CZU: 343.346.8:343(478)(094.4) **http://doi.org/10.59295/sum3(163)2023_18**

ACȚIUNEA ADIACENTĂ DIN CADRUL INFRACȚIUNILOR PREVĂZUTE LA ART. 259 DIN CODUL PENAL

Alexandru STRÎMBEANU
Universitatea de Stat din Moldova

Obiectul de investigație îl reprezintă cele șase modalități normative ale acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 din Codul penal al Republicii Moldova: 1) distrugerea informației computerizate; 2) deteriorarea informației computerizate; 3) modificarea informației computerizate; 4) blocarea informației computerizate; 5) copierea informației computerizate; 6) dereglarea funcţionării calculatoarelor, a sistemului informatic sau a reţelei informatice. În rezultatul examinării opiniilor doctrinare, a prevederilor normative relevante și a exemplelor din jurisprudența națională, este propusă propria viziune asupra înțelesului fiecăreia din noțiunile care se referă la cele șase modalități. În cadrul investigației sunt stabilite carențele ce caracterizează textul legii penale și, drept urmare, sunt recomandate soluții de remediere a acestora.

Cuvinte-cheie: *acțiune adiacentă, faptă prejudiciabilă, distrugere, deteriorare, modificare, blocare, copiere, dereglare, informație computerizată, sistem informatic*.

ADJACENT ACTION FROM THE COMPOSITION OF THE OFFENSES PROVIDED IN ART. 259 OF THE CRIMINAL CODE

The object of the investigation is represented by the six normative variants of the adjacent action from the composition of the prejudicial act provided in art. 259 of the Criminal Code of the Republic of Moldova: 1) destroying computerized information; 2) deteriorating computerized information; 3) changing computerized information; 4) blocking computerized information; 5) copying computerized information; 6) malfunction of the computers, computer systems or networks. As a result of the examination of doctrinal opinions, relevant normative provisions and examples from national jurisprudence, one's own view on the meaning of each of the notions that refer to the six modalities is proposed. During the investigation, the shortcomings that characterize the text of the criminal law are established and, as a result, solutions to remedy them are recommended.

Keywords: *adjacent action, prejudicial act, destroying, deteriorating, changing, blocking, copying, malfunction, computerized information, computer system.*

Introducere

În art. 259 CP RM sunt specificate șase modalități normative ale acțiunii adiacente din cadrul faptei prejudiciabile:

1) distrugerea informației computerizate;
2) deteriorarea informației computerizate;
3) modificarea informației computerizate;
4) blocarea informației computerizate;
5) copierea informaţiei computerizate;
6) dereglarea funcţionării calculatoarelor, a sistemului informatic sau a reţelei informatice.

Modalitățile respective au un caracter alternativ. Prezența oricăreia dintre cele șase modalități este suficientă pentru constatarea prezenței acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM. Numărul de modalități normative ale acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM poate fi luat în considerare la individualizarea pedepsei.

Rezultate obținute și discuții

Cât privește modalitatea normativă de ***distrugere a informaţiei computerizate***, în doctrina penală sunt exprimate variate opinii referitoare la conținutul noțiunii corespunzătoare.

Astfel, S. Brînza şi V. Stati înţeleg prin „distrugere a informaţiei computerizate” „ştergerea ireversibilă şi completă a informaţiei computerizate” [1, p. 354]. După A. Barbăneagră și Gh. Alecu, „prin distrugere se înţelege fapta persoanei orientată spre nimicirea informaţiei, care nu mai poate fi restabilită” [2, p. 568]. M. Gheorghiță menționează: „Prin distrugere se înțelege înlăturarea (ștergerea, defectarea) completă sau parțială a informației, care nu poate fi restabilită [3, p. 570]. Un punct de vedere similar îl exprimă V. Soltan. [4] În viziunea lui A. Borodac, „distrugerea informației computerizate presupune ștergerea completă sau parțială a ei, nemaiputând fi utilizată conform destinației sale inițiale, și neputând fi restabilită chiar nici cu ajutorul unor programe speciale” [5, p. 365]. C. Moțoc și L. Gîrla afirmă: „Distrugerea informației nu înseamnă redenumirea fișierului în care ea se conține, ci și „dispariția” automată a versiunilor vechi ale fișierelor de către ultima dată în timp. Termenul „distrugere” înseamnă un tip de impact asupra informațiilor pe calculator, în urma căruia se pierde posibilitatea utilizării ulterioare de către oricine” [6]. L. Gîrla și Iu. Tabarcea consideră că „distrugerea informației este un gen de influențare asupra informației computerizate, ce presupune că posibilitatea utilizării ei ulterioare de către oricine se pierde pentru totdeauna” [7, p. 17]. Părerea lui N. Lazareva este că „distrugerea informației computerizate constă în lichidarea acesteia prin orice metode, ceea ce duce la imposibilitatea utilizării informației conform destinației, și nu depinde de posibilitatea recuperării acesteia prin mijloace și metode de care dispune victima” [8].

Examinarea sintetică a acestor definiții ne conduce spre următoarea concluzie: distrugerea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, care exclude restabilirea ei ulterioară, indiferent de mijloacele și procedeele aplicate.

Din alin.1 art. 4 al Convenției de la Budapesta ar rezulta că distrugerea datelor informatice nu trebuie echivalată cu ștergerea sau eliminarea acestora: „Fiecare parte va adopta măsurile legislative şi alte măsuri considerate necesare pentru a incrimina ca infracţiune, potrivit dreptului său intern, fapta comisă intenţionat şi fără drept de a distruge, şterge, deteriora, modifica sau elimina date informatice” [9]. Folosirea distinctă a cuvintelor „distruge”, „șterge” și „elimina” demonstrează că aceste cuvinte au semnificații care diferă.

Nu același lucru rezultă din art. 260^3 CP RM care are menirea să transpună pe plan intern prevederile alin.1 art. 4 al Convenției de la Budapesta: „Modificarea, ştergerea sau deteriorarea intenţionată a datelor informatice ţinute într-un sistem informatic ori restricţionarea ilegală a accesului la aceste date, transferul neautorizat de date informatice dintr-un sistem informatic, dintr-un mijloc de stocare, dobândirea, comercializarea sau punerea la dispoziţie, sub orice formă, a datelor informatice cu acces limitat, dacă aceste acţiuni au cauzat daune în proporţii mari [...]”. Dintr-o asemenea formulare, care cu foarte multă aproximație reproduce prevederile alin.1 art.4 al Convenției de la Budapesta, s-ar putea deduce că ştergerea intenţionată a datelor informatice este una dintre manifestările distrugerii informației computerizate.

Acest tablou al ambiguității este completat de explicația din pct. 61 al Raportului explicativ la Convenția de la Budapesta, referitoare la alin.1 art. 4 al Convenției de la Budapesta: „La alineatul 1, „distrugerea” [...] se referă în special la o modificare negativă a integrității sau a conținutului informațional al datelor și programelor. „Ștergerea” datelor este echivalentul distrugerii unui lucru corporal. Le distruge și le face de nerecunoscut. Eliminarea datelor computerizate înseamnă orice acțiune care împiedică sau încetează disponibilitatea datelor pentru persoana care are acces la computer sau suportul de date pe care au fost stocate” [10].

Toate aceste neclarități contribuie la lipsa de previzibilitate a noțiunii „distrugerea informaţiei computerizate”. Considerăm că această carență a art. 259 CP RM nu-i poate fi imputată făptuitorului. Întrucât (așa cum rezultă din alin. (2) art. 3 CP RM) legea penală necesită o interpretare restrictivă, suntem de părerea că ștergerea sau eliminarea informaţiei computerizate nu pot să reprezinte exemple care decurg din noțiunea „distrugerea informaţiei computerizate”, folosite în art. 259 CP RM. Această noțiune poate fi reprezentată numai de distrugerea sau deteriorarea calculatorului, a suportului material de informaţie, a sistemului informatic sau a reţelei informatice, care are ca efect distrugerea informației computerizate ce se afla în acel calculator, pe acel suport material de informaţie, în acel sistem informatic sau în acea reţea informatică. În aceste condiții, art. 259 CP RM trebuie aplicat împreună cu art. 197 CP RM sau cu art.104 din Codul contravențional.

Următoarea modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM este ***deteriorarea informaţiei computerizate***.

S. Brînza și V. Stati înțeleg prin „deteriorarea informaţiei computerizate” „aducerea informaţiei computerizate într-o stare care o face inutilizabilă temporar sau în parte” [1, p. 354]. După părerea lui A. Borodac, „deteriorarea constă în distrugerea parțială a informației, ea neputând fi utilizată conform destinației sale inițiale, dar putând fi restabilită prin intermediul unor programe speciale” [5, p. 365]. L. Gîrla și Iu. Tabarcea consideră că „deteriorarea informaţiei computerizate se exprimă în aducerea ei în stare de inutilitate parțială, atunci când o parte a informației este distorsionată sau alterată” [7, p. 17].

Analizând aceste definiții, putem deduce că deteriorarea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, ce are ca efect pierderea în parte sau pentru un anumit timp a calităților utile ale acesteia. Spre deosebire de distrugerea informaţiei computerizate, deteriorarea informaţiei computerizate nu exclude restabilirea ei ulterioară.

Ca și distrugerea informaţiei computerizate, deteriorarea informaţiei computerizate nu poate presupune ștergerea sau eliminarea acestei informații. Argumentele, prezentate mai sus în legătură cu noțiunea „distrugerea informaţiei computerizate” își păstrează valabilitatea în raport cu noțiunea „deteriorarea informaţiei computerizate”. De aceea, noțiunea „deteriorarea informaţiei computerizate” poate fi reprezentată numai de deteriorarea calculatorului, a suportului material de informaţie, a sistemului informatic sau a reţelei informatice, care are ca efect deteriorarea informației computerizate ce se afla în acel calculator, pe acel suport material de informaţie, în acel sistem informatic sau în acea reţea informatică. În asemenea împrejurări, art. 259 CP RM trebuie aplicat împreună cu art. 197 CP RM sau cu art.104 din Codul contravențional.

O altă modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM este ***modificarea informaţiei computerizate***.

În viziunea lui S. Brînza și V. Stati, prin „modificarea informaţiei computerizate” trebuie de înțeles „alterarea informaţiei computerizate inițiale” [1, p. 354]. Din punctul de vedere al lui A. Barbăneagră și Gh. Alecu, „modificarea desemnează schimbarea aspectului, formei şi a conţinutului informaţiei, adică făptuitorul introduce sau şterge date informatice din calculator, sistemul sau reţeaua informatică” [2, p. 568]. După părerea lui M. Gheorghiță, „modificare înseamnă prelucrarea nesancționată a informației primare, care include orice modificări ale ei (de exemplu, introducerea noilor date, crearea fișierelor etc.)” [3, p. 570]. În mod similar se exprimă V. Soltan [4]. În opinia lui A. Borodac, „modificarea presupune introducerea în informația din calculatoare, de pe suporții materiali de informație, din sistemul sau rețeaua informatică a unor schimbări și completări ce nu sunt în interesul proprietarului, posesorului sau utilizatorului, fie prelucrarea informației primare în așa mod încât informația nu mai poate fi utilizată conform destinației sale inițiale” [5, p. 365-366]. C. Moțoc, L. Gîrla și Iu. Tabarcea menționează că „modificarea informației înseamnă o schimbare a conținutului acesteia în comparație cu informația care a fost inițial la dispoziția proprietarului sau a utilizatorului legitim” [6; 7, p. 17-18]. Nu în ultimul rând, N. Lazareva propune ca prin „modificarea informației computerizate” să fie înțeleasă „introducerea oricăror schimbări neautorizate de către proprietar, posesor sau persoana autorizată de aceștia” [8].

Examinarea sintetică a acestor definiții ne duce spre următoarea concluzie: modificarea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, ce implică schimbarea conținutului, formei sau aspectului acesteia. Spre deosebire de distrugerea și deteriorarea informaţiei computerizate, modificarea informaţiei computerizate presupune afectarea nu a integrității acesteia, ci a autenticității informaţiei computerizate. Informația modificată este – sub aspect cantitativ sau calitativ – diferită față de informația inițială, cea dinaintea modificării. Modificarea informației computerizate presupune fie substituirea unei părți din informația inițială cu alta, fie completarea informației inițiale cu alta. De asemenea, făptuitorul poate: introduce părți ale unei informații computerizate în conținutul unei alte informații computerizate; schimba ordinea părților dintr-o informație computerizată, etc.

În contextul analizei modalității normative de modificare a informației computerizate, prezintă interes

exemplul adus de către G. Zlati: „Agentul lansează un atac informatic împotriva sistemelor informatice deținute de un spital în vederea comiterii unui omor. Spre exemplu, agentul accesează fără drept baza de date a spitalului [...] și modifică [...] tratamentul unui pacient cu intenția de a-i provoca decesul [...]” [11]. Precizăm că, în această ipoteză, concursul dintre infracțiunile prevăzute la art. 145 (cu sau fără referire la art. 27 CP RM) și 259 CP RM este posibil numai dacă accesul ilegal la baza de date a spitalului, însoțit de modificarea acestor date, produce daune în proporții mari sau deosebit de mari. În lipsa unor asemenea daune, se va aplica doar art. 145 CP RM (cu sau fără referire la art. 27 CP RM).

Următoarea modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art.259 CP RM este ***blocarea informaţiei computerizate***.

S. Brînza și V. Stati consideră că, în acest caz, vorbim despre „crearea de inaccesibilitate a informaţiei computerizate, deşi informaţia dată se păstrează”. [1, p. 354] A. Barbăneagră și Gh. Alecu afirmă că „blocarea se realizează prin împiedicarea recepţionării sau transmiterii informaţiei computerizate”. [2, p. 568] Părerea lui M. Gheorghiță este că „blocarea înseamnă închiderea informației păstrate, ceea ce conduce la inaccesibilitatea utilizării ei pentru acțiunile competente ale utilizatorului” [3, p. 570]. În termeni similari își formulează opinia V. Soltan [4]. Din punctul de vedere al lui A. Borodac, „prin blocarea informației computerizate se înțelege introducerea unor informații (piedici, fișiere, parole etc.). care creează imposibilitatea utilizării ei, în cazul în care informația este păstrată pe suporții materiali de informație” [5, p. 365]. C. Moțoc și L. Gîrla consideră că „blocarea informațiilor reprezintă un set de acțiuni sau o singură acțiune ce creează o dificultate artificială totală sau parțială (utilizarea informațiilor devenind imposibilă sau substanțial dificilă) în accesare la informații de către utilizatori; astfel de acțiuni nu sunt legate de distrugerea acestor informații” [6]. După părerea lui L. Gîrla și Iu. Tabarcea, „blocarea informației presupune crearea inaccesibilității acesteia în rezultatul fie al interzicerii executării ulterioare a unei secvențe de comenzi, fie al opririi funcționării unui dispozitiv, fie al împiedicării reacției unui dispozitiv, deși informația în sine se păstrează” [7, p. 17]. În fine, N. Lazareva afirmă că blocarea informației computerizate constă în „influențarea fizică asupra informației computerizate, [...] care are ca efect incapacitatea temporară sau permanentă de a efectua orice operațiuni asupra informației computerizate” [8].

Analizând aceste definiții, putem deduce că blocarea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, ce are ca efect restricționarea totală sau parțială a accesului victimei la informaţia computerizată. Spre deosebire de distrugerea și deteriorarea informaţiei computerizate, blocarea presupune că informaţia computerizată rămâne intactă. Durata și amploarea blocării informaţiei computerizate pot fi luate în considerare la individualizarea pedepsei.

În context, este interesant să analizăm unele spețe din practica judiciară, pentru a stabili dacă trebuia aplicat art. 259 CP RM.

Astfel, într-o speță, J. A. a fost condamnat în baza alin. (1) art. 177, alin. (1) art. 178 și art. 260^5 CP RM. La 26.07.2015, în intervalul de timp 15.42 - 18.53, de la domiciliul său, acesta a accesat ilegal şi fără consimţământul lui P. P. două conturi de poștă electronică ale acestuia, care conţineau informaţii ce constituiau secretul personal al lui P. P. După aceasta, J. A. a modificat parola de acces la conturile respective, astfel restricționând accesul lui P. P. la acestea, precum şi a modificat datele informatice păstrate de către ultimul, rezultând date necorespunzătoare adevărului Aceste acţiuni au fost comise în scopul de a-l avantaja pe J. A. în litigiul civil dintre acesta și P. P. [12]. În acest caz, lipsește temeiul aplicării alin. (1) art. 178 CP RM. J. A. nu a violat dreptul la secretul scrisorilor, telegramelor, coletelor şi altor trimiteri poştale, al convorbirilor telefonice şi înştiinţărilor telegrafice, cu încălcarea legislaţiei. Aplicarea față de J. A. a alin. (1) art. 178 CP RM constituie un exemplu de aplicare a legii penale prin analogie. Violarea dreptului la secretul poștei electronice nu este incriminată în art. 178 CP RM. Invocarea acestui articol pentru violarea dreptului la secretul poștei electronice reprezintă aplicarea art. 178 CP RM dincolo de limitele stabilite de către legiuitor, ceea ce, în mod evident, este ilegal. Accesarea ilegală a conturilor de poștă electronică ale victimei corespunde noțiunii de acces ilegal la informația computerizată, folosite în art. 259 CP RM. Însă, lipsesc celelalte condiții – prezența acțiunii adiacente și a urmărilor prejudiciabile – care ar permite aplicarea art. 259 CP RM. Or, modificarea ilegală a datelor informatice, precum și restricţionarea ilegală a

accesului la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice, au fost săvârșite în contextul infracțiunii de fals informatic (art. 260[5] CP RM). În concluzie, lui J. A. urma să-i fie aplicată răspunderea doar în baza alin. (1) art. 177 și art. 260[5] CP RM. Modificarea și blocarea informaţiei computerizate, care aparținea victimei, nu a fost săvârșită în contextul uneia dintre infracțiunile prevăzute la art. 259 CP RM.

În altă speță, Ţ. A. a fost condamnată în baza art. 260[5] CP RM. La 16.12.2011, în temeiul încheierii executorului judecătoresc, lui A. I. i-a fost transmis în proprietate privată un bun imobil amplasat în or. Ialoveni. La 03.01.2012, Ţ. A., specialist în evidenţa documentelor al unui oficiu cadastral teritorial, nefiind autorizată să acceseze datele din Registrul Bunurilor Imobile, a accesat ilegal aceste date și a introdus date informatice cu privire la punerea interdicţiei pe imobilul transmis în proprietatea lui A. I. După aceasta, Ţ. A. a restricţionat ilegal accesul la aceste date, în scopul de a limita dreptul de dispoziţie a proprietarului A. I. asupra bunului imobil menţionat. Această interdicţie s-a menţinut până la 13.01.2012 [13]. În acest caz, introducerea ilegală a datelor informatice, precum și restricţionarea ilegală a accesului la aceste date, rezultând date necorespunzătoare adevărului, în scopul de a fi utilizate în vederea producerii unei consecinţe juridice, au fost comise în contextul infracțiunii de fals informatic (art. 260[5] CP RM). Deci, aplicarea acestui articol este întemeiată. Modificarea și blocarea informaţiei computerizate din Registrul Bunurilor Imobile nu a fost săvârșită în contextul uneia dintre infracțiunile prevăzute la art. 259 CP RM. Atestăm accesarea ilegală a informației computerizate, și anume – a datelor din Registrul Bunurilor Imobile. Însă, în lipsa acțiunii adiacente și a urmărilor prejudiciabile, această accesare ilegală a informației computerizate nu este suficientă pentru aplicarea art. 259 CP RM. Întrucât Ț. A., ca persoană publică, a săvârșit o acţiune care ţinea de competenţa unei alte persoane publice (și anume – a accesat datele din Registrul Bunurilor Imobile, nefiind autorizată pentru aceasta), urma să-i fie aplicat suplimentar art. 313 din Codul contravențional, care prevede răspunderea pentru excesul de putere sau depășirea atribuţiilor de serviciu (adică pentru săvârșirea unei acţiuni care depășește în mod vădit limitele drepturilor şi atribuţiilor acordate prin lege şi care contravine intereselor publice sau drepturilor şi intereselor ocrotite de lege ale persoanelor fizice sau juridice, dacă fapta nu întrunește elementele constitutive ale infracțiunii).

În altă speță, G. A. și G. T. au fost condamnați în baza alin. (1) art. 260[6] și lit. b), d) alin. (2) art. 261[1] CP RM. În perioada 06.03.2018 - 14.03.2018, în scopul prestării serviciilor de „Call Centru”, cei doi făptuitori au fondat întreprinderea „G.A.L.” S.R.L., al cărei administrator era G. T. Utilizând fraudulos un număr din numerotația de telefonie fixă, atribuită de către compania „Moldtelecom” S.A., G. A. și G. T. au închiriat o cameră într-un imobil, unde au instalat un sistem informatic, interconectat cu alte două sisteme informatice. În aceste împrejurări, făptuitorii au accesat neautorizat rețelele şi serviciile de telecomunicații ale companiei „Moldtelecom” S.A., au restricționat accesul la datele informatice şi au efectuat terminații neautorizate ale traficului voce local şi internațional, generând ilegal 40687,9 minute, cauzând astfel companiei „Moldtelecom” S.A. daune în mărime de 183.790,25 lei [14]. În acest caz, restricționarea accesului la datele informatice a fost săvârșită în contextul infracțiunii prevăzute la alin. (1) art. 260[6] CP RM. Or, restricţionarea accesului la aceste date a urmărit scopul de a obţine un beneficiu material, fiind cauzate daune în proporţii mari. Restricționarea accesului la datele informatice a fost precedată nu de accesul ilegal la informația computerizată în sensul art. 259 CP RM, ci de accesul neautorizat la reţelele şi serviciile de telecomunicaţii. Pune în gardă că daunele în proporții mari au fost reținute la calificare de două ori, deși au fost cauzate o singură dată. Considerăm că daunele în proporții mari au fost cauzate în contextul fraudei informatice (alin. (1) art. 260[6] CP RM), nu al accesului neautorizat la reţelele şi serviciile de telecomunicaţii (lit. b) și d) alin. (2) art. 261[1] CP RM). Accesul neautorizat la reţelele şi serviciile de telecomunicaţii a constituit nu un scop în sine, ci etapa de pregătire de infracțiunea prevăzută la alin. (1) art. 260[6] CP RM. În concluzie, G. A. și G. T. ar fi urmat să răspundă doar în baza alin. (1) art. 260[6] CP RM.

După examinarea acestor exemple din practica judiciară, revenim la analiza modalităților normative ale acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM. Următoarea modalitate de acest gen este ***copierea informaţiei computerizate***.

S. Brînza și V. Stati afirmă că, prin „copierea informaţiei computerizate” se înțelege „reproducerea informaţiei computerizate originale, deşi această informaţie se păstrează intactă şi în stare de utilizare” [1, p. 354]. După

A. Barbăneagră și Gh. Alecu, „acţiunea de copiere presupune transferul ilegal al informaţiei computerizate de pe un suport material pe altul” [2, p. 568]. M. Gheorghiță exprimă punctul de vedere, conform căruia „copierea înseamnă transferul informației de pe un suport material (de informație) pe altul, precum și înregistrarea ilegală a informației computerizate în memoria [calculatorului]” [3, p. 570]. O părere similară are V. Soltan [4]. În opinia lui A. Borodac, „copierea înseamnă reproducerea informației textuale, grafice, a unui desen sau a unei fotografii de pe un suport material de informație pe altul, dintr-un calculator în altul, cu păstrarea informației copiate” [5, p. 365]. C. Moțoc și L. Gîrla menționează: „„Copierea informațiilor” înseamnă o astfel de acțiune neautorizată de către proprietarul legal (proprietar, utilizator) a informațiilor și (sau) încălcarea legii privind utilizarea (deținerea, eliminarea) în rezultatul căreia apare o altă copie (sau mai multe) a informațiilor originale, reprezentând repetarea exactă a acesteia (duplicarea originală a informațiilor)” [6]. În viziunea lui L. Gîrla și Iu. Tabarcea, „copierea informației înseamnă crearea copiei informației originale, păstrând în același timp capacitatea de a o utiliza conform destinației. Din punct de vedere tehnic, copierea constituie crearea unei secvențe similare de octeți în memoria unui dispozitiv, care este diferit în raport cu cel în care se află informația originală” [7, p. 18]. N. Lazareva consideră că „prin „copierea informației computerizate” se are în vedere repetarea și reproducerea stabilă a acesteia prin orice mijloc pe un suport de informație, altul decât cel original, fiind păstrate caracteristicile care identifică acea informație computerizată” [8].

Analizând aceste definiții, putem deduce următoarele: copierea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune reproducerea informaţiei computerizate într-un alt calculator, pe un alt suport material de informaţie, într-un alt sistem informatic sau într-o altă reţea informatică. Spre deosebire de blocarea informaţiei computerizate, copierea informaţiei computerizate nu exclude beneficierea în continuare de către victimă de informaţia computerizată.

În art. 259 CP RM se are în vedere copierea logică a informației computerizate (care presupune folosirea unui program de calculator), nu copierea fizică a acesteia (de exemplu: reproducerea manuală; reproducerea prin fotografierea textului sau a imaginii de pe ecranul calculatorului etc.). În caz contrar, își pierde sensul noțiunea de informație computerizată, care presupune circulația într-un mediu informatic.

Cu atât mai puțin, reproducerea în creierul uman prin memorare a unei informații văzute, auzite sau altfel percepute nu formează conținutul noțiunii „copierea informației computerizate”, folosite în art. 259 CP RM. O astfel de reproducere este inerentă din momentul accesării oricărei informații computerizate și nu poate fi privită în contextul acțiunii adiacente prevăzute la art. 259 CP RM.

Suntem de acord cu G.S.O. Kurbanov, în opinia căruia copierea informației computerizate trebuie deosebită de multiplicarea acesteia: „În acest ultim caz, informația este reprodusă nu pe un suport de informație diferit de cel original, ci pe suportul de informație original (de exemplu, mai multe fișiere cu același conținut sunt stocate în memoria calculatorului)” [15]. Așadar, condiția esențială pentru atestarea copierii informației computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, este ca informația computerizată copiată să fie stocată într-un alt calculator, pe un alt suport material de informaţie, într-un alt sistem informatic sau într-o altă reţea informatică, decât cel/cea pe care se păstra informația computerizată originală.

Este posibil ca: 1) la același calculator, la același suport material de informaţie, la același sistem informatic sau la aceeași reţea informatică să aibă acces două sau mai multe persoane; 2) totodată, să fie restricționat accesul pentru una sau unele dintre aceste persoane la o parte a unui astfel de calculator, suport material de informaţie sau sistem informatic ori a unei astfel de reţele informatice. Într-o asemenea situație, pentru a aplica art. 259 CP RM, informația computerizată copiată trebuie să fie stocată în acea parte din calculator, din suportul material de informaţie, din sistemul informatic sau din reţeaua informatică, la care nu are acces victima.

În contextul examinării modalității de copiere a informației computerizate, menționăm o opinie exprimată de S. Brînza și V. Stati. Conform acesteia, pornografia neconsimțită în varianta „revenge porn” poate fi calificată în baza art. 177 și 259 CP RM, „dacă imaginile sau alte reprezentări pornografice sunt obținute în rezultatul accesului ilegal la informația computerizată” [16]. În această ipoteză, aplicarea art. 259 CP

RM este posibilă numai dacă se produc daune în proporții mari sau deosebit de mari. În afară de aceasta, pentru ca art. 259 CP RM să poată fi aplicat, accesul ilegal la imaginile sau la alte reprezentări pornografice în formă computerizată trebuie să fie însoțit, de exemplu, de copierea acestor informaţii. Dacă însă accesul ilegal la imaginile sau la alte reprezentări pornografice în formă computerizată este însoțit de diseminarea acestor informații, fără ca ele să fie copiate, atunci lipsește temeiul aplicării art. 259 CP RM.

În opinia lui M. Iu. Dvorețki, „copierea ilegală a informației computerizate poate constitui pregătirea sau tentativa de a comite o altă infracțiune (de exemplu, încălcarea dreptului de autor și a drepturilor conexe)” [17]. Considerăm că această poziție necesită o precizare. Copierea informației computerizate, dacă nu produce daune în proporții mari sau deosebit de mari și dacă nu este precedată de accesul ilegal la acea informație, poate să reprezinte pregătirea de infracțiunile care presupun divulgarea anumitor informații (de exemplu, pregătirea de infracțiunile prevăzute la art. 204, alin. (1) art. 315, art. 316, 337, 344 etc. din Codul penal). În asemenea cazuri, nu este necesară aplicarea art. 259 CP RM, întrucât copierea informației computerizate nu reprezintă un scop în sine și întrucât nu sunt întrunite toate condițiile care ar permite aplicarea art. 259 CP RM.

În alte cazuri, copierea informației computerizate (dacă produce daune în proporții mari sau deosebit de mari și *dacă nu este precedată de accesul ilegal la acea informație*), apare ca modalitate faptică a unor infracțiuni care presupun reproducerea anumitor informații (de exemplu, a infracțiunii prevăzute la lit. a) alin. (1) art. 185^1 CP RM). În asemenea cazuri, nu este necesară aplicarea art. 259 CP RM, întrucât nu sunt întrunite toate condițiile care ar permite aplicarea acestui articol. Dacă sunt prezente toate condițiile cerute de lit. a) alin. (1) art. 185^1 CP RM, atunci se aplică această normă.

În cazuri de altă natură, copierea informației computerizate (dacă produce daune în proporții mari sau deosebit de mari și *dacă este precedată de accesul ilegal la acea informație*), nu poate fi privită ca modalitate faptică a infracțiunii prevăzute la lit. a) alin. (1) art. 185^1 CP RM. În acest caz, se aplică, după caz, lit. a) alin. (1) art. 185^1 CP RM sau art. 259 CP RM. La concret, conform principiului subsidiarității, trebuie să se aplice doar acea normă care prevede pedeapsa mai aspră.

În alt context, dar cu referire la aceeași modalitate normativă de copiere a informației computerizate, trebuie de menționat că alin. (2) art. 360 din Codul penal al României [18] prevede răspunderea pentru accesul fără drept la un sistem informatic, săvârșit în scopul obținerii de date informatice. În legătură cu această circumstanță agravantă, I. Kuglay menționează: „Obţinerea” de date informatice are semnificaţia preluării, a transferului lor, nu se limitează la simpla „vizualizare” a informaţiei” [19, p. 779]. Același autor afirmă: „În forma agravată prin scop, dacă transferul de date are loc, această operaţiune este exterioară infracţiunii prevăzute de art. 360 alin. (2) C.pen. şi va constitui infracţiunea distinctă, de transfer neautorizat de date informatice prevăzută de art. 364 C.pen.” [19, p.780].

Din această opinie rezultă că noțiunea „obținerea de date informatice” din art. 360 din Codul penal al României are același înțeles ca noțiunea „copierea informației computerizate” din art. 259 CP RM. Totuși, copierea informației computerizate reprezintă nu scopul cu efect agravant al uneia dintre infracțiunile prevăzute la art. 259 CP RM. Așa cum am menționat deja, copierea informației computerizate constituie modalitatea normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM. Accesul ilegal la informația computerizată, urmat de copierea acestei informații, dacă produce daune în proporții mari sau deosebit de mari, atrage aplicarea exclusiv a art. 259 CP RM. Nu va fi necesară invocarea suplimentară a unei alte norme.

În același timp, la lit. f) alin .(2) art. 259 CP RM, este specificată circumstanța agravantă „cu utilizarea ilegală a calculatorului, sistemului sau reţelei informatice, în scopul săvârşirii uneia dintre infracţiunile prevăzute la alin. (1), la art. 260^1-260^3, 260^5 şi 260^6”. Astfel că există posibilitatea ca – după săvârșirea accesului ilegal la informația computerizată, urmat de copierea acestei informații, dacă se produc daune în proporții mari – să fie comis transferul neautorizat de date informatice dintr-un sistem informatic, care, la rândul său, produce daune în proporţii mari. În acest caz, vom fi în prezența concursului real de infracțiuni prevăzute la lit. f) alin. (2) art. 259 și art. 260^2 CP RM. În mod firesc, informația computerizată, copiată în contextul infracțiunii prevăzute la lit. f) alin. (2) art. 259 CP RM, trebuie să fie alta decât datele informatice transferate neautorizat în contextul infracțiunii prevăzute la art. 260^2 CP RM. Doar în acest fel daunele în

proporţii mari, produse în contextul infracțiunii prevăzute la lit. f) alin. (2) art. 259 CP RM, nu vor coincide cu daunele în proporţii mari, produse în contextul infracțiunii prevăzute la art. 260^2 CP RM.

Ultima modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM este ***dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice***.

După părerea lui S. Brînza și V. Stati, această modalitate presupune „disfuncționalizarea calculatoarelor, a sistemului sau a reţelei informatice, având ca efect oferirea unei informaţii incorecte, refuzul oferirii informaţiei, scoaterea din funcţiune sau întreruperea funcţionării etc.” [1, p. 354]. A. Barbăneagră și Gh. Alecu consideră că „prin dereglare a funcţionării calculatoarelor, a sistemului sau a reţelei informatice se înţeleg acţiunile de defectare a tehnicii menţionate. Drept consecinţe ale dereglării pot fi: deconectarea tehnicii, recepţionarea informaţiei denaturate etc.” [2, p. 568]. În opinia lui M. Gheorghiță, „dereglarea funcționării MEC (adică a mașinii electronice de calcul – *n.a.*) , sistemului MEC și a rețelelor acestora reprezintă o pană în funcționarea tehnicii de calcul, care împiedică funcționarea normală a mijloacelor de programare sau a echipamentelor, canalelor de telecomunicații cu condiția menținerii integrității lor fizice (de exemplu, reprezentarea informației eronate, scoaterea din funcțiune a sistemului de calculatoare etc.)” [3, p. 570]. Un punct de vedere similar este exprimat de către V. Soltan [4]. A. Borodac este de părera că „prin dereglarea funcționării calculatoarelor, a sistemului sau a rețelei informatice se înțelege încetarea funcționării acestora sau apariția diferitelor piedici, întreruperi în funcționare, reprezentarea informației eronate etc., cu condiția menținerii integrității lor fizice” [5, p. 365]. În viziunea lui L. Gîrla și Iu. Tabarcea, „prin „dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice” se înțelege provocarea unor defecțiuni ale echipamentelor, care presupun emiterea de informații incorecte, refuzul de a emite informații [...]” [7, p. 18]. Nu în ultimul rând, N. Lazareva menționează: „Dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice implică o defecțiune în funcționarea calculatoarelor, a sistemului sau a rețelei informatice, care împiedică funcționarea normală a echipamentelor de calcul, cu condiția ca integritatea fizică a acestuia și restabilirea operabilității să fie păstrată” [8].

Examinarea sintetică a acestor definiții ne conduce spre următoarea concluzie: dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra calculatoarelor, a sistemului sau a rețelei informatice, care implică scoaterea din funcțiune – permanentă sau temporară – a acestora. Durata de scoatere din funcțiune a calculatoarelor, a sistemului sau a reţelei informatice, poate fi luată în considerare la individualizarea pedepsei.

Nu intră sub incidența art. 259 CP RM împiedicarea în orice mod a funcţionării unui sistem informatic, în scopul de a obţine un beneficiu material pentru sine sau pentru altul, dacă aceste acţiuni au cauzat daune în proporţii mari sau deosebit de mari. În acest caz se aplică răspunderea pentru frauda informatică (art. 260^6 CP RM). În acest context, prezentăm o speță: C. O. a fost condamnat în baza alin. (5) art. 42 și alin. (1) art. 260^6 CP RM. În perioada 01.01.2017 - 21.02.2017, C. O. a contribuit în calitate de complice la acordarea de mijloace şi de instrumente autorilor infracţiunii şi anume – lui P. V., D. I. şi I. I. Persoanele în cauză au deschis mai multe conturi de card de plată pe numele lor, la unele bănci din Republica Moldova. Ulterior, P. V., D. I. şi I. I. i-au transmis lui C. O. respectivele carduri. În perioada 17.01.2017 - 21.02.2017, persoane neidentificate, prin intermediul cardurilor bancare menţionate, care le-au fost transmise de către C. O., au efectuat mai multe tranzacţii de retragere frauduloasă a numerarului prin metoda „Transaction Reversal Fraud” de la bancomatele din Marea Britanie, restricţionând accesul la datele informatice şi împiedicând funcţionarea sistemelor informatice ale bancomatelor. În rezultat, au fost cauzate daune în proporţii mari [20]. Observăm că, în acest caz, împiedicarea funcţionării unor sisteme informatice (și anume – a unor bancomate din Marea Britanie) este precedată de accesarea ilegală a acestor sisteme informatice. Mai mult, această împiedicare a funcţionării unor sisteme informatice a cauzat daune în proporţii mari. Cu toate acestea, lipsește temeiul aplicării art. 259 CP RM. Prezența scopului special (și anume – a scopului de a obţine un beneficiu material) face ca art. 260^6 CP RM să fie privit în atare condiții ca normă specială față de art. 259 CP RM. În virtutea regulii stabilite la art. 116 CP RM, într-un asemenea caz, aplicarea art. 260^6 CP RM exclude aplicarea art. 259 CP RM.

Concluzii

Distrugerea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, care exclude restabilirea ei ulterioară, indiferent de mijloacele și procedeele aplicate. Distrugerea informaţiei computerizate nu poate presupune ștergerea sau eliminarea acestei informații.

Deteriorarea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, ce are ca efect pierderea în parte sau pentru un anumit timp a calităților utile ale acesteia. Ca și distrugerea informaţiei computerizate, deteriorarea informaţiei computerizate nu poate presupune ștergerea sau eliminarea acestei informații.

Modificarea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, ce implică schimbarea conținutului, formei sau aspectului acesteia.

Blocarea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra informaţiei computerizate, ce are ca efect restricționarea totală sau parțială a accesului victimei la informaţia computerizată.

Copierea informaţiei computerizate, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune reproducerea informaţiei computerizate într-un alt calculator, pe un alt suport material de informaţie, într-un alt sistem informatic sau într-o altă reţea informatică.

Dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice, ca modalitate normativă a acțiunii adiacente din cadrul faptei prejudiciabile prevăzute la art. 259 CP RM, presupune o asemenea influențare asupra calculatoarelor, a sistemului sau a reţelei informatice, care implică scoaterea din funcțiune – permanentă sau temporară – a acestora.

Referințe:

1. BRÎNZA, S., STATI, V. *Tratat de drept penal. Partea Specială. Vol. II*. Chișinău: Tipografia Centrală, 2015.1300 p. ISBN 978-9975-53-470-3.
2. BARBĂNEAGRĂ, A., ALECU, GH., BERLIBA, V. et al. *Codul penal al Republicii Moldova. Comentariu (Adnotat cu jurisprudenţa CEDO şi a instanţelor naţionale)*. Chişinău: Sarmis, 2009. 860 p. ISBN 978-9975-105-20-0.
3. BARBĂNEAGRĂ, A., BERLIBA, V., BÎRGĂU, M. et al. *Codul penal al Republicii Moldova. Comentariu* / Sub red. lui A. Barbăneagră. Chișinău: ARC, 2003. 836 p. ISBN 9975-61-291-1.
4. SOLTAN, V. Infracțiunile informatice (art. 259-261[1] Cod penal). În: *Procuratura Republicii Moldova. Buletin informativ*, 2010, nr. 15, p. 38-43. [Accesat la 11.07.2022] Disponibil: http://procuratura.md/file/BULETIN%20VIRTUAL%2015.pdf
5. BORODAC, A. *Manual de drept penal. Partea specială*. Chișinău: Tipografia Centrală, 2004. 622 p. ISBN 9975-9788-7-8.
6. MOȚOC, C., GÎRLA, L. Protecția juridico-penală a secretului profesional prin prisma incriminărilor prevăzute la art. 178, 259, 260[1], 260[2] CP RM. În: *Revista științifică a USM „Studia Universitatis Moldaviae”, Seria „Ştiinţe Sociale”*, 2020, nr. 3, p. 139-151. ISSN 1814-3199.
7. ГЫРЛА, Л. Г., ТАБАРЧА, Ю. М. *Уголовное право Республики Молдова. Часть Особенная. Том 2*. Кишинэу: Cartdidact, 2010. 592 p. ISBN 978-9975-4158-2-8.
8. ЛАЗАРЕВА, Н. Уголовно-правовая характеристика преступлений в области информатики и электросвязи. În: *Revista științifică a USM „Studia Universitatis”. Seria „Ştiinţe sociale”*. Chişinău: USM, 2007, nr. 6, p. 133-141. ISSN 1814-3199.
9. Convention on Cybercrime. [Accesat la 11.07.2022] Disponibil: https://rm.coe.int/1680081561
10. *Explanatory Report to the Convention on Cybercrime*. [Accesat la 11.07.2022] Disponibil: https://rm.coe.int/16800cce5b

11. ZLATI, G. Legitima apărare și starea de necesitate în domeniul criminalității informatice (I). În: *Dreptul*, 2015, nr. 4, p. 145-172. ISSN 1018-0435.
12. *Decizia Colegiului penal lărgit al Curții Supreme de Justiție din 11.06.2019. Dosarul nr. 1ra-445/2019* [Accesat la 12.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=13789
13. *Decizia Colegiului penal al Curții Supreme de Justiție din 25.06.2014. Dosarul nr. 1ra-1113/2014*. [Accesat la 12.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=2653
14. *Decizia Colegiului penal al Curții Supreme de Justiție din 05.08.2020. Dosarul nr. 1ra-1508/2020*. [Accesat la 12.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=16547
15. КУРБАНОВ, Г. С. О. Объективная сторона преступления, связанного с неправомерным доступом к компьютерной информации. În: *Правовая информатика*, 2013, № 4, p. 17-20. ISSN 1994-1404.
16. BRÎNZA, S., STATI, V. „Sexting", „sextorsion", „revenge porn": fenomene reflectate în Codul penal al Republicii Moldova? În: *Revista științifică a USM „Studia Universitatis Moldaviae", Seria „Ştiinţe Sociale"*, 2021, nr. 3, p. 3-17. ISSN 1814-3199.
17. ДВОРЕЦКИЙ, М. Ю. Проблемы толкования терминов при квалификации преступлений по ст. 272 Уголовного кодекса РФ. În: *Вестник Тамбовского университета. Серия: Гуманитарные науки*, 2013, № 12, p. 527-532. ISSN 2782-5825.
18. Codul penal al României din 17.07.2009. În: *Monitorul Oficial al României*, 2009, nr. 510.
19. BODORONCEA, G., CIOCLEI, V., LEFTERACHE, L. V. et al. *Codul penal: comentariu pe articole*. Bucureşti: C.H. Beck, 2014. 902 p. ISBN 978-606-18-0408-5.
20. *Decizia Colegiului penal al Curții Supreme de Justiție din 07.11.2018. Dosarul nr. 1ra-1891/2018*. [Accesat la 12.07.2022] Disponibil: http://jurisprudenta.csj.md/search_col_penal.php?id=12288

Date despre autor:
Alexandru STRÎMBEANU, doctorand, Facultatea de Drept, Universitatea de Stat din Moldova.
E-mail: avocatstrimbeanu@yahoo.ro
ORCID: 0000-0002-7746-6541

Prezentat la 24.10.2022