STUDIA UNIVERSITATIS MOLDAVIAE, 2021, nr.8(148)
Seria "Ştiinţe Sociale" ISSN 1814-3199, ISSN online 2345-1017, p.114-127

CZU: 343.349 + 343.23:004 **DOI: http://doi.org/10.5281/zenodo.5113126**

MATERIALELE ŞTIINŢIFICE REFERITOARE LA ACCESUL ILEGAL LA INFORMAŢIA COMPUTERIZATĂ PUBLICATE PESTE HOTARE

Alexandru STRÎMBEANU

Universitatea de Stat din Moldova

În cadrul studiului de față sunt analizate materiale 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 astfel de oameni de știință se numără: V.Stati (Republica Moldova); A.Crăciunescu, M.Dobrinoiu, A.T. Drăgan, C.Duvac, G.Florescu, V.Florescu, L.C. Kövesi, C.Manea, T.Medeanu, G.Zlati (România); D.S. Azarov, S.Ia. Burda, D.O. Ricika, N.A. Rozenfeld, A.Ia. Skiba, T.I. Sozanski (Ucraina); I.R. Beghișev, A.M. Doronin, A.N. Popov, V.G. Stepanov-Eghianț (Federația Rusă). Investigațiile acestor autori se axează, în particular, pe infracțiunile prevăzute la: art.259 din Codul penal al Republicii Moldova; art.42 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; art.360 din Codul penal al României; art.361 din Codul penal al Ucrainei; art.272 din Codul penal al Federației Ruse. În prezentul studiu se acordă atenție prioritară examinării elementelor constitutive (obiectul; latura obiectivă; latura subiectivă; subiectul) ale infracțiunilor de acces ilegal la informația computerizată, prevăzute de aceste articole. Ideile și concepțiile analizate urmează a fi luate în considerare 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.

Cuvinte-cheie: *acces ilegal la informaţia computerizată, infracţiuni informatice, obiectul infracţiunii, latura obiectivă a infracţiunii, latura subiectivă a infracţiunii, subiectul infracţiunii.*

SCIENTIFIC MATERIALS REGARDING ILLEGAL ACCESS TO COMPUTER INFORMATION PUBLISHED ABROAD

This study analyses the scientific materials published abroad by scientists who have contributed to the development of the theoretical conception of solving the problem of criminal liability for illegal access to computer information. Among such scientists we shall enumerate: V.Stati (the Republic of Moldova); A.Craciunescu, M.Dobrinoiu, A.T. Dragan, C.Duvac, G.Florescu, V.Florescu, L.C. Kovesi, C.Manea, T.Medeanu, G.Zlati (Romania); S.D. Azarov, S.Ia. Burda, D.O. Ricika, N.A. Rozenfeld, A.Ia. Skiba, T.I. Sozanski (Ukraine); I.R. Beghishev, A.M. Doronin, A.N. Popov, V.G. Stepanov-Eghiants (the Russian Federation). The investigations of these authors focus, in particular, on the offenses provided in: art.259 of the Criminal Code of the Republic of Moldova; art.42 of the Romanian Law no. 161 of 19.04.2003 on some measures to ensure transparency in the exercise of public dignity, public office and in the business environment, the prevention and sanctioning of corruption; art.360 of the Criminal Code of Romania; art.361 of the Criminal Code of Ukraine; art.272 of the Criminal Code of the Russian Federation. In the present study, priority is given to the examination of the constituent elements (object; objective side; subjective side; subject) of the offences of illegal access to computer information, provided by these articles. The analysed ideas and conceptions are to be taken into account in the process of elaborating the theoretical conception of solving the problem regarding the liability for the crimes provided in art.259 of the Criminal Code of the Republic of Moldova.

Keywords: *illegal access to computer information, computer crimes, the object of the crime, the objective side of the crime, the subjective side of the crime, the subject of the crime.*

Introducere

Una dintre sarcinile de bază ale cercetărilor cu caracter juridico-penal constă în contribuirea la dezvoltarea dreptului penal ca ramură a științei. 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.

Rezultate și discuții

În 2003 a fost publicat autoreferatul tezei de doctorat susținute de *A.M. Doronin* [1].

Autorul 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 sfera informațiilor computerizate. Adoptarea și aplicarea acesteia sunt condiționate social, inclusiv sub aspectul prevenirii comiterii unei astfel de fapte". 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 infornație, fie sistemul informatic în care se află informaţia computerizată". Același autor arată că „norma penală care stabilește răspunderea pentru accesul ilegal la informaţia computerizată este o normă de referire. 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.". 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 informaţia computerizată destinată accesului liber al unui număr nelimitat de persoane (de exemplu, bazele de date juridice, programele educaționale etc.)". În aceeași ordine de idei, respectivul autor propune adoptarea unei variante perfecționate a art.272 din Codul penal al Federației Ruse (care este similar cu art.259 CP RM).

În același an 2003 de către *N.A. Rozenfeld* a fost susținută teza de doctorat axată pe problema abordată de noi [2].

Autorul în cauză consideră că obiectul juridic generic al infracțiunilor prevăzute la art.361-363 din Codul penal al Ucrainei îl formează „relațiile sociale în domeniul asigurării atât a funcționării neîntrerupte și stabile a computerelor, a sistemelor și rețelelor de computere, cât și a siguranței și integrității informațiilor computerizate, precum și a suporturilor pentru asemenea informații". În ce privește obiectul juridic special al infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei (care este similar cu art.259 CP RM), N.A. Rozenfeld enunță că acesta îl constituie „dreptul de a deține și a dispune de informaţia computerizată". În opinia aceluiași autor, obiectul material sau imaterial al infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei este reprezentat de: computere; sisteme sau rețele de computere; informații computerizate și suporturi de informații computerizate. Doar posesorii și utilizatorii informației computerizate sunt considerați de către N.A. Rozenfeld victime ale infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei. În viziunea acestui autor, „accesul ilegal la informaţia computerizată trebuie privit ca un astfel de acces la informaţia computerizată sau la suporturile pentru o asemenea informație, care are loc fie fără acordul sau în pofida dezacordului proprietarului informaţiei computerizate sau al unei persoane autorizate de acesta, fie cu încălcarea regulilor de acces stabilite de aceștia, care se comite prin utilizarea de software și (sau) a unor mijloace tehnice speciale". Analiza infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei se încheie cu examinarea elementelor constitutive subiective.

În 2006 iese de sub tipar monografia elaborată de către *M.Dobrinoiu* [3].

În cadrul acesteia este efectuată, printre altele, analiza infracţiunilor prevăzute la art.42[1] 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 [4] (în continuare – Legea României nr.161/2003). În opinia lui M.Dobrinoiu, infracțiunile respective aparţin la 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 concluzionează că acesta „este reprezentat de valoarea socială numită sistem informatic şi de relaţiile sociale care iau naştere în legătură cu utilizarea sistemelor automate de prelucrare a datelor în societate". După M. Dobrinoiu, obiectul juridic special al infracțiunilor supuse analizei îl formează „interesul juridic protejat [...] al proprietarului, deţinăto-

[1] 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".

Articolul 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.

rului sau utilizatorului de drept (legal) al sistemului informatic, dar şi al proprietarului, deţinătorului ori utilizatorului de drept al datelor informatice, stocate sau vehiculate în respectivul sistem informatic". 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. şi software – programe, aplicaţii, baze de date etc.) şi [...] datele informatice spre care se îndreaptă atenţia făptuitorului". 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. Practica judiciară a demonstrat însă că, în marea majoritate a cazurilor, asemenea persoane posedă cunoştinţe în domeniul tehnologiei informaţiei. Dintre acestea, un procent însemnat îl reprezintă experţii în sisteme de calcul şi reţelele de calculatoare, familiarizaţi cu „spargerea" măsurilor de securitate ale calculatoarelor sau reţelelor de calculatoare". Subiectul pasiv al infracţiunilor prevăzute la art.42 al Legii României nr.161/2003 este caracterizat 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. Prin extensie, poate exista subiect pasiv colectiv, alcătuit dintr-o mulţime de persoane fizice sau juridice, atunci când accesul în sistemul informatic generează în mod automat accesul ilegal în alte sisteme similare interconectate cu primul. 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. 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)". 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). Accesul, în înţelesul dat de lege, desemnează intrarea în tot sau numai într-o parte a sistemului informatic. Metoda de comunicare – la distanţă, inclusiv graţie legăturii prin satelit sau nu, ori de aproape – nu prezintă importanţă. 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 (sursă de alimentare, butoane de pornire, tastatură, mouse, joystick). Manipularea acestor dispozitive se transformă în solicitări către Unitatea Centrală de Prelucrare (UCP) a sistemului, care va procesa date ori va rula programe de aplicaţii în beneficiul intrusului. Va exista acces ilegal în formă simplă şi în cazul în care intrusul, manipulând propriile echipamente periferice, de la distanţă, găseşte şi utilizează o cale externă de intrare într-un alt sistem de calcul. Este cazul tipic al accesării unei alte staţii de lucru aflate într-o reţea. Pentru obţinerea accesului, făptuitorul va încerca o gamă variată de procedee tehnice, cum ar fi: atacul prin parolă, atacul de acces liber, atacul care exploatează slăbiciunile tehnologice, atacul care exploatează bibliotecile partajate, atacul IP ori atacul prin deturnarea TCP etc.". 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* [5].

Din punctul de vedere al acestui autor, obiectul juridic generic al infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei îl formează „relațiile sociale cu privire la utilizarea computerelor, sistemelor și rețelelor informatice". D.A. Azarov distinge două obiecte juridice speciale ale acestor infracțiuni: obiectul juridic principal – „relațiile sociale din domeniul informațiilor computerizate, care apar și există în legătură cu desfășurarea activităților de ordin informațional asupra informațiilor computerizate"; obiectul juridic secundar – „relațiile sociale de proprietate". În viziunea acestui autor, în cazul infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei, obiectele supuse influenței nemijlocite infracționale pot fi împărțite în două grupuri: „lucrurile din lumea materială (mijloace tehnice dăunătoare destinate accesului ilegal la informaţia computerizată; sisteme informatice; rețele de computere; rețele de telecomunicații) și alte entități (de exemplu, informație)". Prezintă interes reflecțiile lui D.A. Azarov cu privire la urmările prejudiciabile în contextul infracțiunilor examinate: „Inițial, în art.361 din Codul penal al Ucrainei erau menționate urmările prejudiciabile sub forma distorsionării sau distrugerii informației computerizate sau a suporturilor pentru astfel de informații. O asemenea dispoziție legală a fost supusă unor critici meritate: termenul „distorsiune" este utilizat incorect în raport cu suporturile pentru informațiile computerizate, deoarece informațiile pot fi distorsionate, iar suporturile în cauză pot fi deteriorate sau distruse; pentru cauzarea unor asemenea urmări, răspunderea

poate fi aplicată în conformitate cu articolele din Titlul VI „Infracţiuni contra proprietăţii" al Părţii speciale a Codului penal al Ucrainei". Analiza infracţiunilor prevăzute la art.361 din Codul penal al Ucrainei o încheie examinarea caracteristicilor subiectului şi ale laturii subiective.

În 2009 a fost publicat articolul ştiinţific al cărui autor este *C.Manea* [6].

Această publicaţie este dedicată pertractării infracţiunilor prevăzute la art.42 din Legea României nr.161/2003. Astfel, C.Manea relevă că obiectul juridic special al acestor infracţiuni constă în „relaţiile sociale care se nasc şi se dezvoltă în legătură cu securitatea şi confidenţialitatea sistemului informatic ori care se referă la încrederea în datele şi sistemele informatice sau în desfăşurarea corectă a operaţiunilor legate de acestea". Privitor la obiectul material sau imaterial al infracţiunilor prevăzute la art.42 din Legea României nr.161/2003, autorul respectiv susţine că acesta este reprezentat de „entităţile materiale care reprezintă sistemele sau reţelele informatice (hardware – cabluri, plăci, servere etc. şi software – programe, aplicaţii, baze de date etc.) asupra cărora se îndreaptă acţiunea ilicită". C.Manea nu uită să caracterizeze subiectul activ al infracţiunilor în cauză – „orice persoană fizică ce întruneşte condiţiile generale pentru a răspunde penal. De regulă, aceste persoane sunt experţi în calculatoare şi reţelele de calculatoare, persoane familiarizate cu „spargerea" măsurilor de securitate luate pentru protecţia calculatoarelor sau reţelelor de calculatoare, ori care dispun de un set de cunoştinţe în domeniu. Subiectul activ poate fi şi o persoană juridică cu limitările şi în condiţiile prevăzute în art.19[1] C.pen.[2]". În privinţa subiectului pasiv al infracţiunilor prevăzute la art.42 din Legea României nr.161/2003, doctrinarul în cauză evocă: „Este persoana fizică sau juridică deţinătoare de drept a sistemului informatic. Poate fi subiect pasiv secundar şi altă persoană decât deţinătoarea sistemului informatic, în cazul în care datele informatice vizate de accesul ilegal se referă la o persoană fizică sau juridică, alta decât deţinătoarea sistemului informatic". Nelipsit de interes este punctul de vedere exprimat de C.Manea cu privire la conţinutul elementului material al infracţiunilor analizate: „Practic, făptuitorul acţionează asupra sistemului informatic prin forţarea acestor protecţii. Forţarea unei protecţii logice variază de la încercarea de aflare a combinaţiei corecte prin introducerea repetată, de la tastatură, a unor secvenţe alfanumerice, până la rularea unor programe specializate care identifică secvenţa de acces, ori comandă sistemului anumite instrucţiuni ce permit „ocolirea" dispozitivului logic de blocare. Pentru existenţa elementului material al acestei norme de incriminare 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[3]". Caracterizând latura subiectivă a infracţiunilor 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. 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. Este, totuşi, posibil să existe o motivaţie indirect lucrativă, de exemplu, dorinţa de a face rău unui concurent. 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".

În 2011 a fost susţinută teza de doctorat elaborată de *L.C. Kövesi* [7].

În compartimentul VI.3.3.1 al acestei teze sunt investigate infracţiunile prevăzute de art.42 din Legea României nr.161/2003. Cu privire la obiectul juridic special al infracţiunilor în cauză, L.C. Kövesi susţine că acesta îl constituie „relaţiile sociale care apără securitatea sistemului informatic, inviolabilitatea acestuia şi care sunt de natură a garanta confidenţialitatea şi integritatea atât a datelor, cât şi a sistemelor informatice". După aceasta, autoarea punctează că infracţiunile analizate „lezează mai multe relaţii sociale, precum patrimoniul organizaţiei, instituţiei, persoanei fizice, persoanei juridice, relaţiile privind protecţia acestui patrimoniu şi cele privind încrederea publică în măsurile de siguranţă ale integrităţii datelor şi programelor informatice. Reglementarea legală urmăreşte să protejeze sistemele informatice şi datele stocate pe acestea

[2] Se are în vedere art.19[1] din Codul penal al României din 21.07.1968*: „Persoanele juridice, cu excepţia statului, a autorităţilor publice şi a instituţiilor publice care desfăşoară o activitate ce nu poate face obiectul domeniului privat, răspund penal pentru infracţiunile săvârşite în realizarea obiectului de activitate sau în interesul ori în numele persoanei juridice, dacă fapta a fost săvârşită cu forma de vinovăţie prevăzută de legea penală. Răspunderea penală a persoanei juridice nu exclude răspunderea penală a persoanei fizice care a contribuit, în orice mod, la săvârşirea aceleiaşi infracţiuni".

* Buletinul Oficial, 1968, nr.79-79 bis.

[3] Potrivit acestei norme, „acţionează fără drept persoana care se află în una dintre următoarele situaţii: a) nu este autorizată, în temeiul legii sau al unui contract; b) depăşeşte 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 desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic".

de accesul neautorizat. Putem afirma că în raport cu dispoziţia legală aceste infracţiuni lezează mai multe relaţii sociale şi ca atare au două sau mai multe obiecte juridice, dintre care unul principal şi altul secundar. În cazul de faţă, de exemplu, accesul neautorizat la un sistem informatic în domeniul apărării loveşte atât în siguranţa naţională şi capacitatea de apărare a statului, cât şi în instituţia sau persoana titulară a sistemului penetrat sau a informaţiilor accesate". Referitor la obiectul material sau imaterial al infracțiunilor prevăzute la 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 (hardware-cabluri, servere, plăci, programe etc.) asupra cărora se îndreaptă fapta de a accesa, fără drept, la un sistem informatic". În continuare, dânsa formulează concluzii cu privire 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. Astfel, persoana fizică răspunde penal dacă a împlinit vârsta de 14 ani şi a săvârşit fapta cu vinovăţie şi are discernământ, iar persoana juridică dacă a comis fapta în realizarea obiectului de activitate sau în interesul ori în numele persoanei juridice". 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. De regulă, este persoana fizică sau juridică proprietara sau deţinătoarea de drept a sistemului informatic accesat ilegal sau a datelor informatice vizate. Acest subiect pasiv poate fi şi unul colectiv, alcătuit dintr-o mulţime de persoane fizice sau juridice, atunci când accesul în sistemul informatic generează în mod automat accesul ilegal în alte sisteme similare interconectate cu primul". De asemenea, este analizat elementul material al acestor infracțiuni. L.C. Kövesi consideră că acesta „se realizează printr-o acţiune, şi anume – „accesul interzis", adică fără drept, într-un sistem informatic. Aşadar, pentru realizarea acestei infracţiuni trebuie ca subiectul activ să nu fie autorizat. 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 dintre următoarele situaţii: nu este autorizată, în temeiul legii sau al unui contract; depăşeşte limitele autorizării; 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 desfăşura activităţi ştiinţifice sau de a desfăşura orice altă operaţiune într-un sistem informatic". Nu în ultimul rând, este stabilit conținutul laturii subiective a infracțiunilor prevăzute la art.42 din Legea 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.

În 2012 este publicat articolul științific elaborat de către *V. Florescu* și *G. Florescu* [8].

Obiectul de investigare al acestora îl reprezintă, printre altele, infracțiunile prevăzute la art.42 din Legea României nr.161/2003. În această ordine de idei, V.Florescu și G.Florescu identifică valorile sociale specifice și relațiile sociale aferente apărate împotriva infracțiunilor respective: „În special, în situaţia acestui tip de infracţiune, 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 (adică deţin un drept) asupra sistemului sau a informaţiilor stocate în acel sistem accesat fără drept, ţinând cont de faptul că proprietarul sistemului nu este obligatoriu şi proprietarul informaţiilor stocate în sistemul său. De exemplu: accesul neautorizat la un sistem informatic din domeniul transportului aerian de pasageri (aeroport) loveşte atât în siguranţa pasagerilor, cât şi în instituţia sau persoana titulară a sistemului penetrat ori a informaţiilor accesate, care aparţin mai multor companii aeriene de transport". Comportă originalitate opinia acestor autori cu privire la obiectul material sau imaterial al infracțiunilor prevăzute la art.42 din Legea României nr.161/2003: „Din punct de vedere fizic, material sunt apărate echipamentele electronice şi electromecanice care compun sistemele informatice: calculatoare, reţele de calculatoare cu echipamentele specifice care le compun, echipamente periferice, cabluri electrice sau cabluri optice, canalele radio, blocuri de memorie, servere etc. dar şi programele şi aplicaţiile care rulează în sistemul informatic, baze de date şi datele informatice conţinute de sistem, care reprezintă ţinta infractorului". 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 a persoanei. Rezultă că orice persoană ce întruneşte condiţiile generale pentru a răspunde penal poate avea rolul de subiect activ, inclusiv persoana juridică cu limitările şi în condiţiile prevăzute în art.19[1] Cod penal". Caracterizând subiectul pasiv al infracțiunilor prevăzute la art.42 din Legea României nr.161/2003, aceiași autori susțin: „Poate fi persoana fizică sau juridică deţinătoare de drept a sistemului informatic. Concomitent, în secundar, poate fi şi altă persoană decât deţinătoarea sistemului informatic, în cazul în care datele informatice vizate de accesul ilegal se referă la o persoană fizică sau juridică, alta decât deţinătoarea sistemului informatic, de exemplu,

făptuitorul accesează ilegal, fără drept, serverul de date privind personalul angajat al unei instituţii, de unde extrage date confidenţiale personale ale angajaţilor. Pentru această dispoziţie legală, nu prezintă interes modul sau scopul în care făptuitorul utilizează aceste informaţii, aceasta făcând subiectul unui alt tip de infracţiune". În fine, prezintă valoare explicativă netăgăduită opinia lui V.Florescu și G.Florescu cu privire la elementul material al infracțiunilor examinate: „Accesul fără drept la un sistem informatic înseamnă interacţiunea făptuitorului cu sistemul de calcul vizat prin intermediul echipamentelor periferice de control: tastatura, mouse-ul sau touchscreen-ul. Esenţial pentru existenţa elementului material al acestei norme de incriminare este ca accesul la sistemul informatic să se realizeze de către persoana care se află într-una din următoarele situaţii: nu este autorizată în temeiul legii sau al unui contract, depăşeşte limitele autorizării, 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 desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic, adică fără drept, în înţelesul dat de lege. Nu este necesar ca accesul fără drept să se exercite numai prin acţionarea fizică, nemijlocită, a sistemului de către făptuitor. Acesta poate fi manipulat şi de la distanţă prin intermediul reţelei de calculatoare dacă sistemul ţintă este conectat la ea".

Din același an 2012 datează articolul științific al lui *G. Zlati* [9].

Autorul ia în vizor anumite probleme legate de calificarea faptelor în baza art.42 din Legea României nr.161/2003. Astfel, atrage atenția analiza raportului dintre infracțunile prevăzute la acest articol și infracțiunea prevăzută la alin.(4) art.24[4] al Legii României nr.365 din 07.06.2002 privind comerțul electronic [10] (în continuare – Legea 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. 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 încălcarea măsurilor de securitate, prevăzută în art.42 alin.(1) și (3) din Legea nr.161/2003" [11]. 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. [...] Accesul nu trebuie privit ca fiind o simplă interacțiune cu sistemul informatic vizat. Acest mod simplist de interpretare a noțiunii de acces [...] nu face decât să extindă aplicabilitatea textului de lege dincolo de intenția legiuitorului european, intenție materializată într-un act juridic transpus în mod fidel de legiuitorul român". Abordând raportul dintre infracțiunile prevăzute la art.42 din Legea României nr.161/2003 și infracțiunea prevăzută la alin.(1) art.27[5] din Legea 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)[6] 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. Soluția corectă este de a califica acest raport drept un concurs de calificări. 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. Susținem acest lucru deoarece retragerea de numerar nu poate fi realizată decât prin accesarea bancomatului (introducerea cardului, a codului PIN și a sumei ce se dorește a fi retrasă). Discutăm, așadar, despre o legătură intrinsecă între accesul fără drept la un sistem informatic și retragerea de numerar din bancomat. Cu alte cuvinte, accesul se confundă cu retragerea de numerar ori o tentativă de retragere de numerar. De exemplu, să presupunem că accesul la sistemul informatic (în speță, bancomatul) se consumă în momentul introducerii corecte a codului PIN. 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]".

Tot din 2012 datează articolul științific elaborat de *C.Duvac* [12].

Obiectul de studiu al acestuia îl constituie infracțiunile de acces ilegal la un sistem informatic, prevăzute la art.360 din Codul penal al României. Analizând obiectul juridic special al respectivelor infracțiuni, C.Duvac

[4] Această normă (abrogată prin Legea României nr.187/2012) prevedea răspunderea pentru tentativa la falsificarea instrumentelor de plată electronică.
[5] 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 consimțământul titularului instrumentului respectiv".
[6] Norma dată se referă la „retrageri de numerar, precum și încărcarea și descărcarea unui instrument de monedă electronică".

susţine 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". În ceea ce privește obiectul material sau imaterial al infracțiunilor prevăzute la art.360 din Codul penal al României, doctrinarul opinează că acesta constă în „entităţile materiale care reprezintă sistemele sau reţelele informatice (hardware – cabluri, plăci, servere etc. şi software – programe, aplicaţii, baze de date etc.) asupra cărora se îndreaptă acţiunea ilicită". În vederea interpretării prevederilor art.360 din Codul penal al României, 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, 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)"; „Programul informatic reprezintă un ansamblu de instrucţiuni care pot fi executate de un sistem informatic în vederea obţinerii unui rezultat determinat". Același autor caracterizează condițiile pe care trebuie să le îndeplinească subiecţii infracţiunilor prevăzute la art.360 din Codul penal al României: „Subiectul activ nemijlocit (autor) poate fi orice persoană fizică ce întruneşte condiţiile generale pentru a răspunde penal. De regulă, aceste persoane posedă cunoştinţe temeinice în domeniul IT, fiind familiarizate cu „spargerea" măsurilor de securitate prestabilite pentru protecţia calculatoarelor sau reţelelor de calculatoare. Subiectul activ al acestei infracţiuni poate fi şi o persoană juridică cu limitările şi în condiţiile prevăzute în art.135 C.pen."; „Subiectul pasiv al infracţiunii examinate este persoana fizică sau juridică deţinătoare legitimă a sistemului informatic. Poate fi subiect pasiv secundar şi o altă persoană decât deţinătoarea sistemului informatic, în cazul în care datele informatice vizate de accesul ilegal se referă la o persoană fizică sau juridică, alta decât deţinătoarea sistemului informatic (de exemplu, făptuitorul pătrunde ilegal în reţeaua de evidenţă informatizată a persoanei, extrage date personale referitoare la un anumit cetăţean şi le foloseşte astfel încât îi creează acestuia o serie de consecinţe negative de ordin administrativ ori juridic sau de altă natură)". Cu referire la elementul material al infracțiunilor pertractate, C.Duvac afirmă: „Constituie infracţiunea de acces ilegal la un sistem informatic în concurs real cu violarea secretului corespondenţei accesarea aplicaţiei de poştă electronică pentru a obţine mesajele anterioare, primite sau trimise de către subiectul pasiv, în scopul obţinerii de date informatice"; „Nu sunt întrunite elementele constitutive ale infracţiunii examinate dacă făptuitorul interacţionează cu un sistem informatic ce permite accesul liber sau gratuit al publicului 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, iar datele informatice stocate nu sunt personalizate şi semnalizate ca atare prin criptare sau protejare. Aceeaşi idee se susţine dacă se accesează unele date informatice stocate sau vehiculate de altă persoană care are acces la acelaşi computer, faptă despre care se afirmă însă că reprezintă o încălcare a reglementărilor din instituţia respectivă, pe linia protejării informaţiilor". Nelipsite de interes sunt opiniile acestui autor cu privire la cerinţele esenţiale pe care trebuie să le îndeplinească acțiunile incriminate în art.360 din Codul penal al României: „Acţionează fără drept persoana care se află în una dintre următoarele situaţii: nu este autorizată, în temeiul legii sau al unui contract; depăşeşte limitele autorizării sau 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 desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic – art.35 alin.(2) din Legea nr.161/2003"; „Nu acţionează fără drept însă cei care accesează sistemele informatice cu autorizarea celor în drept (de pildă, cu aprobarea şefului instituţiei, a ordonatorului de credite), 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". Nu în ultimul rând, C.Duvac formulează concluzii care se referă la latura subiectivă a infracţiunilor prevăzute la art.360 din Codul penal al României: „Accesul ilegal la un sistem informatic, în variantele prevăzute în alin.(1) şi (3), se poate comite numai cu intenţie directă sau indirectă. Săvârşirea din culpă a faptei prevăzute în art.360 C. pen. nu atrage incidenţa acestui text"; „Scopul este o condiţie constitutivă a infracţiunii numai în cazul variantei agravate prevăzute în alin.2 al textului. 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".

În 2013 a fost publicat articolul științific elaborat de către *T.Medeanu* și *A.Crăciunescu* [13].

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 din Codul penal

al României. Examinând obiectul juridic special al acestor infracţiuni, T.Medeanu şi A.Crăciunescu enunţă că acesta îl constituie „relaţiile sociale referitoare la ocrotirea şi apărarea sistemelor informatice şi la securitatea datelor informatice". Obiectul material al infracţiunilor prevăzute la art.360 din Codul penal al României este caracterizat astfel de către aceşti autori: „sistemul informatic în care se realizează accesul fraudulos". Caracteristicile subiecţilor acestor infracţiunii, evocate de aceşti doi autori, nu diferă mult de respectivele caracteristici prezentate mai sus, evidenţiate de către alţi doctrinari: „Subiectul activ al infracţiunii poate fi orice persoană fizică ce întruneşte condiţiile de vârstă şi responsabilitate prevăzute de legea penală. În general, aceste persoane sunt experţi în calculatoare şi reţelele de calculatoare, sau persoane care dispun de un set de cunoştinţe în domeniu. Uneori sunt familiarizaţi cu măsurile de securitate luate pentru protecţia calculatoarelor sau reţelelor de calculatoare, provenind din domenii care realizează astfel de programe sau activităţi. Subiect activ poate fi şi o persoană juridică cu limitările şi în condiţiile prevăzute în art.135 C.pen."; „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. Poate fi subiect pasiv secundar şi altă persoană decât deţinătoarea sistemului informatic, în cazul în care datele informatice vizate de accesul ilegal se referă la o persoană fizică sau juridică, alta decât deţinătoarea sistemului informatic. În această ipostază se găseşte persoana inclusă în sistemul informatic accesat ilegal, care poate suferi consecinţe de ordin moral, financiar, administrativ, juridic ori de altă natură". Sub aspectul laturii obiective a infracţiunilor prevăzute la art.360 din Codul penal al României, T.Medeanu şi 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. 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 a reglementărilor din instituţia respectivă, pe linia protejării informaţiilor". În acelaşi context, autorii scot în evidenţă un aspect de maximă relevanţă ce ţine de latura obiectivă a infracţiunilor prevăzute la art.360 din Codul penal al României: „Cerinţa esenţială pentru existenţa infracţiunii constă în realizarea accesului „fără drept". În sensul legii penale, acţionează fără drept persoana care se află în una dintre următoarele situaţii: nu este autorizată, în temeiul legii sau al unui contract; depăşeşte limitele autorizării; 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 desfăşura cercetări ştiinţifice sau de a efectua orice altă operaţiune într-un sistem informatic". În sfârşit, nu poate fi trecută cu vederea opinia expusă de T.Medeanu şi A.Crăciunescu cu privire la latura subiectivă a infracţiunilor respective: „Infracţiunea de bază poate fi săvârşită cu intenţie directă sau indirectă. 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. Cerinţa esenţială referitoare la scop constă în obţinerea de date informatice. Pentru consumarea acesteia nu este necesar să se realizeze, prin acţiunea ilicită a făptuitorului, obţinerea de date informatice. 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".

Teza de doctor habilitat în drept, susţinută în 2016 de către *V.G. Stepanov-Eghianț* [14], este o altă publicaţie consacrată analizei accesului ilegal la informaţia computerizată.

Acest autor a întreprins, printre altele, analiza infracţiunilor prevăzute la art.272 din Codul penal al Federaţiei Ruse. În viziunea lui V.G. Stepanov-Eghianț, obiectul juridic generic al acestor infracţiuni îl formează „relaţiile sociale care reglementează crearea, păstrarea, utilizarea sau transmiterea în siguranţă a informaţiei computerizate". Dânsul consideră că obiectul juridic special al infracţiunilor prevăzute la art.272 din Codul penal al Federaţiei Ruse îl constituie „relaţiile sociale care asigură dreptul proprietarului informaţiei computerizate la crearea, păstrarea, utilizarea şi transmiterea acesteia în condiţii de siguranţă". În calitate de obiect imaterial al infracţiunilor respective V.G. Stepanov-Eghianț vede „nu oricare informaţie în formă computerizată, ci doar aceea care este protejată de lege". În viziunea lui, „accesul ilegal se poate face în două moduri: fie prin sustragerea suportului în sine al informaţiei computerizate (de exemplu, sustragerea unui disc, a unei uniăţi flash etc.), urmată de accesarea informaţiei computerizate stocate pe acesta, fie prin interceptarea informaţiei computerizate pe calea folosirii mijloacelor tehnice computerizate. Majoritatea infracţiunilor sunt comise în al doilea mod". După V.G. Stepanov-Eghianț, „infracţiunile prevăzute la art.272 din Codul penal al Federaţiei Ruse trebuie să rămână infracţiuni materiale, adică să implice producerea uneia dintre urmările prejudiciabile specificate în dispoziţia acestui articol". Cu privire la subiectul infracţiunilor examinate, doctrinarul susţine:

„Analiza dispoziției art.272 din Codul penal al Federației Ruse ne permite să constatăm existența următoarelor categorii de subiecți ai accesului ilegal la informația computerizată: subiectul general și subiectul special. În conformitate cu alin.1 art.272 din Codul penal al Federației Ruse, 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. În ipoteza prevăzută la alin.2 art.272 din Codul penal al Federației Ruse, ne referim la un subiect special al infracțiunii, care comite accesul ilegal la informația computerizată folosind situația sa de serviciu". Referitor la latura subiectivă a infracțiunilor pertractate, V.G. Stepanov-Eghianț afirmă că „accesul ilegal la informația computerizată este săvârșit de făptuitor cu intenție directă sau indirectă", precizând că intenția este manifestată în raport cu producerea urmărilor prejudiciabile enumerate în art.272 din Codul penal al Federației Ruse.

În 2016 vede lumina tiparului un articol științific al cărui autor este *V.Stati* [15].

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 legea penală a Republicii Moldova, a României și de cea a 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 a Ucrainei la Convenţia Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta la 23.11.2001[7] [16]. În codurile penale ale acestor trei state sunt prezente articole în care se stabilește răspunderea pentru accesul ilegal la informația computerizată. În opinia lui V.Stati, „scopul normelor din Capitolul XI al părții speciale a Codului penal al Republicii Moldova este de a apăra ordinea de drept atât împotriva infracțiunilor informatice, cât și împotriva infracțiunilor în domeniul telecomunicațiilor. În mod similar, reieșind din normele Titlului XVI din partea specială a 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. În același timp, 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. Domeniul de utilizare a rețelelor de telecomunicații nu este reprezentat de obiectul generic al acestor infracțiuni". 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 ori să desfăşoare cercetări ştiinţifice sau să efectueze orice altă operaţiune într-un sistem informatic, însă care nu are dreptul de acces la informația computerizată, depășește limitele autorizării ori nu are permisiunea persoanei competente. Pentru comparație, judecând după dispozițiile art.360 din Codul penal al României și ale alin.1 art.361 din Codul penal al Ucrainei, subiectul infracțiunilor corespunzătoare nu este unul special". Cât privește scopul infracțiunilor de acces ilegal la informația computerizată, același autor relevă: „Conform art.360 din Codul penal al României, scopul obținerii de date informatice este special și, în același timp, agravează răspunderea. [...] În art.259 CP RM și în alin.1 art.361 din Codul penal al Ucrainei nu este specificat un asemenea scop". În fine, nu poate fi ignorată comparația cu privire 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. Pentru comparație, atât persoana fizică, cât și persoana juridică pot fi subiecți ai infracțiunilor specificate în Capitolul VI din Titlul VII al părții speciale a Codului penal al României. În același timp, legiuitorul moldovean are o abordare selectivă privind chestiunea în cauză: atât persoana fizică, cât și persoana juridică pot fi subiecți ai infracțiunilor prevăzute de art.259, 260, 260^1, 260^3, 260^4 și 261 CP RM. Totodată, doar persoana fizică poate fi subiectul infracțiunilor specificate la art.260^2, 260^5 și 260^6 CP RM".

În 2017 a fost susținută teza de doctor în drept de către *I.R. Beghișev* [17].

În ea autorul 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

[7] 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 intentionată 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".

art.272 „Accesul ilegal la informația computerizată" din Codul penal al Federației Ruse și starea actuală a dezvoltării științei și tehnologiei". Dezvoltând ideea, I.R. Beghișev explică de ce consideră anacronică terminologia art.272 din Codul penal al Federației Ruse: „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, inclusiv în sistemele de radiocomunicații și de radiodifuziune, în sistemele de radiorelee și de comunicații prin satelit, în sistemele de comunicații mobile și în sistemele de distribuție fără fir. În opinia noastră, în afară de obiectele în care se află și circulă informația deja menționate în art.272 din Codul penal al Federației Ruse, în acest articol trebuie specificate alte tipuri ale acestora, și anume – dispozitivele de informații și telecomunicații, sistemele și rețelele acestora". Din perspectiva perfecționării dispozițiilor referitoare la accesul ilegal la informația computerizată, comportă interes următoarea aserțiune a lui I.R. Beghișev: „În art.272 din Codul penal al Federației Ruse, până în decembrie 2011, ca obiect de localizare a informației computerizate era specificat suportul material de astfel de informații. 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. Atunci când legiuitorul rus a utilizat sintagma „suport material de informații computerizate" el a avut în vedere, cel mai probabil, elementul de stocare a informațiilor computerizate care face parte dintr-un computer. Însă, sistemele de telecomunicații nu sunt mașini de felul lor. Actualmente, în afară de computere, suporturi de informații computerizate pot fi diverse unități flash, hard disk-uri amovibile, CD-uri etc. 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 din Codul penal al Federației Ruse". Cu această ocazie, consemnăm că o sintagmă asemănătoare este folosită în art.259 CP RM.

În 2018 a ieșit de sub tipar lucrarea elaborată de către *A.N. Popov* [18].

În cadrul acestei lucrări distingem analiza infracțiunilor de acces ilegal la informația computerizată. În opinia autorului, obiectul juridic generic al infracțiunilor prevăzute la art.272 din Codul penal al Federației Ruse îl formează „securitatea informațională ca parte a securității publice". Referitor la obiectul 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 „Infracțiuni în sfera informației computerizate" din Partea specială a Codului penal al Federației Ruse: „relațiile sociale în sfera informațională, care asigură starea de protecție a persoanei, societății și statului împotriva amenințărilor informaționale". Lipsită de concretețe este și părerea autorului cu privire la obiectul material sau imaterial al infracțiunilor prevăzute la art.272 din Codul penal al Federației Ruse: „În sens larg, tot ceea ce formează infrastructura informațională poate fi considerat obiect material sau imaterial al infracțiunilor în sfera informației computerizate". Caracterizând latura obiectivă a infracțiunilor de acces ilegal la informația computerizată, A.N. Popov afirmă: „Latura obiectivă a infracțiunilor prevăzute de art.272 din Codul penal al Federației Ruse include trei semne obligatorii: 1) accesul ilegal la informația computerizată protejată de lege; 2) urmările prejudiciabile sub forma distrugerii, blocării, modificării sau copierii informației în cauză; 3) legătura de cauzalitate dintre accesul ilegal la informația computerizată protejată de lege și urmările prejudiciabile prevăzute de lege. Accesul la informația computerizată presupune aflarea conținutului acesteia și utilizarea acesteia, în special copierea, blocarea, modificarea sau distrugerea informației computerizate, săvârșită prin recurgerea la software și hardware". 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. Însă, aceasta nu înseamnă că infracțiunile prevăzute la art.272 din Codul penal al Federației Ruse pot fi săvârșite exclusiv intenționat. Or, legea stabilește răspunderea penală nu pentru accesul ilegal în sine, ci pentru acțiunea care urmează accesului ilegal. Prin urmare, forma vinovăției trebuie stabilită în raport cu urmările prejudiciabile sub forma distrugerii, blocării, modificării sau copierii informației computerizate. În art.272 din Codul penal al Federației Ruse nu se menționează că infracțiunile corespunzătoare pot fi săvârșite doar din imprudență. Astfel, având în vedere dispoziția de la alin.2 art.24 din Codul penal al Federației Ruse[8], se poate concluziona că infracțiunile prevăzute la art.272 din Codul penal al Federației Ruse pot fi săvârșite cu intenție sau din imprudență. De exemplu, dacă făptuitorul a săvârșit cu intenție accesul ilegal la informația

[8] Conform acestei dispoziții, „fapta 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".

computerizată protejată de lege, iar această faptă a cauzat din imprudență modificarea informației în cauză, constatăm temeiul aplicării art.272 din Codul penal al Federației Ruse". În ceea ce privește subiectul infracțiunilor de acces ilegal la informația computerizată, A.N. Popov opinează: „Subiectul infracțiunii este general. Se are în vedere orice persoană fizică responsabilă care a atins vârsta de 16 ani și care a săvârșit accesul ilegal la informația computerizată protejată de lege, ceea ce a cauzat urmările prejudiciabile prevăzute de lege".

Din 2019 datează studiul monografic elaborat de către *T.I. Sozanski, S.Ia. Burda* și *A.Ia. Skiba* [19].

Acești autori examinează, printre altele, infracțiunile prevăzute la art.361 din Codul penal al Ucrainei. 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". Nu este clar dacă teoreticienii respectivi se referă la obiectul juridic generic sau la obiectul juridic special al infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei. 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", „rețea de computere", „rețea de telecomunicații" etc. Latura obiectivă a infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei este descrisă astfel de cei trei autori: „Latura obiectivă se exprimă în modificarea regimului de funcționare a computerului, a sitemului de computere sau a rețelei de computere, pe calea influențării asupra suportului de informație computerizată sau a mijlocului de prelucrare automată a acesteia". Analizând același element constitutiv al infracțiunilor în cauză, T.I. Sozanski, S.Ia. Burda și A.Ia. Skiba formulează definiția noțiunii care desemnează fapta prejudiciabilă din cadrul infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei: „Accesul ilegal la computer, la sistemul de computere sau la rețeaua de computere constă în modificarea regimului de funcționare a acestora, pe calea influențării asupra suportului de informație computerizată sau a mijlocului de prelucrare automată a acesteia, săvârșită cu încălcarea regimului de acces la informația computerizată, stabilit de legislație, ceea ce aduce atingere relațiilor socilae de proprietate asupra informației computerizate". În continuare, sunt definite toate noțiunile care desemnează urmările prejudiciabile prevăzute la art.361 din Codul penal al Ucrainei. Analiza se încheie cu examinarea caracteristicilor subiectului și ale laturii subiective a infracțiunilor prevăzute de acest articol.

Din același an 2019 datează articolul științific elaborat de către *A.T. Drăgan* [20].

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 infracțiunilor prevăzute de art.360 din Codul penal al României; structurii și conținutului juridic al infracțiunilor respective; pedepselor pentru infracțiunile prevăzute de art.360 din Codul penal al României; aspectelor procedurale legate de aceste infracțiuni etc. Comportă originalitate punctul de vedere exprimat de doctrinar cu privire la obiectul juridic al infracțiunilor prevăzute la art.360 din Codul penal al României: „Obiectul juridic este valoarea socială numită „sistem informatic" și relațiile sociale care apar în legătură cu utilizarea sistemelor automate de prelucrare a datelor". 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 la art.360 din Codul penal al României, este enunțată 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 (computere, rețele de computere, hardware – echipamente periferice, cabluri, carduri, servere etc., și software – programe, aplicații, baze de date etc.), precum și datele computerizate către care este îndreptată atenția făptuitorului". În ceea ce privește subiecții infracțiunilor prevăzute la art.360 din Codul penal al României, A.T. Drăgan relevă: „Subiect activ poate fi orice persoană (persoană fizică sau juridică) care are discernământ penal. Nicio calitate specială nu este cerută de lege în acest scop. Cu toate acestea, făptuitorul este, de obicei, o persoană care are cunoștințe tehnice în domeniul computerelor, este oarecum familiarizat cu sistemele de securitate ale computerelor și cu vulnerabilitățile acestor sisteme sau este o persoană angajată de entitățile care au sisteme informatice"; „Subiect pasiv al infracțiunii este persoana fizică sau juridică care deține sisteme informatice și al cărei drept la integritate, confidențialitate și disponibilitate a sistemelor informatice sau a datelor computerizate a fost încălcat sau pus în pericol. Prin extensie, poate exista un subiect pasiv colectiv, format dintr-un număr mare de persoane fizice sau juridice, atunci când accesul la sistemul informatic generează automat acces ilegal la alte sisteme similare interconec-

tate cu primul". Nu putem face abstracție de reflecțiile lui A.T. Drăgan cu privire la elementul material al infracțiunilor prevăzute la art.360 din Codul penal al României: „Accesul ilegal la un sistem informatic are loc adesea prin utilizarea tehnicilor de inginerie socială. De exemplu, făptuitorul poate studia site-ul web al companiei și documentele publice pentru a obține numele managerilor și apoi apela telefonic compania respectivă, pretinzând că este noul tehnician IT. 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"; „În ceea ce privește cerința esențială, legiuitorul prevede necesitatea accesului fără drept (ilegal). 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; b) depășește limitele autorizației; c) nu are permisiunea persoanei fizice sau juridice care are competența de a o acorda". Studiul lui A.T. Drăgan se încheie cu examinarea laturii subiective a infracțiunilor prevăzute la art.360 din Codul penal al României: „Fapta poate fi comisă cu intenție directă sau indirectă. În cazul variantei agravate prevăzute la alin.(2), forma vinovăției este intenția directă, calificată de scop. Textul incriminator prevede cerința unui scop numai în cazul alin.(2): cel de obținere a datelor informatice".

Din 2019 datează și articolul științific al cărui autor este *V.Stati* [21].

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" [22]. La rândul său, R.Abrihan opinează: „Minarea profitabilă de monede necesită o cantitate imensă de putere de calcul, de aceea atacatorii instalează programe malware pe computerele utilizatorilor pentru a „sustrage" puterea de calcul necesară" [23]. În circumstanțele descrise de cei doi autori precitați este aplicabil art.260^6 CP RM, care prevede răspunderea, printre altele, pentru introducerea datelor informatice în scopul de a obține un beneficiu material pentru sine sau pentru altul, dacă aceste acțiuni au cauzat daune în proporţii mari. În afară de aceasta, este aplicabilă prevederea de la lit.f) alin.(2) art.259 CP RM, care stabilește răspunderea pentru accesul ilegal la informaţia computerizată, săvârşit cu utilizarea ilegală a calculatorului, a sistemului sau a reţelei informatice, în scopul săvârşirii, *inter alia*, a uneia dintre infracţiunile prevăzute la art.260^6 CP RM". 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. Astfel de activități dobândesc conotații penale în prezența unor condiții suplimentare, 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)".

Încheiem examinarea materialelor științifice referitoare la accesul ilegal la informaţia computerizată, publicate peste hotare, cu analiza tezei de doctor în drept susținute în 2019 de către *D.O. Ricika* [24].

După părerea acestui autor, obiectul juridic generic al infracțiunilor prevăzute în Titlul XVI al Părții speciale a Codului penal al Ucrainei îl formează „relațiile sociale care suferă atingere datorită influenței asupra informației care circulă în sistemele informatice". Atunci când caracterizează obiectul juridic special al infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei, D.O. Ricika remarcă pluralitatea valorilor sociale specifice și a relațiilor sociale aferente, apărate împotriva acestor infracțiuni: „Obiectul [...] îl formează funcționarea normală a computerelor, a sistemelor automatizate, a rețelelor de computere și a rețelelor de telecomunicații. Sensul normei constă în aceea că ea asigură ocrotirea relațiilor sociale de două tipuri: a relațiilor sociale de proprietate asupra informației computerizate și a relațiilor sociale cu privire la prestarea serviciilor de telecomunicații. Proprietatea asupra informației computerizate constituie ansamblul drepturilor persoanei de a: poseda suportul de informație computerizată; folosi informația stocată pe acest suport, în vederea satisfacerii necesităților informaționale; permite altora să utilizeze informația de pe suportul în cauză, să o modifice, să decidă cine va fi posesorul respectivului suport de informație computerizată". În ceea ce privește obiectul material sau imaterial al infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei, același doctrinar opinează: „La obiectul material sau imaterial al infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei se raportează informația computerizată și informația transmisă prin canalele de telecomunicații. Dacă analizăm esența prevederilor acestui articol, atunci am putea conchide că obiectul material sau imaterial îl reprezintă: 1) computerele; 2) sistemele automatizate; 3) rețelele de computere; 4) rețelele de telecomunicații. În realitate,

nu este așa. Or, rolul-cheie îl joacă tocmai informația care se află în entitățile sus-menționate". În rezultatul analizei laturii obiective a infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei, D.O. Ricika afirmă că „accesul ilegal la informația computerizată se comite pe calea acțiunii. Latura obiectivă îmbracă două forme alternative: 1) accesul ilegal la computere, la sisteme automatizate sau la rețele de computere; 2) accesul ilegal la rețelele de telecomunicații". Referitor la latura subiectivă a infracțiunilor pertractate, doctrinarul susține că acestea pot fi săvârșite doar cu intenție directă sau indirectă. Analiza infracțiunilor prevăzute la art.361 din Codul penal al Ucrainei se încheie cu examinarea caracteristicilor subiectului acestor infracțiuni.

Concluzii

În acest articol au fost examinate ideile și concepțiile unor penaliști care au publicat peste hotare lucrări dedicate infracțiunilor de acces ilegal la informația computerizată: V.Stati (Republica Moldova); A.Crăciunescu, M.Dobrinoiu, A.T. Drăgan, C.Duvac, G.Florescu, V.Florescu, L.C. Kövesi, C.Manea, T.Medeanu, G.Zlati (România); D.S. Azarov, S.Ia. Burda, D.O. Ricika, N.A. Rozenfeld, A.Ia. Skiba, T.I. Sozanski (Ucraina); I.R. Beghișev, A.M. Doronin, A.N. Popov, V.G. Stepanov-Eghianț (Federația Rusă). Obiectul de cercetare al acestor autori îl constituie infracțiunile prevăzute la: art.259 din Codul penal al Republicii Moldova; art.42 al Legii României nr.161 din 19.04.2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei; art.360 din Codul penal al României; art.361 din Codul penal al Ucrainei; art.272 din Codul penal al Federației Ruse. Ideile și concepțiile acestor oameni de știință urmează a fi puse la temelia concepţiei teoretice de soluționare a problemei privind răspunderea pentru infracțiunile prevăzute la art.259 din Codul penal al Republicii Moldova.

Referințe:

1. ДОРОНИН, А.М. *Уголовная ответственность за неправомерный доступ к компьютерной информации:* Автореферат диссертации на соискание ученой степени кандидата юридических наук. Москва, 2003. 24 с.
2. РОЗЕНФЕЛЬД, Н.А. *Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж:* Дисертація на здобуття наукового ступеня кандидата юридичних наук. Київ, 2003. 222 с.
3. DOBRINOIU, M. *Infracţiuni în domeniul informatic*. Bucureşti: C.H. Beck, 2006. 401 p. ISBN 978-973-655-941-9
4. Legea României privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor 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.
5. АЗАРОВ, Д.С. *Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження)*. Київ: Атіка, 2007. 304 с. ISBN 966-326-230-3
6. MANEA, C. Accesul ilegal la un sistem informatic. În: *Revista Pro Lege*, 2009, nr.1, p.40-48. ISSN 1224-2411
7. KÖVESI, L.C. *Combaterea crimei organizate prin dispoziţii de drept penal* / Teză de doctorat. Timișoara, 2011. 479 p.
8. FLORESCU, V, FLORESCU, G. 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, p.21-38. ISSN 1841-4303
9. ZLATI, G. Unele aspecte în legătură cu infracțiunile informatice din perspectiva legislației în vigoare, precum și a noului Cod penal. În: *Dreptul*, 2012, nr.10, p.204-229. ISSN 1018-0435
10. Legea României privind comerțul electronic, nr.365 din 07.06.2002. În: *Monitorul Oficial al României*, 2002, nr.483.
11. *Decizia Secției Penale a Înaltei Curți de Justiție și Casație a României nr.371 din 02.02.2010*. [Accesat: 12.09.2020] Disponibil: https://www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=54367
12. DUVAC, C. Accesul ilegal la un sistem informatic în reglementarea noului Cod penal. În: *Revista română de dreptul proprietăţii intelectuale*, 2012, nr.1, p.88-109. ISSN 1584-7241
13. MEDEANU, T., CRĂCIUNESCU, A. 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, p.28-37. ISBN 978-606-591-723-1
14. СТЕПАНОВ-ЕГИЯНЦ, В.Г. *Методологическое и законодательное обеспечение безопасности компьютерной информации в Российской Федерации (уголовно-правовой аспект):* Диссертация на соискание ученой степени доктора юридических наук. Москва, 2016. 389 с.
15. СТАТИ, В. Компьютерные преступления в уголовном законодательстве Республики Молдова, Румынии и Украины: сравнительно-правовой анализ. В: *Kieler Ostrechts-Notizen*, 2016, no.2; 2017, no.1, p.54-59. ISSN 1862-1589
16. *Convention on Cybercrime*. [Accesat: 12.09.2020] Disponibil: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

17. БЕГИШЕВ, И.Р. *Понятие и виды преступлений в сфере обращения цифровой информации:* Диссертация на соискание ученой степени кандидата юридических наук. Казань, 2017. 204 с.
18. ПОПОВ, А.Н. *Преступления в сфере компьютерной информации*. Санкт-Петербург: Санкт-Петербургский юридический институт (филиал) Университета прокуратуры Российской Федерации, 2018. 68 с.
19. 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.
20. DRĂGAN, A.T. Illegal access to a computer system from the standpoint of the current Criminal Code. In: *Journal of Legal Studies "Vasile Goldiş"*, 2019, no.23, p.33-43. ISSN 1582-5442
21. STATI, V. 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
22. ПЕРОВ, В.А. Уголовно-правовые аспекты «недобросовестного» майнинга криптовалют. В: *Безопасность бизнеса*, 2018, №2, с.25-29. ISSN 2072-3644
23. ABRIHAN, R. *Tendinţe în securitate IT: România, peste medie la minare ilicită de criptomonede, atacuri phishing şi ransomware*. [Accesat: 05.09.2020] Disponibil: https://www.startupcafe.ro/smart-tech/tendinte-securitate-it-atac-minare-ilegalacriptomonede-microsoft.htm
24. 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:* Дисертація на здобуття наукового ступеня кандидата юридичних наук. Ірпінь, 2019. 212 с.

Date despre autor:
Alexandru STRÎMBEANU, doctorand, Şcoala doctorală *Ştiinţe Juridice*, Universitatea de Stat din Moldova.
E-mail: avocatstrimbeanu@yahoo.ro

Prezentat la 15.09.2020