://instante.justice.md/ro/pigd_integration/pdf/FA8E4DB5-A215-4DBA-A2C4-45141DCC4185
96. *Decizia Colegiului penal al Curții de Apel Chișinău din 15.06.2015. Dosarul nr. 1a-805/2015*. [citat 18.12.2020] Disponibil:

https://cac.instante.justice.md/ro/pigd_integration/pdf/87ea8f58-4316-e511-b888-005056a5d154
97. *Decizia Colegiului penal al Curții de Apel Chișinău din 20.05.2020. Dosarul nr. 1a-631/2020*. [citat 06.03.2022] Disponibil: https://cac.instante.justice.md/ro/pigd_integration/pdf/45946398-403f-4820-8c4e-0ed11ad86fc1
98. *Decizia Colegiului penal al Curții de Apel Chișinău din 21.11.2017. Dosarul nr. 1a-842/2017*. [citat 18.12.2020] Disponibil: https://cac.instante.justice.md/ro/pigd_integration/pdf/ac0d8691-62f1-e711-80d5-0050568b7027
99. *Decizia Colegiului penal lărgit al CSJ din 01.02.2022. Dosarul nr. 1ra-1735/2021*. [citat 18.12.2020] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=20563
100. *Decizia Colegiului penal lărgit al CSJ din 11.06.2019. Dosarul nr. 1ra-445/2019*. [citat 11.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=13789
101. *Decizia Colegiului penal lărgit al CSJ din 13.03.2006. Dosarul nr. 1ra-208/2007*. [citat 06.03.2022] Disponibil: http://jurisprudenta.csj.md/archive_courts/cauta/
102. *Decizia Colegiului penal lărgit al CSJ din 15.03.2016. Dosarul nr. 1ra-87/2016*. [citat 18.12.2020] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=6000
103. Decizia Curții Constituționale a Republicii Moldova de inadmisibilitate a sesizării nr. 138g/2017 privind excepţia de neconstituţionalitate a unor prevederi din articolul 243 alineatul (1) literele a) și c) din Codul penal al Republicii Moldova nr. 985-XV din 18 aprilie 2002 (spălarea banilor): nr. 109 din 07.11.2017. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 58-66, 34.
104. Decizia Curții Constituționale a Republicii Moldova de inadmisibilitate a sesizărilor nr. 173g/2017 și nr. 37g/2018 privind excepţia de neconstituţionalitate a articolului 220 din Codul penal și a articolului 89 din Codul contravențional (proxenetismul și practicarea prostituției): nr. 36 din 19.04.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 195-209, 104.
105. Decizia Curții Constituționale a Republicii Moldova de inadmisibilitate a sesizării nr. 4g/2022 privind excepția de neconstituționalitate a unor dispoziții din articolul 322 alin. (1) din Codul penal: nr. 78 din 16.06.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 201-207.
106. Decizia Curții Constituționale a Republicii Moldova de inadmisibilitate a sesizării nr. 27g/2020 privind excepția de neconstituționalitate a unor prevederi din articolul 171 din Codul penal: nr. 67 din 15.06.2020. În: *Monitorul Oficial al Republicii Moldova*, 2020, nr. 212-220.
107. Decizia Curții Constituționale a României referitoare la excepţia de neconstituţionalitate a dispoziţiilor art. 30 alin. (3) din Codul de procedură penală, precum şi a dispoziţiilor art. 244-246, art. 248 şi 279 din Legea nr. 297/2004, raportate la art. 244 alin. (5) lit. a) pct. 2 şi lit. b) şi alin. (7) lit. a), cu aplicarea art. 276 lit. c) din Legea nr. 297/2004 privind piaţa de capital: nr. 53 din 25.01.2012. În: *Monitorul Oficial al României*, 2012, nr. 234.
108. Decizia Curții Constituționale a României referitoare la excepţia de neconstituţionalitate a dispoziţiilor art. 360 alin. (3) din Codul penal: nr. 183 din 29.03.2018. În: *Monitorul Oficial al României*, 2018, nr. 486.
109. Decizia Curții Constituționale a României referitoare la excepția de neconstituționalitate a dispozițiilor art. 181 din Codul penal și ale art. 157 și art. 168 din Codul de procedură penală: nr. 633 din 17.10.2017. În: *Monitorul Oficial al României*, 2018, nr. 126.
110. Decizia Curții Constituționale a României referitoare la excepția de neconstituționalitate a dispozițiilor art. 35 alin. (1) și ale art. 39 alin. (1) lit. b) din Codul penal: nr. 368 din 30.05.2017. În: *Monitorul Oficial al României*, 2017, nr. 566.

111. Decizia Înaltei Curți de Casație și Justiție a României privind interpretarea şi aplicarea unitară a dispoziţiilor art. 42 alin. (1), (2) şi (3) din Legea nr. 161/2003, respectiv pentru interpretarea unitară a noţiunii de acces fără drept la un sistem informatic: nr. 15 din 14.10.2013. În: *Monitorul Oficial al României*, 2013, nr. 760.
112. Decizia Înaltei Curți de Casație și Justiție a României referitoare la interpretarea dispozițiilor art. 360 alin. (1) din Codul penal: nr. 68 din 29.09.2021. În: *Monitorul Oficial al României*, 2022, nr. 56.
113. *Decizia Secției Penale a Înaltei Curți de Justiție și Casație a României nr. 371 din 02.02.2010*. [citat 12.09.2020] Disponibil: https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=54367
114. Decretul Preşedintelui Republicii Moldova privind edificarea societăţii informaţionale în Republica Moldova: nr. 1743 din 19.03.2004. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 50, 300.
115. *Directiva (UE) 2018/1972 a Parlamentului European și a Consiliului din 11.12.2018 de instituire a Codului european al comunicațiilor electronice*. [citat 23.01.2021] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32018L1972&from=ro
116. *Directiva 2002/77/CE a Comisiei din 16.09.2002 privind concurența pe piețele de rețele și servicii de comunicații electronice*. [citat 07.07.2022] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32002L0077&from=RO
117. *Directiva 2008/114/CE a Consiliului din 08.12.2008 privind identificarea și desemnarea infrastructurilor critice europene și evaluarea necesității de îmbunătățire a protecției acestora*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A32008L0114
118. *Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12.08.2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=en
119. DOBRINOIU, Maxim. Accesul ilegal la poşta electronică. În: *Revista de Drept Penal*, 2008, nr. 3, pp. 122-125. ISSN 1223-0790.
120. DOBRINOIU, Maxim. Considerații tehnice și juridice privind reținerea infracțiunii de acces ilegal la un sistem informatic în situația interogării unei baze de date prin depășirea limitelor autorizării. În: *Penalmente Relevant*, 2021, nr. 1, 2021, pp. 70-78. ISSN 2501-1367.
121. DOBRINOIU, Maxim. Infracţiunea de interceptare ilegală a unei transmisii de date informatice. În: *Revista română de dreptul proprietăţii intelectuale*, 2006, nr. 2, pp. 68-85. ISSN 1584-7241.
122. DOBRINOIU, Maxim. *Infracţiuni în domeniul informatic*. Bucureşti: C.H. Beck, 2006. 401 p. ISBN 978-973-655-941-9.
123. DRĂGAN, Alin Teodorus. *Frauda informatică: analiza juridico-penală a infracțiunii*: tz. de doct. în drept. Chişinău, 2017. 179 p.
124. DRĂGULĂNESCU, Nicolae-George. Concepte ale societăţii informaţionale „informare” – „informaţie”. În: *Magazin bibliologic*, 2011, nr. 1-2, pp. 3-6. ISSN 1857-1476.
125. DUMNEANU, Ludmila, GUREV, Dorina. *Infracțiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM. 261 p. ISBN 978-9975-158-29-9.
126. DUNEA, Mihai. Unele provocări juridico-penale ca urmare a evoluţiei tehnologiei informaţiei (inclusiv a evoluţiei Internetului). În: *Analele Ştiinţifice ale Universităţii „Alexandru Ioan Cuza” din Iaşi, seria Ştiinţe Juridice*, 2019, nr. 2-bis, pp. 187-200. ISSN 1221-8464.

127. DUVAC, Constantin. Accesul ilegal la un sistem informatic în reglementarea noului Cod penal. În: *Revista română de dreptul proprietăţii intelectuale*, 2012, nr. 1, pp. 88-109. ISSN 1584-7241.
128. FEȘTEU, Cristina Georgiana. Concursul de calificări (I). În: *Penalmente relevant*, 2016, nr. 1, pp. 67-88. ISSN 2501-1367.
129. FLĂMÂNZEANU, Ion. Doctrina ca izvor de drept. În: *Revista Studii de Drept Românesc*, 2010, nr. 1, pp. 23-30. ISSN 2284 -9394.
130. FLORESCU, Valentin, FLORESCU, Gabriela. Analiza infracţiunilor informatice incriminate în legislaţia în vigoare şi din perspectiva noului Cod penal. În: *Revista Română de Informatică şi Automatică*, 2012, vol. 22, nr. 2, pp. 21-38. ISSN 1841-4303.
131. GAINDRIC, Constantin. Cu privire la noțiunile de date, informații, cunoștințe. În: *Akademos*, 2020, nr. 3, pp. 15-18. ISSN 1857-0461.
132. GIURCĂ, Bogdan. Elementele constitutive ale infracţiunii în lumina noului Cod penal. În: *Politica legislativă între reglementare europeană, naţională şi internaţională: noi perspective ale dreptului / Conferinţa Internaţională de Drept, Studii Europene şi Relaţii Internaţionale (Bucureşti, 24-25 mai 2013)*. Bucureşti: Hamangiu, 2013, pp. 286-296. ISBN 978-606-678-642-3.
133. GLADCHI, Gheorghe. Obiectul material al infracțiunii și victima infracțiunii. În: *Reabilitarea victimelor infracțiunii: Conferința științifico-practică națională dedicată aniversării a 75 de ani de la fondarea Universității de Stat din Moldova (Chișinău, 22 octombrie 2021)*. Chișinău: CEP USM, 2022, pp. 70-76. ISBN 978-9975-159-02-9.
134. GOJAN, Roman, STAN, Iulian. Infracțiunile informaționale și spionajul informațional. În: *Securitatea informaţională 2013. Conferința internațională „Securitatea informaţională" (Chișinău, Moldova, 19 aprilie 2013)*. Chișinău: ASEM, 2013, pp. 103-110. ISBN 978-9975-75-640-2.
135. GORUNESCU, Mirela, CORLĂŢEANU, Sorin. Delictele informatice potrivit noului Cod penal. În: *Revista de Drept Penal*, 2007, nr. 1, pp. 52-53. ISSN 1223-0790.
136. GRAMA, Mariana, BOTNARU, Stela, ȘAVGA, Alina, GROSU, Vladimir. *Drept penal. Partea generală. Vol. I*. Chișinău: Tipografia Centrală, 2012. 328 p. ISBN 978-9975-53-080-4.
137. GRAMA, Mariana, BOTNARU, Stela, ȘAVGA, Alina, MARTIN, Daniel. *Drept penal. Partea generală. Vol. II*. Chișinău: Tipografia Centrală, 2016. 336 p. ISBN 978-9975-53-612-7.
138. GUIU, Mioara-Ketty. Clasificarea infracțiunilor în raport cu rezultatul lor. În: *Dreptul*, 2017, nr. 12, pp. 137-149. ISSN 1811-0770.
139. GUREV, Dorina. Accesul ilegal la informaţia computerizată: problematica încadrării juridice și soluții. În: *Integrare prin cercetare și inovare. Rezumatele comunicărilor. Științe juridice și economice. Vol. I (10-11 noiembrie 2020)*. Chișinău: CEP USM, 2020, pp. 54-57. ISBN 978-9975-152-48-8.
140. GUREV, Dorina. Răpirea unei persoane săvârşită prin participaţie. În: *Studia Universitatis Moldaviae, Seria Ştiinţe Sociale*, 2013, nr. 8, pp. 121-131. ISSN 1814-3199.
141. HADÎRCĂ, Igor. Elementele constitutive subiective ale infracţiunilor prevăzute la art. 217, 217^1-217^6, 218 şi 219 C. pen. RM. În: *Revista Naţională de Drept*, 2008, nr. 2, pp. 46-53. ISSN 1811-0770.
142. HLOPEATNICOV, Claudia. Mecanisme și protocoale de protecția informației în rețele și sisteme informaționale. În: *Conferinţa tehnico-ştiinţifică a studenţilor, masteranzilor şi doctoranzilor. Vol. 1 (26-29 martie 2019, Chişinău)*. Chișinău: Universitatea Tehnică a Moldovei, 2019, pp. 421-422. ISBN 978-9975-45-588-6.
143. Hotărârea ANRCETI cu privire la Regulamentul privind regimul de autorizare generală şi eliberare a licenţelor de utilizare a resurselor limitate pentru furnizarea reţelelor şi

serviciilor publice de comunicaţii electronice: nr. 57 din 21.12.2010. În: *Monitorul Oficial al Republicii Moldova*, 2011, nr. 22-24, 127.
144. Hotărârea ANRCETI pentru aprobarea Regulamentului cu privire la furnizarea serviciilor de comunicații electronice accesibile publicului: nr. 48 din 10.09.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 258-261, 1695.
145. Hotărârea BNM cu privire la aprobarea Regulamentului cu privire la plasarea, tranzacționarea și răscumpărarea valorilor mobiliare de stat în formă de înscriere în cont: nr. 170 din 19.07.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 277-284, 1171.
146. Hotărârea BNM cu privire la aprobarea, modificarea, completarea și abrogarea unor acte normative ale Băncii Naţionale a Moldovei: nr. 157 din 01.08.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 191-197, 1370.
147. Hotărârea Curții Constituționale a Republicii Moldova pentru controlul constituţionalităţii unor prevederi ale Hotărârii Guvernului nr. 79 din 23 ianuarie 2006 privind aprobarea Listei substanţelor narcotice, psihotrope şi a plantelor care conţin astfel de substanţe depistate în trafic ilicit, precum şi cantităţile acestora: nr. 25 din 13.10.2015. În: *Monitorul Oficial al Republicii Moldova*, 2016, nr. 13-19, 01.
148. Hotărârea Curții Constituționale a Republicii Moldova pentru interpretarea articolului 34 alin. (3) din Constituția Republicii Moldova: nr. 19 din 22.06.2015. În: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 330-331, 33.
149. Hotărârea Curții Constituționale a Republicii Moldova privind excepţia de neconstituţionalitate a unor prevederi ale articolului 328 alin. (1) din Codul penal: nr. 22 din 27.06.2017. În: *Monitorul Oficial al Republicii Moldova*, 2017, nr. 352-355, 92.
150. Hotărârea Curții Constituționale a Republicii Moldova privind excepţia de neconstituţionalitate a unor prevederi din articolele 327 alin. (1) și 361 alin. (2) lit. d) din Codul penal: nr. 33 din 07.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 27-32, 04.
151. Hotărârea Guvernului cu privire la aprobarea Conceptului Sistemului informațional de management în educație: nr. 601 din 12.08.2020. În: *Monitorul Oficial al Republicii Moldova*, 2020, nr. 212-220, 746.
152. Hotărârea Guvernului cu privire la aprobarea cuantumului salariului mediu lunar pe economie, prognozat pentru anul 2016: nr. 879 din 23.12.2015. În: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 347-360, 980.
153. Hotărârea Guvernului cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020: nr. 811 din 29.11.2015. În: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 306-310, 905.
154. Hotărârea Guvernului cu privire la Registrul de stat al serviciilor publice: nr. 169 din 08.09.2021. În: *Monitorul Oficial al Republicii Moldova*, 2021, nr. 230-237, 436.
155. Hotărârea Guvernului cu privire la sistemele speciale de telecomunicaţii ale Republicii Moldova: nr. 735 din 11.06.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 79-81, 833.
156. Hotărârea Guvernului cu privire la Strategia naţională de dezvoltare a societăţii informaţionale „Moldova Digitală 2020”: nr. 857 din 31.10.2013. În: *Monitorul Oficial al Republicii Moldova*, 2013, nr. 252-257, 963.
157. Hotărârea Guvernului cu privire la Strategia naţională în domeniul proprietăţii intelectuale până în anul 2020: nr. 880 din 22.11.2012. În: *Monitorul Oficial al Republicii Moldova*, 2012, nr. 245-247, 951.
158. Hotărârea Guvernului pentru aprobarea Conceptului Sistemului informațional „Registrul resurselor și sistemelor informaționale de stat” și a Regulamentului privind modul de ținere a Registrului resurselor și sistemelor informaționale de stat: nr. 153 din 25.08.2021. În: *Monitorul Oficial al Republicii Moldova*, 2021, nr. 226-229, 415.

159. Hotărârea Guvernului pentru aprobarea Regulamentului privind armonizarea legislației Republicii Moldova cu legislația Uniunii Europene: nr. 1171 din 28.11.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 499-503, 1314.
160. Hotărârea Guvernului pentru aprobarea Regulamentului privind protecția antiteroristă a infrastructurii critice: nr. 701 din 11.07.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 277-284, 773.
161. Hotărârea Guvernului pentru modificarea unor hotărâri ale Guvernului (privind funcția publică și statutul funcționarului public): nr. 942 din 28.12.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 460-462, 1072.
162. Hotărârea Guvernului privind aprobarea Cerinţelor faţă de asigurarea securităţii datelor cu caracter personal la prelucrarea acestora în cadrul sistemelor informaţionale de date cu caracter personal: nr. 1123 din 14.12.2010. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 254-256, 1282.
163. Hotărârea Guvernului privind aprobarea cuantumului salariului mediu lunar pe economie, prognozat pentru anul 2023: nr. 936 din 28.12.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 438-439, 1041.
164. Hotărârea Guvernului privind aprobarea cuantumului salariului mediu lunar pe economie, prognozat pentru anul 2015: nr. 974 din 04.12.2014. În: *Monitorul Oficial al Republicii Moldova*, 2014, nr. 364-365, 1056.
165. Hotărârea Guvernului privind aprobarea Regulamentului cu privire la importul, exportul, proiectarea, producerea şi comercializarea mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei şi a Clasificatorului mijloacelor tehnice speciale destinate pentru obţinerea ascunsă a informaţiei: nr. 100 din 09.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 37-40, 164.
166. Hotărârea Guvernului privind punerea în aplicare a unor acte legislative: nr. 1001 din 26.12.2011. În: *Monitorul Oficial al Republicii Moldova*, 2011, nr. 238-242, 1100.
167. Hotărârea Guvernului Republicii Moldova cu privire la Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016-2020: nr. 811 din 29.11.2015. În: *Monitorul Oficial al Republicii Moldova*, 2015, nr. 306-310, 905.
168. Hotărârea Parlamentului pentru aprobarea Strategiei securităţii naţionale a Republicii Moldova: nr. 153 din 15.07.2011. În: *Monitorul Oficial al Republicii Moldova*, 2011, nr. 170-175, 499.
169. Hotărârea Parlamentului privind aprobarea Strategiei securității informaționale a Republicii Moldova pentru anii 2019-2024 și a Planului de acțiuni pentru implementarea acesteia: nr. 257 din 22.11.2018. În: *Monitorul Oficial al Republicii Moldova*, 2019, nr. 13-21, 80.
170. Hotărârea Parlamentului Republicii Moldova pentru aprobarea Strategiei naționale de apărare și a Planului de acțiuni privind implementarea Strategiei naționale de apărare pentru anii 2018-2022: nr. 134 din 19.07.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 285-294, 441.
171. *Hotărârea Plenului CSJ din 30.06.2008. Dosarul nr. 4-1re-209/2008*. [citat 06.03.2022] Disponibil: http://jurisprudenta.csj.md/archive_courts/cauta/
172. IONIȚĂ, Gheorghe Iulian. Accesul la un sistem informatic și recursul în interesul legii formulat în această materie. În: *Revista de Drept Penal*, 2013, vol. 20, nr. 4, pp. 111-125. ISSN 1223-0790.
173. IUGAN, Andrei Viorel. *Acces fără drept la sisteme informatice și alterarea integrității datelor informatice*. [citat 06.03.2022] Disponibil: https://www.universuljuridic.ro/acces-fara-drept-la-sisteme-informatice-si-alterarea-integritatii-datelor-informatice/

174. *Înalta Curte de Casație și Justiție a României. Secția penală. Decizia nr. 416/A/2016*. [citat 06.03.2022] Disponibil: www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=133689
175. JENUNCHI, Elena. Latura subiectivă a infracțiunii de constrângere de a face declarații. În: *Supremația Dreptului*, 2020, nr. 1, p. 171-176. ISSN 2587-4128.
176. JENUNCHI, Elena. *Răspunderea penală pentru constrângerea de a face declarații*: tz. de doct. în drept. Chișinău, 2020. 182 p.
177. KÖVESI, Laura Codruța. *Combaterea crimei organizate prin dispoziţii de drept penal* / tz. de doct. în drept. Timișoara, 2011. 479 p.
178. Legea comunicaţiilor electronice: nr. 241 din 15.11.2007. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 51-54, 155.
179. Legea cu privire la actele normative: nr. 100 din 22.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 7-17, 34.
180. Legea cu privire la informatică: nr. 1069 din 22.06.2000. În: *Monitorul Oficial al Republicii Moldova*, 2001, nr. 73-74, 547.
181. Legea cu privire la informatizare şi la resursele informaţionale de stat: nr. 467 din 21.11.2003. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 6-12, 44.
182. Legea cu privire la schimbul de date și interoperabilitate: nr. 142 din 19.07.2018. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 295-308, 452.
183. Legea ocrotirii sănătăţii: nr. 411 din 28.03.1995. În: *Monitorul Oficial al Republicii Moldova*, 1995, nr. 34, 373.
184. Legea pentru aprobarea Concepţiei securităţii naţionale a Republicii Moldova: nr. 112 din 22.05.2008. În: *Monitorul Oficial al Republicii Moldova*, 2008, nr. 97-98, 357.
185. Legea pentru modificarea şi completarea Codului penal al Republicii Moldova: nr. 277 din 18.12.2008. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 41-44, 120.
186. Legea 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, 98.
187. Legea pentru modificarea şi completarea Legii telecomunicaţiilor nr. 520-XIII din 7 iulie 1995 şi a Codului penal al Republicii Moldova: nr. 254 din 09.07.2004. În: *Monitorul Oficial al Republicii Moldova*, 2004, nr. 189-192, 848.
188. Legea pentru modificarea și completarea unor acte legislative: nr. 207 din 29.07.2016. În: *Monitorul Oficial al Republicii Moldova*, 2016, nr. 369-378, 751.
189. Legea pentru modificarea unor acte normative: nr. 111 din 21.04.2022. În: *Monitorul Oficial al Republicii Moldova*, 2022, nr. 164-169, 291.
190. Legea pentru ratificarea Convenţiei Consiliului Europei privind criminalitatea informatică: nr. 6 din 02.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2009, nr. 37-40, 104.
191. Legea privind accesul la informaţie: nr. 982 din 11.05.2000. În: *Monitorul Oficial al Republicii Moldova*, 2000, nr. 88-90, 664.
192. Legea privind activitatea particulară de detectiv şi de pază: nr. 283 din 04.07.2003. În: *Monitorul Oficial al Republicii Moldova*, 2003, nr. 200-203, 769.
193. Legea privind activitatea specială de investigaţii: nr. 59 din 29.03.2012. În: *Monitorul Oficial al Republicii Moldova*, 2012, nr. 113-118, 373.
194. Legea privind aprobarea Concepţiei securităţii informaţionale a Republicii Moldova: nr. 299 din 21.12.2017. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 48-57, 122.
195. Legea privind completarea Codului penal şi a Codului de procedură penală: nr. 830 din 07.02.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr. 46-48, 304.
196. Legea privind prevenirea şi combaterea criminalităţii informatice: nr. 20 din 03.02.2009. În: *Monitorul Oficial al Republicii Moldova*, 2010, nr. 11-12, 17.
197. Legea privind sănătatea mentală: nr. 1402 din 16.12.1997. În: *Monitorul Oficial al Republicii Moldova*, 1998, nr. 44-46, 310.

198. Legea României a fondului funciar: nr. 18 din 19.02.1991. În: *Monitorul Oficial al României*, 1991, nr. 31.
199. Legea României pentru punerea în aplicare a Legii nr. 286/2009 privind Codul penal: nr. 187 din 24.10.2012. În: *Monitorul Oficial al României*, 2012, nr. 757.
200. Legea României privind comerțul electronic: nr. 365 din 07.06.2002. În: *Monitorul Oficial al României*, 2002, nr. 483.
201. Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităților publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei: nr. 161 din 19.04.2003. În: *Monitorul Oficial al României*, 2003, nr. 279.
202. Legea telecomunicaţiilor: nr. 520 din 07.07.1995. În: *Monitorul Oficial al Republicii Moldova*, 1995, nr. 65-66, 713.
203. LUNCAN, Gabriel-Ilie. *Corporalitatea bunurilor și calitatea de bun a unui lucru*. [citat 06.03.2022] Disponibil: https://www.juridice.ro/701050/corporalitatea-bunurilor-si-calitatea-de-bun-a-unui-lucru.html
204. LUPȘA, Radu-Lucian. *Rețele de calculatoare. Principii*. [citat 08.07.2022] Disponibil: https://www.cs.ubbcluj.ro/~rlupsa/works/retele.pdf
205. MACARI, Ivan. *Dreptul penal al Republicii Moldova. Partea generală*. Chișinău: CE USM, 2002. 308 p. ISBN 9975-70-190-6.
206. MANEA, Cornelia. Accesul ilegal la un sistem informatic. În: *Revista Pro Lege*, 2009, nr. 1, pp. 40-48. ISSN 1224-2411.
207. *Manifest referitor la politica penală europeană*. [citat 18.12.2020] Disponibil: https://www.zis-online.com/dat/artikel/2009_12_387.pdf
208. *Manual anti-discriminare pentru judecători*. [citat 18.12.2020] Disponibil: https://cnajgs.md/uploads/asset/file/ro/419/Manual_Anti-Discriminare_pentru_Judecatori.pdf
209. MARIN, Cătălin. Accesul, fără drept, la un sistem informatic. În: *Conferința studențească anuală „Nicolae Titulescu". Constant 2011 (București, 25-26 martie 2011)*. București: Pro Universitaria, 2011, pp. 430-443. ISSN 2246-9214.
210. MARIȚ, Alexandru, ȘOMICU (BANU), Marcela. Responsabilitatea şi iresponsabilitatea, responsabilitatea redusă în dreptul penal. În: *Vector European*, 2014, nr. 2, pp. 106-111. ISSN 2345-1106.
211. MARTIN, Daniel, COPEȚCHI, Stanislav. Calificarea tentativei de infracțiune. În: *Integrare prin cercetare și inovare. Ştiinţe juridice și economice (10-11 noiembrie 2015)*. Chișinău: CEP USM, 2015, pp. 53-56.
212. MEDEANU, Tiberiu, CRĂCIUNESCU, Adrian. Accesul ilegal la un sistem informatic elemente constitutive şi delimitarea de alte infracţiuni. În: *Sesiunii ştiinţifice internaţionale „Uniunea Europeană – spaţiu de libertate, securitate şi justiţie" (Academia de Poliţie, Bucureşti, 23 mai 2013)*. București: Editura Universitară, pp. 28-37. ISBN 978-606-591-723-1.
213. MIHALAȘ, Ion. Vârsta – condiție a răspunderii penale. Aspecte comparative cu legislația altor state. În: *Sesiune naţională de comunicări ştiinţifice studenţeşti: Ştiinţe sociale. Ştiințe juridice și economice (4-5 mai 2017, Chişinău)*. Chișinău: CEP USM, 2017, pp. 18-20.
214. MOISE, Adrian Cristian. Infractorii și victimele în cyberspatiu. În: *Curierul Judiciar*, 2016, nr. 9, pp. 475-481. ISSN 1582-7526.
215. MORARU, Victor, GUZUN, Mihai. Informaţia şi securitatea informaţională ca obiect al protecţiei juridico-penale. În: *Revista de Ştiinţe Penale*, 2006, Anuar, pp. 150-159. ISSN 1812-3392.
216. MOSCALCIUC, Irina. Consumatorul – victima infracţiunilor săvârşite în sfera consumului de produse şi servicii. În: *Revista Naţională de Drept*, 2007, nr. 5, pp. 47-53. ISSN 1811-0770.

217. MOȚOC, Costică, GÎRLA, Lilia. Protecția juridico-penală a secretului profesional prin prisma incriminărilor prevăzute la art. 178, 259, 260^1, 260^2 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale”*, 2020, nr. 3, pp. 139-151. ISSN 1814-3199.
218. MOȚOC, Costică, GÎRLA, Lilia. Secretul profesional reproductiv ca obiect imaterial al încălcării inviolabilității vieții personale: constatări *de lege lata*, viziuni doctrinare și jurisprudența CtEDO. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2019, nr. 11, pp. 146-159. ISSN 1814-3199.
219. MUNTEANU, Alin, ȘOFRAN, Cristina Ofelia. Sisteme informatice – o privire de ansamblu. În: *Anale. Seria Informatică. Universitatea Tibiscus*, 2004, vol. II, fasc. II, pp. 111-117. ISSN 2065-7471.
220. NESTOR, Raul Alexandru. *Incriminarea accesului ilegal la un sistem informatic sau riscul de a transforma un mijloc esențial de obținere a informației în mod de încălcare a legii penale*. [citat 06.03.2022] Disponibil: https://www.juridice.ro/753151/incriminarea-accesului-ilegal-la-un-sistem-informatic-sau-riscul-de-a-transforma-un-mijloc-esential-de-obtinere-a-informatiei-in-mod-de-incalcare-a-legii-penale.html
221. NIȚĂ, Nelu, DOBRIN, Vasile. *Principalele forme de manifestare a criminalităţii informatice în contextul actual al dezvoltării tehnologice şi al globalizării*. [citat 04.07.2022] Disponibil: https://www.universuljuridic.ro/principalele-forme-de-manifestare-a-criminalitatii-informatice-in-contextul-actual-al-dezvoltarii-tehnologice-si-al-globalizarii/
222. *Note de curs – Introducere în reţelele de calculator*. [citat 09.07.2022] Disponibil: https://www.afahc.ro/ro/facultate/cursuri/retele_note_curs.pdf
223. ONOFREI, Flavius-Vasile. Statutul juridic al informaţiei electronice în dreptul penal comparat. În: *Studia Universitatis Moldaviae. Seria „Ştiinţe Sociale”*, 2009, nr. 8, pp. 152-157. ISSN 1814-3199.
224. Ordinul SIS cu privire la aprobarea unor acte normative în domeniul organizării funcţionării prestatorilor de servicii de certificare în domeniul aplicării semnăturii electronice: nr. 70 din 15.07.2016. În: *Monitorul Oficial al Republicii Moldova*, 2018, nr. 27-32, 1202.
225. PARENIUC, Alexandru, GHIMPU, Andrei. Tipurile și metodele de săvârșire a infracțiunilor informaționale. În: *Legea şi Viaţa*, 2021, nr. 1-2, pp. 54-60. ISSN 2587-4365.
226. PĂVĂLEANU, Vasile. *Drept penal special*. București: Universul Juridic, 2014. 620 p. ISBN 978-606-673-287-1.
227. PILAT, Sofia. Elementele subiective ale vandalismului: concept şi caracterizare. În: *Anale ştiinţifice ale Academiei „Ştefan cel Mare” a MAIRM: ştiinţe juridice*, 2022, nr. 15, pp. 201-213. ISSN 1857-0976.
228. PÎRȚAC, Cristina. Studiu comparat privind obiectul infracţiunilor de fals în acte publice (art. 332 CP RM). În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 3, pp. 185-197. ISSN 1814-3199.
229. POALELUNGI, Mihai et al. *Manualul judecătorului pentru cauze penale*. Chișinău: Tipografia Centrală, 2013. 1192 p. ISBN 978-9975-53-231-0.
230. POPA, N.D. The concept of material object of the crime in the romanian criminal doctrine. In: *The Juridical Current Journal*, 2010, no. 3, pp. 118-130. ISSN 1224-9173.
231. POPESCU, Adrian-Nicușor. *Atacul cibernetic și principiul interzicerii folosirii forței*. [citat 11.07.2022] Disponibil: https://www.universuljuridic.ro/atacul-cibernetic-si-principiul-interzicerii-folosirii-fortei/
232. POPESCU, Răzvan Nicolae. *Legea nr. 87/2020 „Mi se aplică”? Persoanele îndreptățite la constituirea dreptului de proprietate asupra terenului*. [citat 11.07.2022] Disponibil: https://www.juridice.ro/758030/legea-nr-87-2020-mi-se-aplica-persoanele-indreptatite-la-constituirea-dreptului-de-proprietate-asupra-terenului.html

233. POSTOVANU, Nicolae. Obiectul juridic generic și obiectul juridic de subgrup al infracțiunilor prevăzute la art. 264 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Științe sociale”*, 2020, nr. 3, pp. 236-243. ISSN 1814-3199.
234. *Proiect de aviz comun al Comisiei de la Veneția și al Direcției Generale Drepturile Omului și Statul de Drept (DGI) a Consiliului Europei pe marginea Proiectului de lege nr. 161 pentru modificarea și completarea legislației moldovenești din domeniul criminalității informatice*. [citat 07.03.2022] Disponibil: https://www.parlament.md/LinkClick.aspx?fileticket=IbGsshOB2Ys%3D&tabid=90&language=ro-RO
235. *Proiectul de lege pentru modificarea şi completarea unor acte legislative*. [citat 18.12.2020] Disponibil: procuratura.md/file/2020-11-12_proiect%20si%20nota%20info%20cibernetice.pdf
236. *Proiectul de lege pentru modificarea unor acte normative (modificarea Codului penal și odului contravențional) (533/MJ/2022)*. [citat 30.12.2022] Disponibil: https://cancelaria.gov.md/ro/content/privind-aprobarea-proiectului-de-lege-pentru-modificarea-unor-acte-normative-modificarea
237. *Proiectul legii pentru completarea și modificarea Codului penal al RM (art. 21, 196[1], 196[2] ș.a.)*. [citat 23.01.2021] Disponibil: old.parlament.md/lawprocess/laws/december2008/278-XVI-18.12.2008/
238. *Proiectul legii pentru modificarea și completarea unor acte legislative (Legea privind Serviciul de Informații și Securitate al RM – art. 7; Codul penal – art. 178, 208[1], 259 ș.a.)*. [citat 30.08.2020] Disponibil: www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/3183/language/ro-RO/Default.aspx+&cd=3&hl=ro&ct=clnk&gl=at
239. *Proiectul legii privind protejarea obiectelor de infrastructură esențială pentru asigurarea securității naționale și a ordinii publice*. [citat 18.12.2020] Disponibil: https://www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/5019/language/ro-RO/Default.aspx
240. *Raport al Comisiei către Parlamentul European și Consiliu de evaluare a gradului în care statele membre au adoptat măsurile necesare pentru a se conforma Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului*. [citat 18.12.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:52017DC0474&from=GA
241. REŞETNICOV, Artur. Obiectul material al infracţiunii şi obiectul imaterial al infracţiunii: necesitatea delimitării. În: *Revista Națională de Drept*, 2007, nr. 9, pp. 25-30. ISSN 2587-411X.
242. SAVU, Daniel, TOMESCU, Mihaela, BĂJENARU, Lidia. Internetul lucrurilor – o nouă paradigmă a conectării în Internet. În: *Revista Română de Informatică şi Automatică*, 2017, vol. 27, nr. 1, pp. 5-14. ISSN 1841-4303.
243. SELEVESTRU, Irina. Circumstanţele agravante prevăzute la lit. b) şi d) alin. (2) şi la alin. (3) art. 191 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2015, nr. 11, pp. 126-140. ISSN 1814-3199.
244. SELEVESTRU, Irina. Victima infracţiunilor prevăzute la art. 191 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale”*, 2015, nr. 3, pp. 194-199. ISSN 1814-3199.
245. *Sentința Judecătoriei Chișinău (sediul Buiucani) din 14.02.2019. Dosarul nr. 1-601/2018*. [citat 06.03.2022] Disponibil: https://jc.instante.justice.md/ro/pigd_integration/pdf/c8678a6c-f738-e911-80d5-0050568b021b

246. *Sentința Judecătoriei sect. Botanica, mun. Chișinău, din 11.12.2014. Dosarul nr. 1-620/2014*. [citat 18.12.2020] Disponibil: https://jc.instante.justice.md/ro/pigd_integration/pdf/3798ed32-4281-e411-8112-005056a5d154
247. *Sentința Judecătoriei sect. Botanica, mun. Chișinău, din 26.02.2016. Dosarul nr. 1-12/2016*. [citat 18.12.2020] Disponibil: https://instante.justice.md/ro/pigd_integration/pdf/691A992F-6DDC-E511-A1AB-005056A5D154
248. *Sentința Judecătoriei sect. Botanica, mun. Chișinău, din 30.06.2016. Dosarul nr. 1-163/2016*. [citat 18.12.2020] Disponibil: https://jc.instante.justice.md/ro/pigd_integration/pdf/3fd536fe-cd3e-e611-9a6d-005056a5d154
249. SÎLI, Vitalie, SOROCEANU, Igor. Protecţia infrastructurii critice în contextul asigurării securităţii naţionale. În: *Securitatea națională a Republicii Moldova: provocări și tendințe (14 mai 2022, Chișinău)*. Chișinău: Institutul naţional de informaţii şi securitate „Bogdan, întemeietorul Moldovei”, 2022, pp. 51-57.
250. SLISARENCO, Ion. Conceptul omorului săvârșit în stare de afect. În: *Anale ştiinţifice ale Academiei „Ştefan cel Mare” a MAIRM: ştiinţe juridice*, 2016, nr. XVI, pp. 100-103. ISSN 1857-0976.
251. SOLTAN, Veaceslav. Infracțiunile informatice (art. 259-261[1] Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, pp. 38-43. [citat 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf
252. SOROCEANU, Igor. Caracteristica generală și definirea conceptului de „omor simplu”. În: *Intellectus*, 2021, nr. 3-4, pp. 161-166. ISSN 1810-7079.
253. SPÎNU-DUMNEANU, L. Evoluările internaţionale şi naţionale în domeniul infracţiunilor informatice. În: *Realități și perspective ale învățământului juridic național. Culegerea materialelor științifice elaborate în baza comunicărilor de la Conferinţa ştiinţifică naţională cu participare internaţională, organizată cu ocazia a 60 de ani de la înființarea Facultății de Drept (USM, 01-02 octombrie 2019, Chișinău)*. Chișinău: CEP USM, 2020, pp. 112-120. ISBN 978-9975-149-80-8.
254. STATI, Vitalie. Despre „interesul public”, „daunele considerabile” și nu numai: analiza unui proiect de amendare a Codului penal al Republicii Moldova. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4188261
255. STATI, Vitalie. Fabricarea sau punerea în circulație a monedelor virtuale în Republica Moldova: conotații juridico-penale. În: *Актуальные научные исследования в современном мире // Журнал*. Переяслав, 2019, Вып. 11, ч. 5, с. 100-108. ISSN 2524-0986.
256. STATI, Vitalie. Impactul adoptării Legii nr. 207/2016 asupra normelor din Capitolul X din partea specială a Codului penal al Republicii Moldova. În: *Актуальные научные исследования в современном мире: XIX Междунар. научн. конф., 26-27 ноября 2016 г., Переяслав-Хмельницкий // Сб. научных трудов*, 2016, Вып. 11, ч. 4, с. 25-29. ISSN 2524-0986.
257. STATI, Vitalie. *Infracțiuni economice: Note de curs*. Chișinău: Tipografia centrală, 2019. 600 p. ISBN 978-9975-146-73-9.
258. STATI, Vitalie. Interpretarea sintagmei „săvârșirea infracțiunii”, utilizate în art. 311 din Codul penal al Republicii Moldova. În: *SSRN Electronic Journal*. ISSN 1556-5068. [citat 18.12.2020] Disponibil: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4150275

259. STATI, Vitalie. Problema obiectului material în cazul infracțiunii de încălcare a dreptului de autor și drepturilor conexe. În: *Probleme teoretice şi practice ale economiei proprietăţii intelectuale*. Chișinău: AGEPI, 2007, pp. 228- 230. ISBN 978-9975-911-02-03.
260. STATI, Vitalie. Răspunderea penală pentru infracţiunile în domeniul informaticii şi telecomunicaţiilor. În: Analele Ştiinţifice ale Universităţii de Stat din Moldova. Seria „Ştiinţe socioumanistice". Vol. 1. Chişinău: CEP USM, 2005, pp. 387-394. ISSN 1811-2668.
261. STRATAN, Andrei. Calitatea victimei în cadrul infracțiunilor prevăzute la art. 238 CP RM. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe sociale"*, 2020, nr. 3, pp. 198-203. ISSN 1814-3199.
262. STRÎMBEANU, Alexandru. Accesul ilegal la informaţia computerizată: analiza comparativă a normelor din codurile penale ale Republicii Moldova și statelor membre ale Uniunii Europene. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234979
263. STRÎMBEANU, Alexandru. Acțiunea adiacentă din cadrul infracțiunilor prevăzute la art. 259 din Codul penal. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale"*, 2023, nr. 3, pp. 149-158. ISSN 1814-3199.
264. STRÎMBEANU, Alexandru. Anumite aspecte ale obiectului material (imaterial) al infracțiunilor prevăzute la art. 259 CP RM. În: *Conferinţa ştiinţifică internaţională „Infracţiunea – Răspunderea penală – Pedeapsa. Drept şi Criminologie", Ediţia a 2-a (24-25 martie 2022, Chişinău): Culegere de comunicări*. Chişinău: CEP USM, 2022, pp. 231-242. ISBN 978-9975-62-476-3.
265. STRÎMBEANU, Alexandru. Calculatorul – obiect material al infracțiunilor prevăzute la art. 259 din Codul penal. În: *Conferința științifică națională cu participare internațională „Integrare prin cercetare și inovare", dedicată Zilei internaționale a Științei pentru pace și Dezvoltare (10-11 noiembrie 2022)*. Chișinău: CEP USM, 2022, pp. 69-71. ISBN 978-9975-152-48-8.
266. STRÎMBEANU, Alexandru. Caracterul ilegal al accesului la informaţia computerizată: condiţie de aplicare a art. 259 din Codul penal al Republicii Moldova. În: *Revista Institutului Naţional al Justiţiei*, 2023, nr. 1, pp. 9-13. ISSN 1857-2405.
267. STRÎMBEANU, Alexandru. Circumstanțele agravante ale infracțiunilor de acces ilegal la informația computerizată (art. 259 din Codul penal al Republicii Moldova). În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4331505
268. STRÎMBEANU, Alexandru. Coerența teleologică dintre art. 259 Cod penal și prevederile complementare din legislația națională. În: *Integrare prin cercetare și inovare. Științe juridice și economice. Vol. 1 (7-8 noiembrie 2020, Chișinău)*. Chișinău: CEP USM, 2020, pp. 13-16. ISBN 978-9975-152-48-8.
269. STRÎMBEANU, Alexandru. Condiționarea socială și juridică a incriminării accesului ilegal la informația computerizată. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234976
270. STRÎMBEANU, Alexandru. Elementele constitutive subiective ale infracțiunilor de acces ilegal la informația computerizată (art. 259 din Codul penal al Republicii Moldova). [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313475
271. STRÎMBEANU, Alexandru. Materiale științifice referitoare la accesul ilegal la informaţia computerizată publicate în Republica Moldova. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale"*, 2021, nr. 3, pp. 133-142. ISSN 1814-3199.

272. STRÎMBEANU, Alexandru. Materialele științifice referitoare la accesul ilegal la informaţia computerizată publicate peste hotare. În: *Studia Universitatis Moldaviae, Seria „Ştiinţe Sociale”*, 2021, nr. 8, pp. 114-127. ISSN 1814-3199.
273. STRÎMBEANU, Alexandru. Noţiunea de acces la informaţia computerizată în accepţiunea art. 259 din Codul penal al Republicii Moldova. În: *Revista Institutului Naţional al Justiţiei*, 2022, nr. 3, pp. 16-22. ISSN 1857-2405.
274. STRÎMBEANU, Alexandru. Obiectul juridic generic al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): aspectul *de lege lata*. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234980
275. STRÎMBEANU, Alexandru. Obiectul juridic generic al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): aspectul *de lege ferenda*. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4234982
276. STRÎMBEANU, Alexandru. Obiectul juridic special al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): premise conceptuale. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313468
277. STRÎMBEANU, Alexandru. Obiectul juridic special al infracțiunilor de acces ilegal la informaţia computerizată (art. 259 din Codul penal al Republicii Moldova): reflecții, abordări și soluții. [citat 30.12.2022] Disponibil: În: *SSRN Electronic Journal*. ISSN 1556-5068. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4313472
278. STRÎMBEANU, Alexandru. *Răspunderea penală pentru accesul ilegal la informaţia computerizată: Monografie*. Chişinău: Tipografia Centrală, 2023. 430 p. ISBN 978-5-88554-178-7.
279. STRÎMBEANU, Alexandru. Victima secundară a infracțiunilor prevăzute la art. 259 din Codul penal. În: *Conferința științifică națională cu participare internațională dedicată aniversării a 75-a a Universității de Stat din Moldova „Integrare prin cercetare și inovare” (10-11 noiembrie 2021).* Chișinău: CEP USM, 2021, pp. 6-8. ISBN 978-9975-152-48-8.
280. TAMAS-ERNO, Peter. Accesarea ilegală a conturilor de Facebook privit din perspectiva dreptului penal. În*: Revista Facultății de Drept Oradea*, 2019, nr. 1, pp. 151-157. ISSN 1582-7585.
281. TÎRZIU, Andreea-Maria. Protecția și securitatea informațiilor la nivelul autorităților publice naționale din România. În: *Sesiunea de comunicări ştiinţifice „Oraşul inteligent”*. București: Editura Economică, 2015, pp. 120-138. ISSN 2501-1677.
282. *Tratatul privind funcționarea Uniunii Europene*. [citat 09.07.2022] Disponibil: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0001.02/DOC_2&format=PDF
283. *Tribunalul Bucureşti. Sentinţă penală **** din 02.06.2020*. [citat 18.12.2020] Disponibil: https://www.jurisprudenta.com/jurisprudenta/speta-1763657a/
284. *Tribunalul Covasna. Sentinţă penală nr. 11 din 05.03.2019*. [citat 06.03.2022] Disponibil: https://www.jurisprudenta.com/jurisprudenta/speta-150kzrwm/
285. *Tribunalul Neamț. Sentinţă penală 56/P din 31.08.2016*. [citat 06.03.2022] Disponibil: https://www.jurisprudenta.com/jurisprudenta/speta-109d7k31/
286. *Tribunalul Prahova. Sentinţă penală 614 din 15.12.2017*. [citat 30.12.2022] Disponibil: https://www.jurisprudenta.com/jurisprudenta/speta-144rmtop/
287. ȚURCANU, Valeriu, RUSU, Iulian. *Protecția infrastructurii critice: o nouă prioritate a Republicii Moldova*. [citat 18.12.2020] Disponibil: ipre.md/2021/07/02/protectia-

infrastructurii-critice-o-noua-prioritate-a-republicii-moldova-comentariu-de-valeriu-turcanu-si-iulian-rusu-ipn-md/
288. UDROIU, Mihail. *Dicționar de drept penal și de procedură penală*. București: C.H. Beck, 2009, p. 381. 437 p. ISBN 978-973-115-425-1.
289. URS, Iosif Robi. Consideraţii asupra reglementării posesiei şi detenţiei precare în noul Cod civil român. În: *Analele Universităţii Titu Maiorescu. Drept, Serie Nouă*, 2008, pp. 9-19. ISSN 1584-4781.
290. VARĂ, Octavian. Criminalitatea informatică şi criminalitatea organizată. Elemente de drept comparat. În: *Revista de Investigare a Criminalităţii*, 2014, nr. 1, pp. 101-104. ISSN 1844-7945.
291. VASILOI, Djulieta. Unele raționamente ale noțiunii de „obiect imaterial" al infracțiunii. În: *Legea și viața*, 2020, nr. 8-9, pp. 39-41. ISSN 1810-309X.
292. VASIU, Ioana, VASIU, Lucian, Contaminanţii informatici ca vector ai accesului ilegal. În: *Revista de Drept Penal*, 2006, nr. 2, pp. 37-40. ISSN 1223-0790.
293. VASIU, Ioana, VASIU, Lucian. *Informatică juridică şi drept informatic*. Cluj-Napoca: Editura Albastră, 2002. 225 p. ISBN 973-650-068-3.
294. VASIU, Lucian. *Informatică juridică şi drept informatic. Suport de curs pentru frecvență redusă*. [citat 06.07.2022] Disponibil: file.ucdc.ro/cursuri/8_4_dt4752_Informatica_juridica_Vasiu_Lucian.pdf
295. VISTERNICEANU, Emilia. *Răspunderea penală pentru tâlhărie*. Chișinău: Tipografia Centrală, 2006. 232 p. ISBN 978-9975-78-192-3.
296. ZLATI, George. *Art. 35 din Legea 161/2003 – problematica definiţiilor*. [citat 06.03.2022] Disponibil: https://www.penalmente.eu/2011/06/03/art-35-din-legea-1612003-problematica-definitiilor/
297. ZLATI, George. Dematerializarea obiectului material al infracţiunii în contextul evoluţiei tehnologice şi consecinţele acesteia. În: *Dreptul*, 2013, nr. 9, pp. 163-180. ISSN 1811-0770.
298. ZLATI, George. *Greşita interpretare a accesului la un sistem informatic. Consecinţe practice*. [citat 06.03.2022] Disponibil: https://www.juridice.ro/259331/gresita-interpretare-a-accesului-la-un-sistem-informatic-consecinte-practice.html
299. ZLATI, George. Legitima apărare și starea de necesitate în domeniul criminalității informatice (I). În: *Dreptul*, 2015, nr. 4, pp. 145-172. ISSN 1811-0770.
300. ZLATI, George. *Percheziția informatică. Noțiuni de bază*. [citat 07.07.2022] Disponibil: https://www.universuljuridic.ro/perchezitia-informatica-notiuni-de-baza/
301. ZLATI, George. *Secţia penală a I.C.C.J. şi sistemele informatice*. [citat 07.07.2022] Disponibil: https://www.penalmente.eu/2011/11/02/sectia-penala-i-c-c-j-si-sistemele-informatice/
302. ZLATI, George. *Tratat de criminalitate informatică. Vol. I*. București: Solomon, 2020. 658 p. ISBN 978-606-8892-62-7.
303. ZLATI, George. Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare, precum și a noului Cod penal. În: *Dreptul*, 2012, nr. 10, pp. 204-229. ISSN 1018-0435.
304. ZLATI, George. *Utilizarea clandestină a puterii de calcul a sistemelor informatice aparţinând utilizatorilor unor platforme online. Incidenţa dreptului penal*. https://www.penalmente.eu/2017/09/30/utilizarea-clandestina-a-puterii-de-calcul-a-sistemelor-informatice-apartinand-utilizatorilor-unor-platforme-online-incidenta-dreptului-penal/

B. Surse în limba rusă

305. АБРАМЯН, Т.А. Актуальные проблемы привлечения к ответственности лиц за преступления в сфере информационных технологий. În: *Юрис*т, 2018, № 5, с. 68-72. ISSN 1812-3929.
306. АБУБАКИРОВ, Ф.М., ДЖАФАРОВ, А.Г. Достаточно ли признаков, характеризующих убийство по УК РФ? În: *Законность и правопорядок в современном обществе*, 2016, № 31, с. 115-119. ISBN 978-5-907088-23-8.
307. АГАЕВ, И.Б.О. *Уголовное право Азербайджанской Республики*. Москва: Юристъ, 2009. 684 с. ISBN 978-5-7975-0975-2.
308. АМИРАСЛАНОВ. А.С. Эволюция понятия убийства в уголовном праве России. În: *Актуальные мировые тренды развития социально-гуманитарного знания. Сборник научных трудов по материалам Международной научно-практической конференции*, 2017, с. 110-113. ISBN 978-5-9500429-6-6.
309. АХРАМЕНКА, Н.Ф. Компьютерная информация как предмет преступлений против информационной безопасности. În: *Правовые средства и механизмы противодействия преступности в современном обществе: материалы междунар. науч.- практ. конф. Минск, 16 окт. 2009 г*. Минск: БГУ, 2010, с. 88-90. ISBN 978-985-518-351-9.
310. БАЕВ, О.Я., МЕЩЕРЯКОВ, В.А. Проблемы уголовно-правовой квалификации преступлений в сфере компьютерной информации. În: *Защита информации. Конфидент*, 1998, № 7, с. 8-9. ISSN 2413-3582.
311. БЕГИШЕВ, И.Р. *Понятие и виды преступлений в сфере обращения цифровой информации*: дис. на соиск. учен. степ. канд. юрид. наук. Казань, 2017. 204 с.
312. БЕКМАГАМБЕТОВ, А.Б., РЕВИН, В.П., РЕВИНА, В.В. *Уголовное право Республики Казахстан. Особенная часть*. Москва: Издательский дом Академии Естествознания, 2017. 396 с. ISBN 978-5-91327-448-9.
313. БИКМУРЗИН, М.П. *Предмет преступления: теоретико-правовой анализ*. Москва: Юрлитинформ, 2006. 184 с. ISBN 5-93295-226-1.
314. БОЧАРОВ, Е.В., ШУЛЬГА, И.В. *Уголовное право Российской Федерации*. Владивосток: ВГУЭС, 2015. 44 с. ISBN 978-5-9273-2385-2.
315. ВОРОБЬЁВ, В.В. О предмете преступления, его месте в составе преступления и особенностях в компьютерных преступлениях. În: *Символ науки*, 2015, № 6, с. 221-223. ISSN 2410-700X.
316. ГАБИДУЛЛИН, Э.С. Социальная обусловленность как основание уголовно-правового запрета. În: *Журнал правовых и экономических исследований*, 2017, № 4, с. 32-37. ISSN 1995-1248.
317. ГАЙФУТДИНОВ, Р.Р. Уголовно-правовая характеристика посягательств на персональные данные, обрабатываемые в автоматизированных системах. În: *Ученые записки Казанского университета. Серия Гуманитарные науки*, Том 156, № 4, 2014, с. 158-164. ISSN 2541-7738.
318. ГАСАН, Л.И. К вопросу о трактовке несанкционированного доступа к компьютерной информации (ст. 349 УК Республики Беларусь). În: *Правовое обеспечение инновационного развития общества и государства: материалы междунар. науч. конф. студентов, магистрантов и аспирантов. Минск, 29-30 окт. 2010 г*. Минск, 2011, с. 229-230. ISBN 978-985-518-543-8.
319. ГОЛУБЕВ, В. *Компьютерная информация как объект правоотношений*. [citat 07.03.2022] Disponibil: http://www.crime-research.ru/ library/Golubev09_03.html
320. ГРЕБЕНЬКОВ, А.А. Понятие информационных преступлений, место в уголовном законодательстве России и место признаков информации в структуре их состава. În: *Lex Russica*, 2018, № 4, с. 108-120. ISSN 1729-5920.

321. ГРИЩУК-БУЧКА, Светлана. Уголовно-правовая характеристика преступлений против компьютерной безопасности (по законодательству Республики Молдова). În: *Securitatea informaţională 2010. Conferinţă internaţională (Chişinău, 15-16 aprilie 2010)*. Chișinău: ASEM, 2010, pp. 97-101. ISBN 978-9975-75-509-2.
322. ГУЗЕЕВА, О.С. *Квалификация преступлений в сфере компьютерной информации*. Москва: АГП РФ, 2016. 60 с.
323. ГУЛЬБИН, Ю. Преступления в сфере компьютерной информации. În: *Российская юстиция*, 1997, № 10, с. 24-25. ISSN 0131-6761.
324. ГЫРЛА, Л.Г., ТАБАРЧА, Ю.М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010. 592 с. ISBN 978-9975-4158-2-8.
325. ДВОРЕЦКИЙ, М.Ю. Проблемы толкования терминов при квалификации преступлений по ст. 272 Уголовного кодекса РФ. În: *Вестник Тамбовского университета. Серия: Гуманитарные науки*, 2013, № 12, с. 527-532. ISSN 1810-0201.
326. ДОЛГИЕВА, М.М. Социальная обусловленность возникновения уголовно-правовых запретов нарушений, совершаемых в сфере оборота криптовалюты. În: *Актуальные проблемы российского права*, 2018, № 10, с. 225-235. ISSN 1994-1471.
327. ДОРОНИН, А.М. *Уголовная ответственность за неправомерный доступ к компьютерной информации*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Москва, 2003. 24 с.
328. ДУБКО, М.А. Основание и причины криминализации неправомерного завладения компьютерной информацией. În: Вестник Академии МВД Республики Беларусь, 2017, № 1, с. 87-91. ISSN 2079-9837.
329. ЕФРЕМОВА, М.А. *Уголовно-правовая охрана информационной безопасности*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Москва, 2018. 59 с.
330. ЕФРЕМОВА, М.А. *Уголовно-правовая охрана информационной безопасности*: дис. на соиск. учен. степ. докт. юрид. наук. Москва, 2018. 427 с.
331. ЗУБОВА, М.А. *Компьютерная информация как объект уголовно-правовой охраны*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Казань, 2008. 28 с.
332. ИВАНОВА, Л.В. Виды киберпреступлений по российскому уголовному законодательству. În: *Юридические исследования*, 2019, № 1, с. 25-33. ISSN 2409-7136.
333. ИСМАГУЛОВА, А.Т., ГАЛИАСКАРОВА, А.М. *Уголовные правонарушения в сфере информатизации и связи в Республике Казахстан*. Костанай: New Line Media, 2016. 160 с. ISBN 978-601-7798-10-9.
334. *Комментарий к Уголовному кодексу Республики Казахстан* / Под ред. И.Ш. БОРЧАШВИЛИ. Алматы: Жеті жарғы, 2007. 992 с. ISBN 9965-11-261-4.
335. КОС, А.Д. Направления уголовно-правовой политики в борьбе с преступностью. În: *Право и общество*, 2009, № 4, с. 98-100.
336. КОЧОИ, С., САВЕЛЬЕВ, Д. Ответственность за неправомерный доступ к компьютерной информации. În: *Российская юстиция*, 1999, № 1, с. 44-45. ISSN 0131-6761.
337. КРЫЛОВ, В. Криминалистические проблемы оценки преступлений в сфере компьютерной информации. În: *Уголовное право*, 1998, № 3, с. 81-89. ISSN 2071-5870.
338. КРЫЛОВА, Н.Е. Существует ли уголовное право «в широком смысле слова». În: *Научные основы уголовного права и процессы глобализации: материалы V Российского конгресса уголовного права, 27-28 мая 2010 г*. Москва: Проспект, 2010, с. 721-727. ISBN 978-5-392-01701-0.
339. КУРБАНОВ, Г.С.О. Объективная сторона преступления, связанного с неправомерным доступом к компьютерной информации. În: *Правовая информатика*, 2013, nr. 4, с. 17-20. ISSN 1994-1404.

340. ЛАЗАРЕВА, Наталья. Проблемы квалификации преступлении в области информатики и электросвязи. În: *Закон и жизнь*, 2007, № 12, с. 49-56. ISSN 1810-309X.
341. ЛАЗАРЕВА, Наталья. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista științifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*, 2007, nr. 6, pp. 133-141. ISSN 1857-2081.
342. ЛОКТЮХИН, В.Н. *Архитектура компьютера. Кн.1: Структура персонального компьютера*. Рязань: Ряз. гос. ун-т им. С.А. Есенина, 2008. 136 с. ISBN 978-5-88006-549-3.
343. ЛУКАШОВ, А.И. *Уголовное право Республики Беларусь. Особенная часть* / Под общ. ред. А.И. ЛУКАШОВА. Минск: Гревцов, 2009. 892 с. ISBN 978-985-6826-49-1.
344. ЛЯПУНОВ, Ю., МАКСИМОВ, В. Ответственность за компьютерные преступления. În: *Законность*, 1997, № 1, с. 8-15. ISSN 0869-4486.
345. МАЛЫШЕНКО, Д.Г. *Уголовная ответственность за неправомерный доступ к компьютерной информации*: дис. на соиск. учен. степ. канд. юрид. наук. Москва, 2002. 166 с.
346. *Модельный Уголовный кодекс. Рекомендательный законодательный акт для Содружества Независимых Государств*. [citat 06.03.2022] Disponibil: docs.cntd.ru/document/901781490
347. МУРАДОВ, Э. Признаки специального субъекта как критерий классификации преступлений в сфере экономической деятельности. În: *Уголовное право*, 2003, № 4, с. 51-52. ISSN 2071-5870.
348. *Научно-практический комментарий к Уголовному кодексу Республики Беларусь* / Под общ. ред. А.В. БАРКОВА, В.М. ХОМИЧА. Минск: ГИУСТ БГУ, 2007. 1007 с. ISBN 978-985-6739-60-9.
349. НИКИТЕНКО, О.Г. Несанкционированный доступ к компьютерной информации. În: *Теория и практика совершенствования законодательства и правоприменения: традиции и новации: материалы междунар. науч. конф. студентов, магистрантов и аспирантов (Минск, 30-31 окт. 2009 г.)*. Минск, 2010, с. 189-190. ISBN 978-985-518-379-3.
350. НОВОСЕЛОВ, Г.П. *Учение об объекте преступления. Методологические аспекты*. Москва: Норма, 2001. 208 с. ISBN 5-89123-533-1.
351. ОЗЕРОВА, А.С. О необходимости изменения подхода к понятию «информация» в законодательстве и судебной практике. În: *Правоведение*, 2019, Т. 63, № 1, с. 137-156. ISSN 0131-8039.
352. ОРЕЛ, Ю.В. Системно-правовая непротиворечивость и международно-правовая необходимость и допустимость как принципы криминализации деяний против нормальной деятельности органов и учреждений пенитенциарной службы Украины. În: *Известия Гомельского государственного университета имени Ф. Скорины*, 2015, № 5, с. 105-110. ISSN 1609-9672.
353. ПЕРОВ, В.А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют. În: *Безопасность бизнеса*, 2018, № 2, с. 25-29. ISSN 2072-3644.
354. ПОПОВ, А.Н. О предмете преступления, предусмотренного ст. 272 УК РФ. În: *Криминалистъ*, 2008, № 1, с. 5-10. ISSN 2686-7753.
355. ПОПОВ, А.Н. *Преступления в сфере компьютерной информации*. Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. 68 с.
356. ПОПОВ, А.Н., АИСТОВА, Л.С. *Объект преступления*. Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Академии Генеральной прокуратуры Российской Федерации, 2014. 40 с.

357. *Право на доступ к информации. Доступ к открытой информации* / Отв. ред. БОГДАНОВСКАЯ, И.Ю. Москва: Юстицинформ, 2009. 344 с. ISBN 978-5-7205-1003-9.
358. *Приложение к постановлению МПА СНГ от 27.11.2015 г. № 43-16. Межпарламентская Ассамблея государств-участников Содружества Независимых Государств. Изменения в модельный Уголовный кодекс для государств-участников Содружества Независимых Государств по вопросам борьбы с преступлениями в информационной сфере*. [citat 06.03.2022] Disponibil: www.parliament.am/library/modelayin%20orenqner/336.pdf
359. *Проект Конвенции Организации Объединенных Наций о сотрудничестве в сфере противодействия информационной преступности*. [citat 23.01.2021] Disponibil: https://www.mid.ru/documents/10180/3024875/Проект+конвенции+по+преступности+с+правками+секр+ООН.pdf/c93e68c9-9994-4769-951d-057c4881b8fd
360. РОМАНЮК, С.Н. *Сложные единичные преступления*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Тюмень, 2008. 22 с.
361. РУССКЕВИЧ, Е.А. Законодательные подходы к криминализации деяний, связанных с неправомерным доступом к компьютерной информации в странах Содружества Независимых Государств. În: *Журнал зарубежного законодательства и сравнительного правоведения*, 2018, № 1, с. 116-121. ISSN 1991-3222.
362. САФОНОВ, О.М. *Уголовно-правовая оценка использования компьютерных технологий при совершении преступлений: состояние законодательства и правоприменительной практики, перспективы совершенствования*: дис. на соиск. учен. степ. канд. юрид. наук. Москва, 2015. 222 с.
363. СИВИЦКАЯ, Н.А. Объект компьютерных преступлений в УК Белоруссии. În: *Информационное право*, 2007, № 3, с. 25-29. ISSN 1999-480X.
364. СМОКИНЭ, Андрей, ГРИЩУК-БУЧКА, С.К. вопросу о правовом соотношении понятий: «информационная безопасность», «защита информации» и «кибербезопасность». În: *Studii Juridice Universitare*, 2013, nr. 1-2, pp. 81-88. ISSN 1857-4122.
365. *Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации*. [citat 06.03.2022] Disponibil: https://docs.cntd.ru/document/902140948
366. СПИРИНА, С.Г. Криминологические и уголовно-правовые проблемы преступлений в сфере компьютерной информации: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Волгоград, 2001. 24 с.
367. СТАРИЧКОВ, М.В. Понятие «компьютерная информация» в российском уголовном праве. În: *Вестник Восточно-Сибирского института МВД России*, 2014, № 1, с. 16-20. ISSN 2312-3184.
368. СТАТИ, Виталий. Компьютерные преступления в уголовном законодательстве Республики Молдова, Румынии и Украины: сравнительно-правовой анализ. În: *Kieler Ostrechts-Notizen*, 2016, nr. 2 - 2017, nr. 1, pp. 54-59. ISSN 1862-1589.
369. СТЕПАНОВ-ЕГИЯНЦ, В.Г. *Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект)*: дис. на соис. учен. степ. докт. юрид. наук. Москва, 2016. 389 с.
370. СТРИГУНОВ, В.В. *Введение в компьютерные сети*. Хабаровск: Изд-во Тихоокеан. гос. ун-та, 2016. 103 с. ISBN 978-5-7389-1860-5.
371. ТАНАНА, Ю.Н. Границы уголовно-правовой охраны информационной безопасности. În: *Уголовная политика Республики Беларусь: состояние и пути совершенствования: сб. материалов III Междунар. науч.-практ. конф. (Барановичи, 11-13 мая 2017 г.)*. Барановичи: БарГУ, 2017, с. 161-162. ISBN 978-985-498-763-7.

372. *Уголовное право. Особенная часть* / Под ред. В.А. КАШЕВСКОГО. Минск: Академия МВД, 2012. 736 с. ISBN 978-985-427-775-2.
373. *Уголовный кодекс Республики Армения*. [citat 18.12.2020] Disponibil www.parliament.am/legislation.php?ID=1349&lang=rus&sel=show
374. *Уголовный Кодекс Республики Беларусь: № 275-З от 9 июля 1999 г*. [citat 06.03.2022] Disponibil: https://kodeksy-by.com/ugolovnyj_kodeks_rb.htm
375. *Уголовный кодекс Республики Казахстан*. [citat 06.03.2022] Disponibil: https://online.zakon.kz/Document/?doc_id=31575252
376. Уголовный кодекс Российской Федерации. În: *Собрание законодательства Российской Федерации*, 1996, № 25.
377. *Уголовный кодекс Украины: научно-практический комментарий* / Отв. ред. Е.Л. СТРЕЛЬЦОВ. Харьков: Одиссей, 2007. 864 с. ISBN 978-966-633-611-1.
378. ХИСАМОВА, З.И. Зарубежный опыт уголовно-правовой охраны отношений в сфере использования информационно-коммуникационных технологий. În: *Юридический мир*, 2016, № 2, с. 58-62. ISSN 1811-1475.
379. ШАРКОВ, А.Е. *Неправомерный доступ к компьютерной информации: преступность деяния и проблемы квалификации*: автореф. дис. на соиск. учен. степ. канд. юрид. наук. Ставрополь, 2004. 24 с.

C. Surse în limba engleză

380. *2009 Nevada Code. Title 15 – Crimes and punishments*. [citat 06.03.2022] Disponibil: https://law.justia.com/codes/nevada/2009/title-15/chapter-205/unlawful-acts-regarding-computers-and-information-services/
381. *2010 Arkansas Code. Title 5 – Criminal Offenses*. [citat 06.03.2022] Disponibil: https://law.justia.com/codes/arkansas/2010/title-5/subtitle-4/chapter-41/subchapter-1/5-41-102/
382. *Convention on Cybercrime*. [citat 06.03.2022] Disponibil: https://rm.coe.int/1680081561
383. *Criminal Code of Georgia*. [citat 18.12.2020] Disponibil: https://matsne.gov.ge/en/document/view/16426?publication=241
384. DRĂGAN, Alin Teodorus. Illegal access to a computer system from the standpoint of the current Criminal Code. În: *Journal of Legal Studies "Vasile Goldiş"*, 2019, nr. 23, pp. 33-43. ISSN 1582-5442.
385. *European Council conclusions on Ukraine, the membership applications of Ukraine, the Republic of Moldova and Georgia, Western Balkans and external relations, 23 June 2022*. [citat 18.12.2020] Disponibil: https://www.consilium.europa.eu/en/press/press-releases/2022/06/23/european-council-conclusions-on-ukraine-the-membership-applications-of-ukraine-the-republic-of-moldova-and-georgia-western-balkans-and-external-relations-23-june-2022/
386. *Explanatory Report to the Convention on Cybercrime*. [citat 30.12.2022] Disponibil: https://rm.coe.int/16800cce5b
387. *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*. [citat 18.12.2020] Disponibil: https://www.coe.int/en/web/cybercrime/parties-observers
388. *Recommendation No. R. (89) 9 of the Committee of the Ministers to Member States on Computer-related Crime*. [citat 18.12.2020] Disponibil: http://www.cm.coe.int/ta/rec/1989/89r9.htm
389. SADÂC, Zafer. Theoretical and Practical Considerations regarding the Illegal Access to a Computer System in the Romanian Criminal Law. În: *Technium Social Sciences Journal*, 2021, nr. 26, pp. 944-949. ISSN 2668-7798.
390. *T-CY Guidance Note no. 1 on the notion of "computer system"*. [citat 06.03.2022] Disponibil: https://rm.coe.int/09000016802e79e6

391. *T-CY Guidance Notes*. [citat 18.12.2020] Disponibil: https://rm.coe.int/16802e7132
392. *United Nations Charter*. [citat 11.07.2022] Disponibil: https://www.un.org/en/about-us/un-charter
393. *United Nations Convention on the Rights of the Child*. [citat 06.03.2022] Disponibil: https://www.unicef.org/child-rights-convention/convention-text#
394. *United Nations Convention on the Use of Electronic Communications in International Contracts*. [citat 06.03.2022] Disponibil: https://uncitral.un.org/sites/uncitral.un.org/files/media-documents/uncitral/en/06-57452_ebook.pdf

D. Surse în limba ucraineană

395. АЗАРОВ, Д.С. *Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)*. Київ: Атіка, 2007. 304 с. ISBN 966-326-230-3.
396. АЗАРОВ, Д.С. *Кримінальна відповідальність за злочини у сфері комп'ютерної інформації*: автореф. дис. на здоб. науков. ступ. канд. юрид. наук. Київ, 2003. 18 с.
397. АНДРУШКО, П.П. *Кримінально-правова охорона прав інтелектуальної власності в Україні*. Київ: Форум, 2004. 160 с. ISBN 966-95843-8-8.
398. КАРЧЕВСЬКИЙ, М.В. Злочини у сфері використання комп'ютерної техніки. Київ: Атіка, 2010. 168 с.
399. КАРЧЕВСЬКИЙ, М.В. *Кримінальна відповідальність за незаконне втручання в роботу обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину)*: автореф. дис. на здоб. науков. ступ. канд. юрид, 2003. 19 с.
400. КОЗАК, Н.С. Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. În: *Збірник наукових праць Ірпінської фінансово-юридичної академії (економіка, право)*, 2013, № 2, с. 154-159.
401. *Кримінальний кодекс України*. [citat 18.12.2020] Disponibil: https://zakon.rada.gov.ua/laws/show/2341-14#Text
402. МИХАЙЛОВ, В.Є. *Кримінальна відповідальність за зараження вірусом імунодефіциту людини чи іншої невиліковної інфекційної хвороби: соціальна обумовленість та склад злочину*. Харків: Право, 2011. 248 с. ISBN 978-966-458-295-4.
403. РИЧКА, Д.О. *Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку*: дис. на здоб. наук. ступ. канд. юрид. наук. Ірпінь, 2019, 212 с.
404. РОЗЕНФЕЛЬД, Н.А. *Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж*: дис. на здоб. наук. ступ. канд. юрид. наук. Київ, 2003. 222 с.
405. СОЗАНСЬКИЙ, Т.І., БУРДА, С.Я., СКИБА, А.Я. *Кримінально-правова характеристика злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку у схемах*. Львів: Львівський державний університет внутрішніх справ, 2019. 20 с.
406. ЧУГУНІКОВ, І.І. Додатковий об'єкт злочину: проблема визначення та класифікації. În: *Правове життя сучасної України: матеріали Міжнар. наук.-практ. конф. (м. Одеса, 15 трав. 2020 р.)*. Одеса: Гельветика, 2020, Т. 3, с. 151-155. ISBN 978-966-992-106-2.

DECLARAȚIA PRIVIND ASUMAREA RĂSPUNDERII

Subsemnatul, Strîmbeanu Alexandru, declar pe răspundere personală că materialele prezentate în teza de doctorat sunt rezultatul propriilor cercetări şi realizări ştiinţifice. Conştientizez că, în caz contrar, urmează să suport consecinţele în conformitate cu legislaţia în vigoare.

Strîmbeanu Alexandru

23 ianuarie 2023

CV-UL AUTORULUI

Numele şi prenumele: STRÎMBEANU Alexandru

Cetățenia: Republica Moldova

Studii
1999-2003 – licență în științe juridice, Facultatea de Științe juridice, Universitatea „Valahia” din Târgoviște
2001-2002 – master în drept, Facultatea de Drept, Universitatea Titu Maiorescu din București
2019-2023 – studii de doctorat, Școala Doctorală de Științe Juridice a Universității de Stat din Moldova, Specialitatea 554.01 – Drept penal și execuțional penal

Domeniile de interes științific: dreptul penal

Participări la foruri științifice: manifestări internaționale – 2; manifestări naționale cu participare internațională – 3; manifestări naționale – 1.

Lucrări științifice publicate: 18 publicații științifice la tema tezei de doctorat, inclusiv o monografie

Cunoașterea limbilor străine
rusa – bine
engleza – elementar

Date de contact
adresa: satul Javgur, raionul Cimișlia, Republica Moldova
telefon: + 373 24133321
e-mail: alexandrustrimbeanu@yahoo.ro