CZU: 343.72:004.056
https://doi.org/10.52277/1857-2405.2022.3(62).02

NOŢIUNEA DE ACCES LA INFORMAŢIA COMPUTERIZATĂ ÎN ACCEPŢIUNEA ART. 259 DIN CODUL PENAL AL REPUBLICII MOLDOVA

Alexandru STRÎMBEANU,
doctorand,
Universitatea de Stat din Moldova
https://orcid.org/0000-0002-7746-6541

SUMAR

Noţiunea „acces la informaţia computerizată” se referă la una dintre componentele laturii obiective a infracţiunilor prevăzute la art. 259 din Codul penal al Republicii Moldova. Principalul rezultat al prezentului studiu îl reprezintă definirea acestei noţiuni, care generează controverse în teoria şi practica dreptului penal. Un alt rezultat notabil constă în susţinerea cu argumente a soluţiei de calificare a faptelor de: 1) menţinere a accesului ilegal la informaţia computerizată după retragerea ori expirarea autorizării; 2) intruziune ilegală în calculatorul, în suportul material de informaţie, în sistemul informatic sau în reţeaua informatică în care sau pe care se află informaţia computerizată, dacă, din cauze independente de voinţa făptuitorului, nu este săvârşit accesul ilegal la acea informaţie.

Cuvinte-cheie: *acces, intruziune, menţinerea accesului, informaţie computerizată, sistem informatic, calculator, suport material de informaţie, reţea informatică.*

The concept of access to computerized information according to art. 259 of the Criminal Code of the Republic of Moldova

SUMMARY

The concept of „access to computerized information” refers to one of the components of the objective side of the offenses provided in art. 259 of the Criminal Code of the Republic of Moldova. The main result of the present study is the definition of this concept that generates controversies in the theory and practice of criminal law. Another notable result consists in supporting with arguments the solution to qualify the acts of: 1) maintaining illegal access to computerized information after the withdrawal or expiration of the authorization; 2) illegal intrusion into the computer, the data storage device, the computer system or the computer network, in which or on which the computerized information is located, if, due to reasons independent of the perpetrator's will, the illegal access to that information is not committed.

Key-words: *access, intrusion, maintaining access, computerized information, computer system, computer, data storage device, computer network.*

Din art. 15 și 52 CP RM rezultă că latura obiectivă reprezintă unul dintre elementele constitutive ale infracţiunii. Indiferent dacă infracţiunea este formală sau materială, latura ei obiectivă include ca semn constitutiv fapta prejudiciabilă (elementul material). Acest semn se referă la manifestarea exterioară a infracţiunii, la comportamentul făptuitorului, care se concretizează în acţiune sau inacţiune.

După cum deducem din denumirea art. 259 CP RM și din dispoziţia de la alin. (1) art. 259 CP RM, fapta prejudiciabilă, prevăzută de acest articol, cuprinde acţiunea de acces ilegal la informaţia computerizată. Precizăm că această acţiune este doar una dintre componentele faptei prejudiciabile prevăzute la art. 259 CP RM. Cealaltă componentă a faptei în cauză va fi examinată în cadrul unui alt studiu.

În Raportul explicativ la Convenţia Consiliului Europei privind criminalitatea informatică [28] (în continuare – Convenţia de la Budapesta), în pct. 46 este definită noţiunea de accesare, utilizată în art. 2 „Accesarea ilegală” din Convenţia respectivă: „Noţiunea „accesare” presupune pătrunderea în întregime într-un sistem informatic sau în oricare parte a acestuia (*hardware*, componente, date stocate ale sistemului instalat, directoare, date de

trafic și date legate de conținut) [...]. 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, cum ar fi LAN (rețea locală) sau Intranet în cadrul unei organizații. Nu este relevantă metoda de conectare (de exemplu, de la distanță, inclusiv prin legături fără fir sau la o distanță apropiată)" [29]. 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. 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, prin intermediul unor programe specializate ori prin intermediul unei rețele, în scopul de a identifica probe" [3]. 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 informația computerizată" utilizată în art. 259 CP RM. Or, obiectul accesului ilegal în accepțiunea acestui articol este informația 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 că „acces" înseamnă uzitarea de resursele unui sistem informatic, adică darea de instrucțiuni unui sistem informatic, comunicarea cu/printr-un sistem informatic, stocarea informației sau regăsirea acesteia într-un sistem informatic. Accesul include intrarea într-un alt sistem informatic, conectat prin rețele de telecomunicații publice sau într-un alt sistem informatic din aceeași rețea informatică, indiferent de metoda de comunicare. Metoda de comunicare – la distanță, inclusiv grație legăturii prin satelit sau nu, ori de aproape – nu prezintă relevanță la calificare" [2, p. 351]. La rândul lor, L. Dumneanu și D. Gurev afirmă: „Prin acces se înțelege folosirea de componentele unui sistem informatic, cum ar fi accesarea elementelor unui sistem informatic, comunicarea cu/printr-un sistem informatic, depozitarea informației sau regăsirea acesteia într-un sistem informatic. Accesul presupune penetrarea unui alt sistem informatic, conectat prin rețele de telecomunicații publice sau într-un alt sistem informatic din aceeași rețea, indiferent prin ce metodă de comunicare" [13, p. 93].

Într-o măsură mai pronunțată, exigențelor dispoziției art. 259 CP RM îi corespunde definiția formulată 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 [...]" [18].

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 informație, într-un sistem informatic sau într-o rețea informatică. Este clar că, pentru a accesa informația computerizată, este necesar mai întâi să fie accesat calculatorul, suportul material de informație, sistemul informatic sau rețeaua 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 informație, în sistemul informatic sau în rețeaua informatică, în care sau pe care se află respectiva informație. *(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 informație, în sistemul informatic sau în rețeaua informatică, în care sau pe care se află informația computerizată, dacă, din cauze independente 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).* 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 aparţine victimei, după care intră în posesia acelui bun, pentru a-l putea folosi și/sau a dispune de el.

Ţinând cont de acest aspect și de înţelesul noţiunii de informaţie computerizată, precum și având ca puncte de reper definiţiile propuse de către C. Moţoc, L. Gîrla, S. Brînza, V. Stati, L. Dumneanu și D. Gurev, considerăm că prin „acces la informaţia computerizată" în accepţiunea art. 259 CP RM trebuie de înţeles: obţinerea posibilităţii de a recurge la informaţia computerizată, în vederea beneficierii de calităţile utile ale acesteia.

Astfel, accesul la informaţia computerizată implică intrarea în posesia informaţiei computerizate care aparţine victimei, însă nu neapărat folosirea și/sau dispunerea de această informaţie. Accesul la informaţia computerizată doar deschide calea pentru o eventuală folosire și/sau dispunere de respectiva informaţie. De fapt, folosirea și/sau dispunerea de informaţia computerizată se referă la următoarea etapă de executare a laturii obiective a infracţiunilor prevăzute de art. 259 CP RM. Este corect să afirmăm că folosirea și/sau dispunerea de informaţia computerizată reprezintă scopul acţiunii de acces la informaţia computerizată, scop care depășește cadrul acestei acţiuni.

În alt context, în art. 2 al Convenţiei de la Budapesta se vorbește despre „accesarea [...] ansamblului ori a unui sistem informatic" [28]. În art. 3, „Accesarea ilegală a sistemelor informatice" din 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, este menţionată „accesarea [...] unui sistem informatic sau a unei părţi a acestuia" [12]. Făcând analogie cu art. 259 CP RM, observăm că legiuitorul trece cu tăcerea acest detaliu, ceea ce înseamnă că, în cazul infracţiunilor prevăzute de acest articol, accesul la informaţia computerizată este fie integral, fie parţial. Amploarea accesării informaţiei computerizate nu influenţează asupra calificării faptei în baza art. 259 CP RM, dar poate fi luată în considerare la individualizarea pedepsei.

Mai important este însă să stabilim nu atât amploarea accesării informaţiei computerizate, în sensul art. 259 CP RM, cât mai ales caracterul accesării acesteia.

În context, atrage atenţia următoarea opinie a lui G.S.O. Kurbanov, care vizează infracţiunile prevăzute de un articol din Codul penal al Republicii Azerbaidjan, care corespunde art. 259 CP RM: „Accesul ilegal este un concept complex care include următoarele acte: intruziunea „fizică", care oferă posibilitatea de a prelua informaţii dintr-un calculator; operarea neautorizată cu informaţiile dintr-un calculator" [30]. În aceeași ordine de idei se înscriu punctele de vedere exprimate de către unii autori români. De exemplu, Gh.Iu. Ioniţă 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 interacţiunea cu *hardware*-ul (partea fizică) sistemului informatic (componentele); 2) la nivel logic, accesul presupune interacţiunea cu *software*-ul (partea logică) sistemului informatic (programe/aplicaţii). 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, pentru că interacţionăm cu *hardware*-ul (componentele fizice) acelui sistem informatic (fantă de acces pentru card, tastatură, ecran), cât și la nivel logic, pentru că interacţionăm cu *software*-ul (partea logică) sistemului informatic (programele/aplicaţiile/sistemul de operare)" [15]. De asemenea, R.A. Nestor susţine: „În forma sa cea mai simplă, accesul 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" [19].

Aceste păreri se deosebesc de cele exprimate de alţi autori români. Astfel, I. Kuglay relevă: „Accesarea sistemului constituie, în principiu, acea operaţiune prin care se realizează o interacţiune funcţională cu sistemul informatic. O primă delimitare pe care practica neunitară a reclamat-o a fost între interacţiunea de ordin material, fizic şi cea de ordin logic; numai aceasta din urmă are semnificaţia accesării sistemului informatic, respectiv numai cea care conferă făptuitorului posibilitatea „de a da comenzi, de a cauza introducerea, obţinerea, afișarea, stocarea ori diseminarea de date informatice sau folosirea în orice alt mod a resurselor unui calculator, sistem ori reţea informatică sau comunicarea cu unităţile sale aritmetice, logice ori de memorie" [24, 1, p. 778-779]. De asemenea, G. Zlati menţionează: „Accesul trebuie să fie unul propriu-zis, înţelegând prin aceasta posibilitatea ca agentul, prin interacţiunea logică pe care o are cu sistemul informatic, să poată beneficia (ori să existe cel puţin potenţial această posibilitate) de funcţiile ori resursele sistemului informatic. Această abordare ar fi, din punctul nostru de vedere, suficient de restrictivă pentru a nu extinde câmpul de aplicabilitate a normei de incriminare

dincolo de ceea ce s-a dorit, şi suficient de abstractă încât să poată suferi anumite interpretări evolutive" [25].

Susţinem opinia lui I. Kuglay şi G. Zlati. Interacţiunea făptuitorului cu partea fizică (materială) a unui sistem informatic doar precede accesarea acestuia, dar fără a se identifica cu accesul la sistemul informatic. Cu atât mai mult, interacţiunea făptuitorului cu partea fizică (materială) a unui sistem informatic nu poate fi confundată cu accesul la informaţia computerizată. Or, informaţia computerizată are, prin excelenţă, o natură imaterială, incorporală. Așa cum am menţionat 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 informaţie, trebuie deosebită de accesul la informaţia computerizată. Or, accesul la informaţia computerizată este precedat de o astfel de intruziune, fără însă a o include. În concluzie, în cazul infracţiunilor prevăzute la art. 259 CP RM, accesul la informaţia computerizată presupune o interacţiune logică, nu fizică, cu o astfel de informaţie. Interacţiunea logică cu informaţia computerizată se exprimă în aceea că făptuitorul foloseşte un program informatic sau mai multe programe informatice care asigură prelucrarea acelei informaţii.

În acest context, precizăm că accesul ilegal la informaţia computerizată (în sensul 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, interacţiunea 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. 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 infracţiuni, se poate apela, cu ajustările de rigoare, la următoarea explicaţie din jurisprudenţa română, dată de Înalta Curte de Casaţie și Justiţie a României: „Infracţiunea prevăzută de art. 361 C. pen. (se are în vedere infracţiunea de interceptare ilegală a unei transmisii de date informatice – *n.a.*) se diferenţiază de infracţiunea de acces, fără drept, la un sistem informatic, prin faptul că acţiunea de interceptare se realizează în procesul de transmitere a acestor date de la un sistem informatic la altul. Ambele infracţiuni sunt săvârșite cu scopul de a obţine ilegal date informatice (de regulă, folosite ulterior pentru comiterea infracţiunii contra patrimoniului), interceptarea comportând, însă, un caracter dinamic, în timp ce accesul ilegal la un sistem informatic are un caracter static" [17]. Într-adevăr, infracţiunea 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 infracţiunilor prevăzute la art. 259 CP RM, se accesează ilegal informaţia computerizată din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică, nu informaţia computerizată transmisă între calculatoare, între suporţii materiali de informaţie, între sisteme informatice sau între reţele informatice.

După această divagaţie, este necesar de menţionat că exemplele de acces ilegal la un sistem informatic ne ajută să percepem înţelesul noţiunii „accesul la informaţia computerizată". Așa cum am specificat *supra*, accesul la informaţia computerizată poate fi precedat de accesul la sistemul informatic în care se află respectiva informaţie. Totodată, nu trebuie să uităm că, în cazul infracţiunilor prevăzute de art. 259 CP RM, accesul la informaţia computerizată poate fi precedat de accesul nu doar la sistemul informatic în care se află respectiva informaţie, ci și la calculatorul, la suportul material de informaţie ori la reţeaua informatică în care sau pe care se află informaţia computerizată.

În Decizia Înaltei Curţi 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 reţinut 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 [11]. De exemplu, într-o speţă din practica judiciară română, art. 360 „Accesul ilegal la un sistem informatic" din Codul penal al României [7] a fost aplicat, deoarece „inculpata M.M. a introdus cardul [autentic, pierdut de către victimă] în bancomat de două ori şi a retras de fiecare dată câte 400 lei, fără a avea consimţământul persoanei vătămate" [22].

În speţa următoare s-a omis nejustificat aplicarea art. 259 CP RM: F.S. a fost condamnat în baza alin. (1) art. 237 şi 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, cu ajutorul unui program informatic, coduri de acces la un sistem informatic, pentru obţinerea informaţiei de pe banda magnetică a unor carduri bancare. Ulterior, după modificarea informaţiei de pe banda

magnetică a acelor carduri bancare, făptuitorii au efectuat plăţi în mărime totală de 118.512,62 lei prin intermediul terminalelor care aparţineau unor bănci comerciale din R. Moldova [20, 9]. Printre scopurile infracţiunii prevăzută la art. 260[4] CP RM se numără cel de săvârşire a uneia dintre infracţiunile prevăzute la art. 259 CP RM. În ultima speţă analizată acest scop a fost prezent și, mai mult, a fost realizat. Or, după cum rezultă din speţă, făptuitorii au efectuat plăţi prin intermediul terminalelor care aparţineau unor bănci comerciale. O astfel de acţiune ar fi posibilă doar pe calea accesării serverelor (sisteme informatice) care aparţineau băncilor ce deserveau deţinătorii acelor carduri. Ca urmare, soluţia de calificare a celor comise de către F.S. și persoanele neidentificate ar fi trebuit să includă art. 259 CP RM.

Printre exemplele de acces la un sistem informatic, G. Zlati specifică următoarele: accesarea unui cont bancar online; folosirea de la distanţă *(remote access)* a unui sistem informatic prin intermediul programului Team Viewer; autentificarea (accesul) fără drept la interfaţa de administrare a unei pagini web; utilizarea clandestină a puterii de calcul a unui sistem informatic prin intermediul unui program informatic în vederea generării de noi monede electronice [26, p. 195-197; 21].

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. [21]. 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 [8]. Despre astfel de cazuri, în care s-a aplicat art. 360 din Codul penal al României, 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. 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. 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. 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. Pentru a avea control asupra paginii de Facebook, inculpata a modificat parola de acces" [23]. 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 soţia inculpatului, i-a spus inculpatului că user name-ul și parola de la adresa de mail a soţiei sale ar putea să fie salvate, astfel că acesta din urmă a accesat aplicaţia Yahoo Messenger și a observat că era afișat Yahoo! ID: I@yahoo.com, parola (Password) fiind memorată, iar prin intermediul butonului „Sign in" a deschis aplicaţia. În acest mod, inculpatul C., ajutat de martorul B., a accesat, fără a avea acordul soţiei sale, G., adresa de poștă electronică a acesteia, având denumirea: I@yahoo.com, comportându-se, din punct de vedere informatic, ca și cum ar fi fost utilizatorul autorizat G." [16]. O speţă asemănătoare găsim în jurisprudenţa 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 aparţinea lui D.M. și a modificat parola de acces la această adresă. Apoi, V.A., aflând informaţia 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 [10, 14].

Observăm că, în ultima speţă, făptuitorul nu doar a accesat un sistem informatic (serverul prin intermediul căruia era prestat serviciul de poștă electronică), ci și a obţinut posibilitatea de a recurge la informaţia computerizată din contul de poștă electronică al victimei, în vederea beneficierii de calităţile utile ale acestei informaţii. În general, indiferent de modalitatea faptică sub care se înfăţișează accesul la un sistem informatic, trebuie să stabilim dacă acest acces a avut o continuitate, astfel încât să putem vorbi despre accesul la informaţia computerizată din acel sistem. Doar într-un asemenea caz putem vorbi despre accesul la informaţia computerizată în sensul art. 259 CP RM.

În mod similar – indiferent de modalitatea faptică sub care se înfăţișează accesul la un calculator, la un suport material de informaţie ori la o reţea informatică – trebuie să stabilim dacă acest acces a avut o continuitate, astfel încât să putem vorbi despre accesul la informaţia computerizată din acel calculator, din acel suport material de informaţie ori din acea reţea informatică. În lipsa unei astfel de continuităţi, nu putem vorbi despre accesul la informaţia computerizată în sensul art. 259 CP RM.

Încheiem examinarea noţiunii de acces la informaţia computerizată cu analiza unui alt aspect, nelipsit de interes. Astfel, unele norme corespondente cu art. 259 CP RM, prevăzute de anumite legi penale străine, conţin formulări pe care nu le atestăm în art. 259 CP RM. Spre exemplu, § 1 art. 550bis din Codul penal al Regatului Belgiei prevede: „Cel care, ştiind că nu este au-

torizat, accesează un sistem informatic *sau se menţine în acesta* (subl. noastră) este pedepsit cu închisoare 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 sau doar la una din aceste pedepse" [5]. Art. 615-ter din Codul penal al Republicii Italia prevede: „Cel care pătrunde în mod abuziv într-un sistem informatic sau de telecomunicaţii protejat de măsuri de siguranţă *sau rămâne acolo contrar voinţei exprimate sau tacite a celui care are dreptul să-l dea afară* (subl. noastră) este pedepsit cu închisoare până la 3 ani" [6]. De asemenea, art. 509-1 din Codul penal al Marelui Ducat de Luxemburg prevede: „Cel care, în mod fraudulos, a accesat *sau a rămas, în întregime sau în parte, într-un sistem de prelucrare sau de transmitere automată a datelor* (subl. noastră) se pedepseşte cu închisoare de la 2 luni la 2 ani şi cu amendă de la 500 euro la 25.000 euro sau cu una dintre aceste două pedepse [...]" [4].

La fel ca în art. 259 CP RM, în art. 360 din Codul penal al României nu sunt utilizate formulări de genul celor evidenţiate în dispoziţiile reproduse mai sus. Ca urmare, G. Zlati consideră nereglementată în art. 360 din Codul penal al României ipoteza menţinerii accesului după retragerea ori expirarea autorizării: „În măsura în care, după un acces intenţionat autorizat sau un acces obţinut în mod fortuit (de exemplu, o redirecţionare automată a utilizatorului) ori din eroare (de exemplu, agentul crede că interacţionează cu propriul sistem informatic), agentul păstrează accesul, rămânând în pasivitate, nu se va putea reţine – art. 360 C. pen. 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" [26, p. 192].

Așa cum rezultă din dispoziţia de la alin. (1) art. 259 CP RM, accesul ilegal la informaţia computerizată presupune, printre altele, lipsa autorizării. Aceasta presupune, printre altele, ipoteza când, iniţial, făptuitorul a fost autorizat să acceseze informaţia computerizată. Odată consumată autorizarea, dacă făptuitorul continuă să acceseze cu intenţie informaţia computerizată, el devine pasibil de răspundere în baza art. 259 CP RM. Într-o altă ipoteză, dacă făptuitorul a obţinut accesul la informaţia computerizată în mod fortuit sau din eroare, acesta devine pasibil de răspundere în baza art. 259 CP RM, dacă va continua să acceseze cu intenţie informaţia computerizată. Desigur, în ambele ipoteze, art. 259 CP RM este aplicabil numai dacă sunt prezente toate celelalte condiţii stabilite în cadrul acestui articol.

Așadar, nu este necesar ca art. 259 CP RM să fie completat după modelul § 1 art. 550bis din Codul penal al Regatului Belgiei, al art. 615-ter din Codul penal al Republicii Italia și al art. 509-1 din Codul penal al Marelui Ducat de Luxemburg. Menţinerea accesului ilegal la informaţia computerizată după retragerea ori expirarea autorizării este avută în vedere implicit în dispoziţia art. 259 CP RM.

Concluziile acestui studiu sunt:

1) prin „acces la informaţia computerizată", în accepţiunea art. 259 CP RM, trebuie de înţeles: obţinerea posibilităţii de a recurge la informaţia computerizată, în vederea beneficierii de calităţile utile ale acesteia;
2) acţiunea 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 informaţie, trebuie privită ca situaţie-premisă, nu ca etapă în procesul de săvârșire a accesului ilegal la informaţia 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 informaţia computerizată, dacă, din cauze independente de voinţa făptuitorului, nu este săvârșit accesul ilegal la acea informaţie;
3) folosirea și/sau dispunerea de informaţia computerizată reprezintă scopul acţiunii de acces la informaţia computerizată, scop care depășește cadrul acestei acţiuni;
4) în cazul infracţiunilor prevăzute la art. 259 CP RM, accesul la informaţia computerizată este fie integral, fie parţial;
5) în cazul infracţiunilor prevăzute la art. 259 CP RM, accesul la informaţia computerizată presupune o interacţiune logică, nu fizică, cu o astfel de informaţie. Interacţiunea logică cu informaţia computerizată se exprimă în aceea că făptuitorul folosește un program informatic sau mai multe programe informatice care asigură prelucrarea acelei informaţii;
6) infracţiunea 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 infracţiunilor prevăzute la art. 259 CP RM, se accesează ilegal informaţia computerizată din calculatoare, de pe suporţii materiali de informaţie, din sistemul sau reţeaua informatică, nu informaţia computerizată transmisă între calculatoare, între suporţii materiali de informaţie, între sisteme informatice sau între reţele informatice;
7) menţinerea accesului ilegal la informaţia computerizată după retragerea ori expirarea autorizării este avută în vedere implicit în dispoziţia art. 259 CP RM.

Referinţe bibliografice:

1. Bodoroncea G. ș.a. *Codul penal: comentariu pe articole*. Bucureşti: C.H. Beck, 2014. 902 p.
2. Brînza S., Stati V. *Tratat de drept penal. Partea Specială. Vol. II*. Chișinău: Tipografia Centrală, 2015. 1300 p.
3. Codul de procedură penală al României din 01.07.2010. În: *Monitorul Oficial al României*, 2010, nr. 486. În vigoare din 1 februarie 2014.
4. *Codul penal al Marelui Ducat de Luxemburg*. codexpenal.just.ro/laws/Cod-Penal-Luxemburg-RO.html (vizitat 20.07.2022).
5. *Codul penal al Regatului Belgiei*. codexpenal.just.ro/laws/Cod-Penal-Belgia-RO.html (vizitat 20.07.2022).
6. *Codul penal al Republicii Italia*. codexpenal.just.ro/laws/Cod-Penal-Italia-RO.html (vizitat 20.07.2022).
7. Codul penal al României din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510. În vigoare din 1 februarie 2014.
8. Coman V. *Accesarea contului de e-mail şi de Facebook. Noţiunea de date informatice. Forma agravată prevăzută de art. 360 alin. (3) CP*. 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/ (vizitat 20.07.2022).
9. *Decizia Colegiului penal al Curţii de Apel Chișinău din 20.05.2020. Dosarul nr. 1a-631/2020*. https://cac.instante.justice.md/ro/pigd_integration/pdf/45946398-403f-4820-8c4e-0ed11ad86fc1 (vizitat 19.07.2022).
10. *Decizia Colegiului penal lărgit al Curţii Supreme de Justiţie din 13.03.2006. Dosarul nr. 1ra-208/2007*. http://jurisprudenta.csj.md/archive_courts/cauta/ (vizitat 20.07.2022).
11. Decizia Înaltei Curţi de Casaţie şi 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. În: *Monitorul Oficial al României*, 2013, nr. 760.
12. *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*. https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=RO (vizitat 18.07.2022).
13. Dumneanu L., Gurev D. *Infracţiuni în domeniul informatic: Note de curs*. Chișinău: CEP USM, 2021. 261 p.
14. *Hotărârea Plenului Curţii Supreme de Justiţie din 30.06.2008. Dosarul nr. 4-1re-209/2008*. http://jurisprudenta.csj.md/archive_courts/cauta/ (vizitat 20.07.2022).
15. Ioniță Gh.Iu. Accesul la un sistem informatic și recursul în interesul legii formulat în această materie. În: *Revista de Drept Penal*, 2013, vol. 20, nr. 4, p. 111-125.
16. Iugan A.V. *Acces fără drept la sisteme informatice și alterarea integrității datelor informatice*. https://www.universuljuridic.ro/acces-fara-drept-la-sisteme-informatice-si-alterarea-integritatii-datelor-informatice/ (vizitat 20.07.2022).
17. *Înalta Curte de Casaţie şi Justiţie a României. Secţia penală. Decizia nr. 416/A/2016*. www.scj.ro/1093/Detalii-jurisprudenta?customQuery%5B0%5D.Key=id&customQuery%5B0%5D.Value=133689 (vizitat 19.07.2022).
18. Moţoc C., Gîrla L. Protecţia juridico-penală a secretului profesional prin prisma incriminărilor prevăzute la art. 178, 259, 260[1], 260[2] CP RM. În: *Revista ştiinţifică a USM „Studia Universitatis Moldaviae", Seria Ştiinţe Sociale*, 2020, nr. 3, p. 139-151.
19. Nestor R.A. *Incriminarea accesului ilegal la un sistem informatic sau riscul de a transforma un mijloc esenţial de obţinere a informaţiei în mod de încălcare a legii penale*. 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 (vizitat 18.07.2022).
20. *Sentinţa Judecătoriei Chișinău (sediul Buiucani) din 14.02.2019. Dosarul nr. 1-601/2018*. https://jc.instante.justice.md/ro/pigd_integration/pdf/c8678a6c-f738-e911-80d5-0050568b021b (vizitat 19.07.2022).
21. Tamas-Erno P. Accesarea ilegală a conturilor de Facebook privit din perspectiva dreptului penal. În: *Revista Facultăţii de Drept Oradea*, 2019, nr. 1, p. 151-157.
22. *Tribunalul Covasna. Sentinţă penală nr. 11 din 05.03.2019*. https://www.jurisprudenta.com/jurisprudenta/speta-150kzrwm/ (vizitat 19.07.2022).
23. *Tribunalul Neamţ. Sentinţă penală 56/P din 31.08.2016*. https://www.jurisprudenta.com/jurisprudenta/speta-109d7k31/ (vizitat 20.07.2022).
24. Vasiu I., Vasiu L., Contaminanţii informatici, ca vector ai accesului ilegal. În: *Revista de Drept Penal*, 2006, nr. 2, p. 37-40.
25. Zlati G. *Greşita interpretare a accesului la un sistem informatic. Consecinţe practice*. https://www.juridice.ro/259331/gresita-interpretare-a-accesului-la-un-sistem-informatic-consecinte-practice.html (vizitat 19.07.2022).
26. Zlati G. *Tratat de criminalitate informatică. Vol. I*. București: Editura Solomon, 2020. 658 p.
27. Zlati G. *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/ (vizitat 20.07.2022).
28. *Convention on Cybercrime*. https://rm.coe.int/1680081561 (vizitat 18.07.2022).
29. *Explanatory Report to the Convention on Cybercrime*. https://rm.coe.int/16800cce5b (vizitat 18.07.2022).
30. Курбанов Г.С.О. Объективная сторона преступления, связанного с неправомерным доступом к компьютерной информации. В: *Правовая информатика*, 2013, №4, с. 17-20.