ACCESUL ILEGAL LA INFORMAŢIA COMPUTERIZATĂ: PROBLEMATICA ÎNCADRĂRII JURIDICE ȘI SOLUȚII

Dorina GUREV

CZU: 343.21:004.056.5

În legătură cu pătrunderea largă a tehnologiilor informaționale în toate sferele activităților umane, a apărut necesitatea stringentă, nu doar în sensul înțelegerii consecințelor elaborării și utilizării practice a acestora, ci și în analiza complexă a problemelor apărute în sfera informatizării societății și susținerii securității informaționale. Astfel, în vederea protecției informației computerizate și a sistemului informațional, legiuitorul moldav a incriminat la art.259 CP RM [2] infracțiunea de acces ilegal la informația computerizată.

Problematica încadrării juridice a infracţiunii prevăzute al art.259 CP RM se datorează, în primul rând, structurii complexe a laturii obiective a faptei prejudiciabile, şi anume, faptului că acţiunea principală (accesul ilegal la informaţia computerizată), în mod obligator trebuie să fie însoţită de acţiunea adiacentă (distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice). Astfel în lipsa acesteia, aşa cum o specifică şi S.Copeţichi [4, p.33], cele comise nu pot fi încadrate potrivit art.259 CP RM. Totuşi, în condiţiile în care făptuitorul totodată doreşte să cauzeze şi daune în proporţii mari, cele comise trebuie catalogate drept tentativă la infracţiunea de acces ilegal la informaţia comuterizată, în ipoteza în care făptuitorul realizează acţiunea principală, dar din cauze independente de voinţa lui să nu-i reuşească comiterea uneia din acţiunile adiacente.

În asemenea circumstanțe, nu este clar raţionamentul legiuitorului moldav care la incriminarea infracţiunii de acces ilegal la informaţia computerizată reuneşte în cadrul normei de la art.259 CP RM pe lângă fapta prevăzută la art.2 (Accesarea ilegală) din Convenţia Consiliului Europei privind criminalitatea informatică de la Budapesta [3] şi faptele distinse drept infracţiuni de la art.4 (Afectarea integrităţii datelor), precum şi art.5 (Afectarea integrităţii sistemului), fapt ce

complică semnificativ calificarea faptei.

O altă dilemă apare şi în cazul determinării prejudiciilor în proporţii mari şi a legăturii de cauzalitate dintre acestea, ca semne obligatorii ale laturii obiective. Aceasta deoarece nu toate *modus operandi* care duc la distrugerea, deteriorarea, modificarea, blocarea sau copierea informaţiei, de dereglarea funcţionării calculatoarelor, a sistemului sau a reţelei informatice prevăzute la art.259 CP RM cauzează un prejudiciu ce poate fi estimat în bani (spre exemplu, prin acces ilegal la un calculator, în scop de a împiedica promovarea unei persoane, a fost distrusă o lucrare ştiinţifică sau un program ce reprezintă munca acesteia timp de doi ani). Astfel, apare întrebarea, care este modalitatea de evaluare a informaţiei deţinute într-un sistem informaţional? În asemenea situaţii, prejudiciul cauzat este constituit din prejudiciul moral şi un eventual venit ratat (dacă va fi constatată valoarea propriu-zisă a informaţiei), care este stabilită de către instanţă.

În ceea ce priveşte prejudiciul în proporţii mari cauzat, urmare inclusă de legiuitor prin Legea, nr. 278 din 18.12.2008 [9], care în corespundere cu art.126 CP RM este acela, valoarea căruia depăşeşte 20 de salarii medii lunare pe economie prognozate, stabilite prin Hotărârea Guvernului în vigoare în momentul săvârşirii faptei (cuantumul salariului mediu lunar pe economie, prognozat pentru anul 2020, este în mărime de 7953 lei [8]), credem că este mult prea mare pentru a criminaliza fapta doar în condiţiile prevăzute la art.259 CP RM.

Pe de altă parte, din analiza de drept penal comparată, cum menţionează S.Copeţchi [4, p.35], normele din legiuirile penale ale majorităţii statelor europene, ce incriminează accesul ilegal la sisteme informatice, nu prevăd urmarea prejudiciabilă în calitate de semn constitutiv. Precum şi Convenţia de la Budapesta, care la art.2 prevede, *inter alia,* „incriminarea ca infracţiune, pentru dreptul său intern, accesarea intenţionată şi fără drept a asamblului sau a unei părţi a unui sistem informatic" nu vizaează urmare prejudiciabilă.

Să presupunem că legiuitorul moldav la adoptarea acestei norme s-a dirijat de pct.37 al Raportului explicativ al Convenţia Consiliului Europei privind criminalitatea informatică [7] care, se acordă părţilor posibilitatea de a *exclude infracţiunile minore sau nesemnificative din*

câmpul de aplicare a art.2 până la art.10 din Convenţie, însă este greu de conceput că cauzarea unei daune mai mici de 20 de salarii medii lunare pe economie prognozate (pentru anul 2020 – în sumă mai mică de 159 060 lei), poate fi apreciată drept infracţiune minoră sau nesemnificativă. Mai mult, în conformitate cu pct.11 al Directivei 2013/40/UE referitoare la atacurile împotriva sistemelor informatice [5], *un caz poate fi considerat minor în situaţiile în care prejudiciile cauzate de infracţiune şi/sau riscul la adresa intereselor publice sau private este nesemnificativ sau de alta natură… încât aplicarea unei sancţiuni penale în cadrul limitelor legale sau angajarea răspunderii penale nu este necesară.*

În viziunea noastră, atât Raportul explicativ al Convenției, cât şi Directiva 2013/40/UE referindu-se la infracțiunile minore sau nesemnificative vizează faptele care cauzează un prejudiciu în proporții mici; or, în legislația națională a statelor ce fac parte din Convenţia de la Budapesta, faptele ilicite sunt clasificate diferit în coraport cu gradul de prejudiciabilitate al acestora. De altfel, în conformitate cu dreptul intern al Republicii Moldova, faptă, acţiune sau inacțiune, ilicită, cu un grad de pericol social mai redus decât infracţiunea este contravenția (art.10 Cod contravenţional [1]), ceea ce corespunde cu cele stipulate în Directiva 2013/40/UE.

În context remarcăm că analiza sistemică a normelor din Codul contravenţional al Republicii Moldova ne arată că accesul ilegal la informația computerizată nu își are existența, nici parțială, în calitate de contravenție. Prin urmare, în cazul comiterii acţiunilor prevăzute la art.259 CP RM şi provocând victimei o daună în valoare de până la 159 060 lei, totodată neurmărind cauzarea de daune în proporţii mari, făptuitorul rămâne nepedepsit. În asemenea împrejurări, legiuitorul moldav nu apără pe deplin relaţiile sociale privind accesul legal la informaţia computerizată, şi nici relaţiile sociale privind imixtiunea legală în sistemul informaţional.

Dacă facem o analogie *grosso modo* (în pofida faptului că nu este permisă, însă în cazul nostru, raţională) cu infracţiunea prevăzută la art.179 CP RM (Violarea de domiciliu) ce prevede acţiunea (inacțiunea) de pătrundere sau rămânere ilegală în domiciliul sau în reşedinţa

unei persoane fără consimţământul acesteia, se observă că aceasta nu reprezintă altceva decât accesul ilegal în domicilul sau reşedinţa persoanei. Mai mult, cum este recunoscut şi în doctrină [*a se vedea:* 6, p.159], sistemul informatic împreună cu datele informatice reprezintă *spaţiul informatic* sau *domiciliul informatic*. În asemenea circumstanţe, se prezumă necesitatea reglementării similară a *spaţiul informatic (domiciliul informatic)* cu cel al domiciliului real.

Axându-ne pe raționamentele invocate *supra,* considerăm oportun ca legiuitorul nostru să reevalueze propunerea *de lege ferenda* consemnată în Proiectul de Lege pentru modificarea şi completarea unor acte legislative [10], înregistrat la data de 13.04.2016 şi retras la 14.06.2018, susţinută de către doctrină [4, p.36], şi anume: 1) excluderea urmării prejudiciabile sub formă de daune în proporţii mari din dispoziţia de la alin.(1) art.259 CP RM; şi 2) prevederea accesteia în calitate de circumstanţă agravantă la lit.h) alin.(2) art.259 CP RM.

Referințe:

1. Codul contravențional al Republicii Moldova, adoptat de Parlamentul Republicii Moldova la 24.10.2008. În: *Monitorul Oficial al Republicii Moldova,* 2017, nr.78-84.
2. Codul penal al Republicii Moldova, adoptat de Parlamentul Republicii Moldova la 18.04.2002. În: *Monitorul Oficial al Republicii Moldova*, 2002, nr.128-129.
3. Convenţia Consiliului Europei privind criminalitatea informatică de la Budapesta din 23.11.2001 [Accesat 20.08.2020] Disponibil: http://legislatie.just.ro/Public/DetaliiDocumentAfis/51289
4. COPETCHI, S. Infracţiunile informatice potrivit legii penale moldave: studiu de drept penal comparat şi propuneri de lege ferenda. În: *Culegerea comunicărilor Conferinţa ştiinţifică naţională cu participare Internaţională: ,,Realităţi şi perspective ale învăţământului juridic naţional",* Volumul II, 01-02 octombrie 2019, pp.29-36.
5. Directiva 2013/40/UE a Parlamentului European şi a Consiliului privind atacurile împotriva sistemelor informatice şi de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului din 12 august 2013 [Accesat 20.08.2020] Disponibil: https://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=RO.
6. DOBRINOIU, M. *Infracțiuni în domeniul informatic.* București: C.H.Beck, 2006, 401 p. ISBN:973-655-941-6.

7. Explanatory Report to the Convention on Cybercrime. Budapest, 23.XI.2001. European Treaty Series, no.185 [Accesat 20.08.2020] Disponibil: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent? documentId=09000016800cce5b.
8. Hotărârea Guvernului Republicii Moldova privind aprobarea cuantumului salariului mediu lunar pe economie, prognozat pentru anul 2020, nr.678 din 27.12.2019. În: *Monitorul Oficial al Republicii Moldova*, nr.400-406 din 31.12.2019.
9. Legea pentru modificarea și completarea Codului penal al Republicii Moldova nr. 278 din 18.12.2008. În: *Monitorul Oficial al Republicii Moldova*, nr. 37-40 din 20.02.2009.
10. Proiectul legii pentru modificarea și completarea unor acte legislative (Legea privind Serviciul de Informații și Securitate al RM – art.7; Codul penal – art.178, 208^1, 259, ș.a.). [Accesat 20.08.2020] Disponibil: http://www.parlament.md/ProcesulLegislativ/Proiectedeactelegislative/tabid/61/LegislativId/3183/language/ro-RO/Default.aspx