

**ANALIZA COMPARATIVĂ A LEGISLAȚIEI PRIVIND PRODUCEREA,
IMPORTUL, COMERCIALIZAREA SAU PUNEREA ILEGALĂ LA
DISPOZIȚIE A MIJLOACELOR TEHNICE SAU PRODUSELOR PROGRAM
CONFORM ART. 260 COD PENAL AL REPUBLICII MOLDOVA**

**COMPARATIVE ANALYSIS OF LEGISLATION ON THE PRODUCTION, IMPORT,
MARKETING, OR ILLEGAL PROVISION OF TECHNICAL MEANS OR SOFTWARE
PRODUCTS ACCORDING TO ARTICLE 260 OF THE PENAL CODE OF THE REPUBLIC
OF MOLDOVA**

**LISNIC Sergiu,
doctorand, Academia „Ștefan cel Mare” a MAI
ORCID: 0009-0000-1406-7052
Email: lisnicsergiu@gmail.com**

Abstract

The rapid advancement of technology in recent decades has not only brought significant innovations but also new legal challenges, particularly in the realm of cybercrime. This comparative analysis examines the legislation concerning the production, import, marketing, or illegal provision of technical means or software products, specifically in accordance with Article 260 of the Penal Code of the Republic of Moldova. By comparing the national legislations of various countries, including Germany, Romania, the Netherlands, the United Kingdom, and China, this study aims to identify the differences and similarities in legislative approaches to combat cybercrime. The analysis highlights the effectiveness of these measures, the jurisdictional challenges, and the need for international cooperation to address the transnational nature of cyber offenses. It also discusses the impact of significant international legal frameworks, such as the Council of Europe's Convention on Cybercrime, on shaping national laws. The findings underscore the importance of adaptive and robust legal responses to the evolving landscape of cyber threats, emphasizing the need for a cohesive global legal framework to effectively prevent and combat cybercrime.

Keywords: *Cybercrime, comparative legislation, legal framework, malware, software products, technical means.*

Ascensiunea tehnologiei în ultimele decenii a adus cu sine nu doar inovații semnificative, ci și noi provocări legale, în special în domeniul criminalității informatice. În acest context, anii 1980 au marcat un moment decisiv în recunoașterea și abordarea acestor provocări la nivel internațional. Inițiativele timpurii ale Organizației pentru Cooperare și Dezvoltare Economică (OECD) au subliniat importanța răspunsului legal la aceste noi forme de criminalitate. Cu toate acestea, un pas semnificativ în consolidarea eforturilor internaționale a fost realizat prin Recomandarea No. R (89) 9, adoptată de Consiliul Europei în septembrie 1989 [1]. Acest document a stabilit un cadru pentru definirea și combaterea infracțiunilor informatice, subliniind necesitatea unei cooperări și armonizări legale între statele membre pentru a adresa caracterul transfrontalier și complex al acestor infracțiuni.

Recomandarea menționată a evidențiat necesitatea definirii clare a infracțiunilor informatice, incluzând accesul neautorizat, interceptarea datelor fără permisiune, distrugerea intenționată a datelor și sistemelor informatice precum și alte forme a criminalității informatice.

Problema jurisdicțională care guvernează infracțiunile cibernetice a făcut ca autoritatea legală a fiecărei țări să acționeze ca un atlet care aleargă pe o pistă într-un stadion, în timp ce infractorii cibernetici sunt colegii și spectatorii, analizând modul în care autoritatea aleargă și determinând scurgerile și slăbiciunile. Indiferent de câte ture aleargă autoritatea pe pistă, rezultatul este întotdeauna același: să ajungă la linia de finisaj doar pentru a descoperi că este din nou punctul de plecare [2, p.404].

Astfel, în decursul timpului, Consiliul Europei a inițiat numeroase demersuri de reglementare a activității în spațiul cibernetic, acestea răspunzând în principal, la acea vreme, nevoilor juridice corespunzătoare dezvoltării tehnologice de moment [3, p.85].

Prin promovarea unor directive clare pentru legislațiile naționale, Consiliul Europei a încurajat statele să adapteze și să îmbunătățească răspunsurile legale la aceste infracțiuni emergente, asigurându-se că sistemul juridic poate face față rapidității schimbărilor tehnologice, având ca exemplu și următoarele recomandări:

Recomandarea R(95)13 - "Privind problemele de drept procesual penal legate de tehnologia informației" - aceasta tratează adaptarea procedurilor penale pentru a răspunde provocărilor tehnologice, asigurând că legislația este adecvată pentru investigarea și procesarea infracțiunilor informatice [4].

Recomandarea R(2001)3 - "Privind furnizarea de servicii judiciare și legale cetățeanului prin utilizarea noilor tehnologii" - recomandarea îndrumă statele să utilizeze tehnologia pentru a îmbunătăți accesul la serviciile judiciare, inclusiv în cazurile de criminalitate informatică [5].

După stabilirea unui cadru inițial prin recomandările menționate anterior, un pas semnificativ în evoluția legislației internaționale privind criminalitatea informatică a fost "Convenția de la Budapesta privind criminalitatea cibernetică", cunoscută și sub numele de *Convenția Consiliului Europei privind criminalitatea cibernetică* [6]. Aceasta reprezintă primul tratat internațional care abordează infracțiunile informatice și probele electronice la un nivel global, stabilind standarde comune pentru legile naționale pentru a combate aceste infracțiuni.

În acest context, răspunsul legislativ la infracțiunile informatice nu a fost doar o necesitate juridică, ci și o reflectare a evoluției înțelegerii și abordării securității cibernetice la nivel global. Acesta a pus bazele pentru dezvoltări ulterioare în politica de securitate cibernetică și a influențat profund legislația națională și internațională în deceniile care au urmat.

În timp ce Convenția de la Budapesta a oferit un cadru esențial pentru standardele internaționale în combaterea criminalității cibernetice, este interesant de observat cum diferite națiuni au adoptat aceste norme la contextele lor specifice.

Următoarea analiză va explora și compara legislațiile naționale ale mai multor țări în ceea ce privește producerea, importul, comercializarea sau punerea la dispoziție, sub orice altă formă, în mod ilegal, a mijloacelor tehnice sau produselor program, concepute sau adaptate, în scopul comiterii infracțiunilor informatice. Acest studiu detaliat ne va permite să identificăm nu doar modul în care fiecare stat interpretează și implementează aceste legi, ci și provocările și succesul acestor eforturi în cadrul luptei globale împotriva criminalității cibernetice.

În ceea ce privește infracțiunile legate de malware, jurisdicția extrateritorială și legea extrădării se completează reciproc pentru a funcționa perfect, dar niciodată nu a existat o regulă universală standard care să le guverneze [2, p.403]. Acest vid legislativ permite infractorilor

cibernetici să își aleagă strategic țările sau teritoriile cu legislații mai permissive pentru a comite infracțiuni, profitând astfel de pedepsele mai blânde și de lacunele în cooperarea internațională pentru extrădare.

Analiza comparativă a legislațiilor diferitelor țări privind importul, comercializarea sau punerea la dispoziție a produselor program sau a mijloacelor tehnice este esențială pentru a identifica eficacitatea măsurilor de combatere a infracțiunilor cibernetice la nivel global. Această analiză nu doar că dezvăluie diferențele și similitudinile în abordările legislative, dar și modul în care acestea se aliniază sau contravin normelor internaționale. De exemplu, pedepsele impuse pentru aceste infracțiuni variază semnificativ de la o jurisdicție la alta, influențând direct strategiile infractorilor cibernetici de a alege locații mai permissive pentru activitățile lor ilicite. Mai mult, examinarea detaliată a mecanismelor de aplicare a legii și a cooperării transfrontaliere între statele afectate poate oferi perspective valoroase despre lacunele existente în cadrul legislativ actual și necesitatea unei abordări mai coordonate la nivel internațional. Astfel, această analiză nu numai că sprijină dezvoltarea unor politici de securitate cibernetică mai robuste, ci și contribuie la formarea unui cadru legislativ global mai coeziv și mai eficient în prevenirea și combaterea criminalității informatice.

Legislația țărilor europene, în general, reflectă un angajament comun în implementarea unor norme stricte și coerente pentru combaterea infracțiunilor legate de malware, arătând o tendință spre unificarea practicilor de securitate cibernetică pe continent.

Astfel, în contextul juridic german, secțiunea § 202c din Codul Penal (StGB) joacă un rol crucial în combaterea crimelor cibernetice, adresându-se direct pregătirii activităților de spionaj și interceptare a datelor. Această secțiune este esențială pentru înțelegerea mecanismelor prin care legislația germană sancționează activitățile preliminare ce pot facilita accesul neautorizat la date informatice protejate.

Conform § 202c StGB, este considerată infracțiune pregătirea mijloacelor necesare pentru comiterea de infracțiuni specificate în secțiunile 202a (Accesul neautorizat la datele protejate) și 202b (Interceptarea ilegală a datelor). Astfel, legea penalizează producerea, achiziția, vânzarea, transmiterea, distribuirea sau punerea la dispoziție în orice formă a:

1. Parolelor sau altor coduri de securitate care facilitează accesul ilegal la date.
2. Software-ului conceput explicit pentru a comite astfel de acte ilegale [7].

Acest cadru legal reflectă preocuparea constantă a legiuitorului german pentru protecția datelor și sistemelor informatice, oferind un instrument eficient în prevenirea atacurilor cibernetice. Pedepsa prevăzută pentru încălcarea acestei secțiuni include închisoare de până la doi ani sau amendă, subliniind seriozitatea percepută a acestor pregătiri infracționale.

În cadrul legislativ global pentru combaterea criminalității cibernetice, Codul Penal Român se distinge printr-o abordare particularizată asupra infracțiunilor legate de dispozitivele și programele informatice. Articolul 365 din Codul Penal Român evidențiază specificitatea acestui cadru prin incriminarea producției, distribuției, importului sau oricărei forme de punere la dispoziție a dispozitivelor sau programelor informatice concepute pentru comiterea infracțiunilor, precum și a parolelor și codurilor de acces [8]. Notabil este faptul că legislația română include de asemenea pedepsirea deținerii acestor elemente, un aspect care nu este întotdeauna prezent în legislațiile altor țări sau chiar în Convenția de la Budapesta.

Comparativ, legislațiile din Germania și Republica Moldova, deși riguroase în abordarea infracțiunilor cibernetice, nu accentuează în mod explicit penalizarea deținerii dispozitivelor sau datelor de acces în scopul comiterii infracțiunilor, un aspect care este însă prezent în Articolul 365

din Codul Penal Român. Această diferențiere subliniază o precauție suplimentară în cadrul legislativ român, reflectând o strategie proactivă în prevenirea criminalității cibernetice.

Atât în legislația română, cât și în legislația germană, precum și în Convenția de la Budapesta, găsim articole care incriminează într-un singur context modalitățile normative de producere, import, distribuție sau punere la dispoziție atât a dispozitivelor și programelor informatice destinate comiterii infracțiunilor cibernetice, cât și a parolelor, codurilor de acces sau alte date informatice care facilitează accesul la sisteme informatice. Această integrare într-un singur articol a multiplelor modalități de comitere a infracțiunilor reflectă o abordare unificată și comprehensivă, menită să acopere spectrul larg al mijloacelor prin care se poate realiza ca exemplu accesul neautorizat.

Pe de altă parte, Codul Penal al Republicii Moldova separă aceste aspecte în articole diferite. De exemplu, Articolul 260⁴ se concentrează exclusiv pe producerea, importul, comercializarea sau punerea la dispoziție a parolelor, codurilor de acces sau a datelor similare, tratând separat de art. 260, care se referă la producerea, importul, comercializarea sau punerea la dispoziție a mijloacelor tehnice sau produselor program [9]. Această segregare poate oferi claritate și specificitate fiecărui tip de infracțiune cibernetică, dar poate și să fragmenteze abordarea legislativă, posibil complicând aplicarea și interpretarea legii.

Unificarea infracțiunilor sub un singur articol precum în legislațiile menționate mai sus, poate facilita o mai bună înțelegere și o aplicare mai coerentă a legii, în timp ce separarea clară a tipurilor de infracțiuni în legislația din Republic Moldova poate ajuta la specificarea măsurilor punitive și la focalizarea pe tipuri particulare de infracțiuni cibernetice

Trecerea de la o jurisprudență la alta în discuția despre legislația anti-cibernetică evidențiază diversitatea abordărilor și complexitatea provocărilor pe care le întâmpină fiecare stat în parte. În Olanda, un exemplu notabil de răspuns legislativ la aceste provocări este reprezentat de Articolul 139d, paragraful 2 din Codul Penal Olandez [10]. Acesta stabilește un cadru legal strict pentru gestionarea și penalizarea utilizării neautorizate a tehnologiei în scopuri infracționale, ilustrând angajamentul țării pentru protecția securității cibernetice.

Conform acestui paragraf, este considerată infracțiune producerea, vânzarea, achiziționarea, importul, distribuția, punerea la dispoziție sau deținerea unui dispozitiv tehnic adaptat sau proiectat primordial pentru comiterea infracțiunilor descrise în articolele 138ab(1), 138b, sau 139c, prevăzând închisoare de până la un an sau amendă de categoria a patra pentru infracțiunile specificate.

Articolul 138ab(1) tratează infracțiunile de hacking, definind ilegalitatea accesului neautorizat la sistemele informatice. Articolul 138b din Codul Penal Olandez specifică că orice persoană care intenționează și ilegal împiedică accesul la sau utilizarea unui dispozitiv sau sistem informatizat prin oferirea sau trimiterea de date către acesta este pasibilă de pedeapsă. Această infracțiune poate include atacurile de tip denial of service (DoS) și distributed denial of service (DDoS) cunoscute și sub numele de "e-bombing", care sunt forme de atac cibernetic ce implică inundarea unui sistem cu trafic excesiv sau date, în scopul de a-l face inoperabil pentru utilizatorii săi legitimi. Articolul 139c se concentrează pe interceptarea ilegală a comunicațiilor, abordând problema ascultării sau înregistrării neautorizate a datelor [10].

Această abordare oferă claritate juridică și facilitează interpretarea și aplicarea legii de către autoritățile judiciare. În contrast, Republica Moldova adoptă o strategie mai cuprinzătoare, unde un singur articol, cum ar fi art. 260 Cod Penal al R.M., poate acoperi o gamă largă de infracțiuni informatice, de la accesul ilegal la date până la fraudă informatică.

Ambele abordări legislative sunt conformate cu cerințele Convenției de la Budapesta, fiecare având avantajele și dezavantajele sale. Olanda, cu specificitatea sa, poate limita necesitatea modificărilor legislative frecvente, în timp ce abordarea Republicii Moldova poate facilita adaptarea rapidă la noile provocări în domeniul securității cibernetice. Totuși, complexitatea și diversitatea amenințărilor cibernetice pot impune ajustări legislative continue pentru a menține eficacitatea răspunsului juridic.

Comparând abordările legislative ale Olandei și Republicii Moldova, se observă că eficacitatea legislației în combaterea criminalității cibernetice nu depinde numai de conținutul legilor, ci și de modul în care acestea sunt implementate și adaptate la contextul tehnologic și social actual. Integrarea flexibilă și reactivă a noilor amenințări cibernetice în legislația națională este crucială pentru protecția eficientă împotriva infracțiunilor informatice.

În comparație cu alte jurisdicții internaționale, putem menționa și despre legislația Chinei privind criminalitatea informatică, așa cum este detaliată în Articolul 286 din Codul Penal, adoptă o abordare severă față de răspândirea intenționată a produsului program și anume a software-ului dăunător. Textul legii stipulează că: ”Cine încalcă reglementările statului și creează sau răspândește viruși informatici și alte programe care sabotează funcționarea normală a sistemului informatic și cauzează consecințe grave, va fi pedepsit cu până la cinci ani de închisoare; în cazuri deosebit de grave, pedeapsa poate fi de nu mai puțin de cinci ani” [11]. Aceasta evidențiază angajamentul ferm al Chinei de a combate infracțiunile legate de software, subliniind gravitatea cu care astfel de acte sunt tratate, reflectând o politică de toleranță zero față de aceste comportamente dăunătoare.

Analiza comparativă între diverse jurisdicții arată că există discrepanțe considerabile în magnitudinea pedepselor pentru utilizarea de malware. [wang, pag. 10]

Potrivit lui Ș. Daneș și V. Papadopol ”individualizarea pedepsei este operația de adaptare a pedepsei în raport cu fiecare infracțiune concretă și cu fiecare infractor în parte”[12, p.68]. Această abordare este esențială pentru a asigura că pedeapsa este proporțională cu gravitatea faptei și cu circumstanțele personale ale celui condamnat, reflectând astfel principiile de dreptate și echitate în aplicarea legii.

De-a lungul timpului, pedeapsa a fost utilizată pentru a combate infracțiunile. Diferiți cercetători au scris despre perspectivele filosofice ale pedepsei, proces care a dezvoltat diverse teorii, cunoscute în lumea modernă ca teorii ale pedepsei. Acestea includ teoria retributivă, teoria utilitaristă, teoria reabilitării, teoria restaurativă și teoria descurajării. Este important de menționat că aceste teorii nu sunt exclusiv separate; diferite societăți și sisteme juridice adesea aplică o combinație a acestor abordări. Factorul care variază este datorat naturii infracțiunii și protecției necesare. Filosofia pedepsei este întotdeauna deschisă pentru deliberări privind mecanismul cel mai potrivit pentru gestionarea infracțiunilor [13, p.2].

În contextul unei analize globale asupra pedepselor aplicate infracțiunilor cibernetice, Regatul Unit se distinge prin abordarea sa detaliată a legilor sale. Sub Computer Misuse Act 1990, amendat prin Police and Justice Act 2006, legislația britanică tratează cu seriozitate infracțiunile de modificare neautorizată a informațiilor din sistemele informatice. Astfel, Secțiunea 3A abordează „Crearea, furnizarea sau obținerea de articole pentru utilizare în infracțiuni de utilizare abuzivă a computerelor”. Aceasta specifică că este o infracțiune să furnizezi sau să obții orice articol „știind că este destinat utilizării în cursul sau în legătură cu comiterea unei infracțiuni de utilizare abuzivă a computerului”. „Articolul” aici se referă la orice program software sau orice altă dată care este folosită pentru a comite o infracțiune, inclusiv software-ul de hacking și alte instrumente similare [14].

Legislația Regatului Unit, prevede pedepse de până la doi ani de închisoare pentru infracțiuni legate de utilizarea neautorizată a computerelor, inclusiv manipularea programelor malițioase.

Conform L. Dumneanu ”În Anglia, relativ la misiunea pedepsei penale au fost remarcate trei teorii de bază:

- a) pedeapsa este o răsplată;
- b) pedeapsa este un mijloc de intimidare;
- c) pedeapsa este un mijloc de corectare a condamnatului” [15, p. 112].

Prima teorie, cea a pedepsei ca răsplată, implică ideea de retribuție, adică aplicarea unei pedepse proporționale cu gravitatea infracțiunii comise. În cazul infracțiunilor informatice, unde daunele pot varia considerabil, acest principiu asigură că pedeapsa reflectă în mod adecvat prejudiciul adus societății.

A doua teorie, pedeapsa ca mijloc de intimidare, subliniază rolul disuasiv al legislației. Deși pedepsele pentru producerea și comercializarea ilegală a software-ului pot părea moderate — adesea limitate la maximum doi ani de închisoare — acestea sunt concepute pentru a descuraja pe oricine ar lua în considerare angajarea în astfel de activități ilegale, demonstrând astfel angajamentul statului împotriva infracțiunilor cibernetice.

În final, teoria corectării condamnatului este de asemenea pivotantă. Legislația își propune să reintegreze infractorul în societate ca membru responsabil, ceea ce este crucial în cazul infracțiunilor tehnologice, unde infractorii pot adesea să-și redirectioneze aptitudinile către activități licite post-condamnare.

În ansamblu, chiar dacă pedeapsa de până la doi ani poate părea inițial blândă, ea este deliberat structurată pentru a echilibra aceste trei scopuri fundamentale ale pedepsei penale. Prin acest echilibru, legislația engleză își propune nu doar să pedepsească, dar și să prevină recidiva și să promoveze reforma, subliniind o abordare pragmatică și echilibrată în fața infracțiunilor cibernetice.

În comparație cu legislația Regatului Unit, Codul Penal Olandez specifică pedepse relativ moderate, cu închisoare de până la un an sau amendă de categoria a patra pentru distribuirea și utilizarea software-ului malițios, Germania și România oferă pedepse de până la doi, respectiv trei ani de închisoare pentru astfel de infracțiuni, iar Codul Penal din Republica Moldova prevede pedepse mai severe, cu sancțiuni ce variază între 2 și 5 ani de închisoare pentru infracțiuni similare, indicând o abordare mai aspră.

Conform art. 13 din Convenția Consiliului Europei privind criminalitatea cibernetică ”fiecare stat parte este obligat să adopte măsuri legislative și alte măsuri necesare pentru a asigura că infracțiunile penale stabilite în conformitate cu Articolele 2 până la 11 sunt pedepsibile prin sancțiuni eficace, proporționale și descurajante, care includ privarea de libertate. Acest cadru de sancțiuni este conceput pentru a asigura un răspuns adecvat și riguros la infracțiunile cibernetice, subliniind necesitatea unei abordări ferme și corespunzătoare în legislația națională a statelor semnatare” [6].

În Republica Moldova, pedepsele severe impuse pentru infracțiunile legate de software și tehnologia informației pot fi explicate prin mai mulți factori care reflectă caracteristicile socio-politice și prioritățile de securitate națională ale țării:

Protecția infrastructurii critice: legislația Republicii Moldova impune pedepse severe pentru infracțiunile legate de software și tehnologia informației, recunoscând impactul devastator pe care acestea le pot avea asupra infrastructurilor critice. Severitatea pedepselor reflectă necesitatea de a proteja serviciile esențiale și structurile economice vitale ale națiunii, de la bănci la sisteme

guvernamentale, care sunt adesea ținte ale atacurilor cibernetice. Acesta este un efort direct de a asigura că infrastructurile cheie sunt protejate împotriva perturbărilor care ar putea paraliza funcționarea societății.

Impactul legislației asupra comportamentului societal: legislația cu privire la criminalitatea cibernetică în Republica Moldova este proiectată nu doar pentru a proteja resursele naționale, ci și pentru a modela comportamentul societal. Pedepsele stabilite vizează atât prevenirea infracțiunilor viitoare, cât și promovarea unei culturi de responsabilitate și conștientizare în utilizarea tehnologiilor. Prin aceasta, se urmărește o reducere a incidentelor de criminalitate cibernetică, încurajând totodată practici sigure și etice în rândul populației și al companiilor.

Printre jurisdicțiile cu cele mai severe pedepse, SUA adoptă unele dintre cele mai dure sancțiuni pentru infracțiunile legate de malware. În Statele Unite, legislația care abordează distribuția de software malițios este detaliată în Computer Fraud and Abuse Act (CFAA), codificată sub 18 U.S.C. § 1030. Mai specific, secțiunea 1030(a)(5)(A) prevede că orice persoană care transmite intenționat un program, informație, cod sau comandă, și ca rezultat al unei astfel de conduite, cauzează daune neautorizate unui computer protejat, se confruntă cu pedepse care pot ajunge până la 10 ani de închisoare pentru o primă acțiune ilegală și până la 20 de ani pentru infracțiuni subsecvente [16].

Aceste diferențe subliniază diversitatea răspunsurilor legislative și importanța adaptării legilor la contextul specific al fiecărei țări în ceea ce privește combaterea programelor malițioase și a altor amenințări cibernetice. Fiecare jurisdicție evaluează severitatea acestor acte în mod diferit, ajustând sancțiunile pentru a reflecta riscurile percepute și impactul asupra securității informatice naționale.

În analiza legislațiilor penale ale diferitelor țări, un aspect remarcabil este utilizarea terminologiei specifică pentru descrierea infracțiunilor legate de răspândirea mijloacelor tehnice sau a produselor program. Codul Penal al Republicii Moldova preferă termenul „comercializare”, care subliniază tranzacțiile economice implicând dispozitivele și programele informatice concepute pentru comiterea infracțiunilor. Această alegere de terminologie reflectă o preocupare pentru aspectele economice ale infracțiunilor cibernetice, concentrându-se pe fluxurile financiare ilegale care susțin piața neagră a tehnologiei periculoase.

Pe de altă parte, legislațiile din România, Olanda, Germania, precum și Convenția de la Budapesta, utilizează termenul „distribuție” pentru a descrie acțiunile de răspândire a unor astfel de dispozitive sau programe. Prin includerea atât a vânzării directe cât și a distribuirii gratuite sau a partajării între diverse entități, termenul acoperă o gamă largă de modalități prin care software-ul și dispozitivele periculoase pot fi răspândite în societate. Această abordare legislativă recunoaște că dispozitivele și produsele program concepute pentru a facilita activități ilegale pot circula prin canale care nu implică neapărat tranzacții comerciale. De exemplu, un individ ar putea să distribuie gratuit un produs program/ software de hacking prietenilor sau cunoscuților, sau un grup de infractori cibernetici, ar putea să partajeze între ei unelte și resurse fără a efectua o tranzacție financiară directă. Aceste scenarii, deși lipsite de un profit financiar imediat, contribuie la proliferarea amenințărilor cibernetice și pot avea impacturi semnificative asupra securității informatice.

Prin urmare, termenul de „distribuție” subliniază importanța unui efort concertat de a controla nu doar punctele de vânzare comercială, ci și alte forme de transfer de material informatic periculos. Legislația care include acest termen vast și inclusiv demonstrează o înțelegere aprofundată a naturii distribuite și adesea descentralizate a infracțiunilor cibernetice. Astfel, statele

pot implementa măsuri de control și prevenție mai eficace, capabile să adreseze atât schimburile comerciale cât și pe cele non-comerciale, închizând astfel porțile prin care tehnologiile periculoase ar putea ajunge în mâini greșite.

Această diferență în alegerea terminologiei nu este doar o subtilitate lingvistică, ci indică o diferențiere semnificativă în abordarea legislativă. În timp ce Republica Moldova vizează direct componenta comercială, punând accent pe interceptarea și penalizarea fluxurilor financiare ilegale, abordările României și Germaniei, aliniate cu directivele Convenției de la Budapesta, au un scop mai larg de a limita accesul și răspândirea tehnologiilor care pot fi utilizate pentru comiterea infracțiunilor cibernetice. Astfel, această analiză comparativă evidențiază modul în care diferitele jurisdicții își configurează răspunsurile legislative la provocările securității cibernetice, reflectând prioritățile naționale și angajamentul față de cooperarea internațională în combaterea criminalității informatice.

În concluzie, acest studiu comparativ subliniază importanța adaptării continue a legislațiilor naționale la dinamica în schimbare a criminalității cibernetice, un fenomen global care transcende granițele tradiționale ale jurisdicției. Prin examinarea detaliată a legislațiilor specifice din diverse țări, reiese clar că, deși există o tendință de armonizare sub egida convențiilor internaționale cum ar fi Convenția de la Budapesta, abordările naționale rămân diverse și sunt profund influențate de contextele culturale, economice și politice locale. Aceasta diversitate necesită o colaborare internațională mai strânsă și un dialog continuu pentru a asigura nu doar conformitatea cu standardele globale, dar și eficacitatea în combaterea amenințărilor cibernetice care evoluează rapid. Astfel, este esențial ca cercetarea și politica legislativă să rămână agile, adaptându-se la noi provocări și integrând tehnologii emergente în strategiile de prevenire și combatere a infracțiunilor informatice. În acest mod, se poate spera la consolidarea unui cadru juridic global care să fie nu doar reactiv, ci și anticipativ, în fața criminalității cibernetice.

Referințe bibliografice

1. Consiliul Europei. (1989). "Recomandarea Nr. R(89)8 a Comitetului de Miniștri către statele membre privind protecția provizorie acordată de instanță pe probleme administrative" (adoptată de Comitetul de Miniștri la 13 septembrie 1989 la reuniunea cu nr. 428 a Delegaților Miniștrilor). Strasbourg: Consiliul Europei. [accesat: 05.04.2024]. Disponibil: <https://www.oas.org/juridico/english/89-9&final%20Report.pdf>.
2. Rahman R. "Legal jurisdiction over malware-related crimes: From theories of jurisdiction to solid practical application." *Computer Law & Security Review*, vol. 28, no. 4, August 2012, pp. 403-415. <https://doi.org/10.1016/j.clsr.2012.03.004>
3. Maxim Dobrinou, *Infracțiuni în domeniul informatic*, Editura C.H. Beck, 2006, București, p. 85.
4. Consiliul Europei. (1995). "Recomandarea Nr. R (95) 13 a Comitetului de Miniștri către statele membre privind problemele de drept procedural penal legate de tehnologia informației" (adoptată de Comitetul de Miniștri la 11 septembrie 1995 la cea de-a 543-a reuniune a Delegaților Miniștrilor). Strasbourg: Consiliul Europei. [accesat: 05.04.2024]. Disponibil: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016804f6e76>.

5. Consiliul Europei. (2001). "Recomandarea Rec(2001)3 a Comitetului de Miniștri către statele membre privind furnizarea de servicii juridice și judiciare cetățeanului prin utilizarea noilor tehnologii" (adoptată de Comitetul de Miniștri la 28 februarie 2001 la cea de-a 743-a reuniune a Delegaților Miniștrilor). Strasbourg: Consiliul Europei. [accesat: 05.04.2024]. Disponibil: https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=09000016805e2aa7.
6. Convenția Consiliului Europei privind criminalitatea informatică, semnată la Budapesta la 23 noiembrie 2001 și ratificată prin Legea R.M. nr. 6 din 02.02.2009, în vigoare din 01.09.2009.
7. Codul Penal al Republicii Federale Germania din 01 ianuarie 1985 (Strafgesetzbuch - StGB). [accesat: 07.04.2024]. Disponibil: https://www.gesetze-im-internet.de/englisch_stgb/.
8. Codul Penal al României din 24.07.2009. Monitorul Oficial al României, Partea I, nr. 510.
9. Codul penal al Republicii Moldova. Nr. 985-XV din 18.04.2002 Republicat. În: Monitorul Oficial al R.Moldova, 14.04.2009, nr.72-74/195, Monitorul Oficial al R. Moldova, 13.09.2002, nr.128- 129/1012.
10. Codul penal al Olandei din 03.03.1881, cu ultimele modificări și completări din 01.01.2024. [accesat: 01.05.2024]. Disponibil: <https://wetten.overheid.nl/BWBR0001854/2024-01-01>.
11. Codul penal al Chinei din 14.03.1997. [accesat: 01.05.2024]. Disponibil: <https://www.warnathgroup.com/wp-content/uploads/2015/03/China-Criminal-Code.pdf>.
12. Daneș Șt., Papadopol V. Individualizarea judiciară a pedepselor. Ediția a II-a revizuită. – București: Editura Juridică, 2005, p. 68.
13. Wang Y., Liu X., Zhou Y., & Yilmaz A. (2023). How to punish cyber criminals: A study to investigate the target and consequence based punishments for malware attacks in UK, USA, China, Ethiopia & Pakistan. *Heliyon*, 9(3), e14172. <https://doi.org/10.1016/j.heliyon.2023.e14172> [accesat: 02.05.2024]. Disponibil: <https://www.sciencedirect.com/science/article/pii/S2405844023100314>.
14. Actul privind Tranzacțiile Frauduloase din Regatul Unit. (1990). [accesat: 01.05.2024]. Disponibil: <https://www.legislation.gov.uk/ukpga/1990/18/contents>.
15. Dumneanu L. "Conceptul de pedeapsă în dreptul penal comparat." Studia Universitatis, Revista Științifică a Universității de Stat din Moldova, 2007, nr. 3, p. 112. [accesat: 02.05.2024]. Disponibil: <https://social.studiamsu.md/wp-content/uploads/2007/01/22.-p.112-115.pdf>.
16. Legislația federală din Statele Unite (The United States Code) specific Titlul 18, Secțiunea 1030. [accesat: 01.05.2024]. Disponibil: [https://uscode.house.gov/view.xhtml?req=\(title:18%20section:1030%20edition:preli\)](https://uscode.house.gov/view.xhtml?req=(title:18%20section:1030%20edition:preli)).