CRIMINALITATEA CIBERNETICĂ – CONSECINŢĂ A PROGRESULUI TEHNOLOGIC

Alexandrina RUSU,

studentă, anul IV, Facultatea de Drept, Universitatea de Stat din Moldova

CZU: 343.9:004.8:343.346.8 E-mail: rusu.alexa10@gmail.com

În era digitală contemporană, criminalitatea cibernetică s-a transformat dintr-un fenomen marginal într-o componentă inevitabilă a progresului tehnologic accelerat, manifestându-se tot mai frecvent în toate domeniile societății moderne. Dezvoltarea rapidă a tehnologiei informației, a comunicațiilor și a infrastructurilor digitale a generat o expansiune exponențială a interconectivității globale, însă această interconectivitate a venit la pachet cu noi forme de vulnerabilitate. Spațiul virtual – odinioară perceput ca o zonă de creativitate, inovație și libertate nelimitată – a suferit o metamorfoză profundă, devenind un teren ambiguu și adesea periculos, în care oportunitățile tehnologice se împletesc cu riscuri majore, greu de anticipat sau de gestionat eficient. **Astăzi, criminalitatea informatică nu mai poate fi considerată o simplă abatere izolată sau o excepție rară, ci trebuie înțeleasă ca o amenințare sistemică, cu un impact profund asupra securității societății contemporane.** Aceasta afectează în mod direct nu doar infrastructurile informatice și bazele de date, ci și echilibrul economic, stabilitatea politică, siguranța persoanelor și, nu în ultimul rând, sănătatea psiho-socială a indivizilor expuși.

Atacurile cibernetice pot provoca prejudicii uriașe, de la furturi de identitate și fraude bancare până la compromiterea datelor critice din instituții publice sau private. În plus, prin manipularea informației sau propagarea dezinformării, se pot induce stări de incertitudine și instabilitate în rândul populației, cu efecte directe asupra încrederii în instituțiile statului și în mecanismele democratice. **În acest context, devine evident faptul că infracționalitatea cibernetică nu reprezintă doar o provocare pentru sistemele de justiție penală, ci și un factor de risc cu implicații extinse în plan economic, social și geopolitic.** Securitatea cibernetică, așadar, nu mai este doar o preocupare tehnică a specialiștilor IT, ci o prioritate strategică la nivel național și internațional, impunând o colaborare strânsă între autorități, companii, instituții academice și cetățeni. Doar printr-un efort colectiv și bine coordonat se poate construi un cadru eficient de prevenire, detectare și combatere a acestui tip de criminalitate, care amenință să devină una dintre cele mai complexe și imprevizibile forme de deviere din secolul XXI.

Diversitatea formelor prin care se manifestă criminalitatea cibernetică – de la fraude informatice și furturi de identitate, la atacuri ransomware, escrocherii cu criptomonede sau manipulări prin inteligență artificială – reflectă capacitatea acestui feno-

men de a se adapta și prolifera într-un ritm care depășește reacția tradițională a sistemelor juridice [1, p.5]. Spațiul digital nu cunoaște frontiere clasice, iar lipsa granițelor fizice face ca infracțiunile comise în Republica Moldova să aibă autori în alt colț al lumii, ceea ce complică investigațiile și aplicarea legii.

Este evident că inovația tehnologică, deși esențială pentru progres, produce efecte secundare care generează insecuritate. Așa cum s-a afirmat în literatura de specialitate, „noile tehnologii sunt pregătite să cucerească lumea și să modifice realitatea pe care o cunoșteam până acum” [2]. În acest proces de transformare, drepturile fundamentale, precum viața privată, integritatea datelor sau libertatea de exprimare, sunt frecvent puse la încercare. Mai mult, apariția și dezvoltarea inteligenței artificiale și a sistemelor autonome ridică probleme juridice de o complexitate fără precedent – de la definirea răspunderii pentru acțiuni automate până la stabilirea limitelor morale și legale ale utilizării algoritmilor în domenii precum justiția sau medicina [3]. Această criză normativă este alimentată de decalajul dintre ritmul accelerat al progresului tehnologic și lentoarea procesului legislativ. Pe măsură ce sistemele informatice devin tot mai sofisticate, iar interdependențele globale cresc, răspunsul juridic clasic se dovedește tot mai inadecvat. După cum afirmă unii autori, „dezvoltările tehnologice [...] ridică întrebări fundamentale cu privire la aplicabilitatea normelor tradiționale într-un mediu digitalizat”[4,p.16].

Evoluția cronologică a tehnologiei și reacția juridică aferentă reflectă clar acest decalaj. Transformările profunde generate de digitalizare în ultimele trei decenii au remodelat nu doar societatea, ci și natura criminalității. Spațiul cibernetic, odinioară marginal, a devenit scena principală a interacțiunilor umane, dar și a noilor forme de pericol juridic. Accesibilitatea globală a Internetului, începând cu anii ’90, a deschis calea unei conectivități fără precedent, dar și a unui vid normativ în fața fenomenelor emergente. Atacul informatic global cunoscut sub numele „ILOVEYOU” din anul 2001 a fost unul dintre primele semnale de alarmă asupra vulnerabilității spațiului digital, determinând adoptarea **Convenției de la Budapesta privind criminalitatea informatică** – primul instrument internațional cu forță juridică în acest domeniu [5]. Ulterior, apariția rețelelor sociale (2005), extinderea criptomonedelor (2009), dezvoltarea Big Data (2012) și utilizarea inteligenței artificiale (din 2016) au transformat radical natura riscurilor informatice. Fiecare inovație a venit cu beneficii tehnologice, dar și cu provocări juridice de proporții: de la manipularea datelor și atacurile asupra vieții private, până la imposibilitatea de a defini răspunderea penală într-un context algoritmic. Intrarea în vigoare a **Regulamentului general privind protecția datelor (GDPR)** în 2018 a constituit o încercare a Uniunii Europene de a uniformiza standardele de protecție, însă limitele sale sunt evidente în fața avansului accelerat al fenomenelor precum Internet of Things (IoT) sau AI generativ, utilizat masiv, începând cu 2023 (ex.ChatGPT).

Această succesiune istorică a transformărilor digitale evidențiază cu o acuitate tot mai pronunțată existența unui decalaj constant și adesea alarmant între ritmul alert al inovației tehnologice și capacitatea sistemului juridic de a

reacționa adecvat și eficient. Tehnologia avansează cu o viteză amețitoare, remodelând nu doar modul în care comunicăm, lucrăm sau ne desfășurăm viața cotidiană, ci și mecanismele prin care se săvârșesc faptele ilicite. În schimb, răspunsul normativ rămâne adesea lent, reactiv, constrâns de proceduri legislative rigide, de interpretări doctrinare conservatoare sau de lipsa unei viziuni juridice ancorate în realitățile digitale. Astfel, între ceea ce tehnologia permite și ceea ce legea reglementează se creează un spațiu de incertitudine juridică, pe care infractorii cibernetici îl exploatează cu abilitate.

Într-un asemenea cadru, teza de licență capătă o relevanță deosebită, reprezentând un demers necesar și oportun în peisajul științific și juridic actual. Lucrarea își propune nu doar o simplă descriere a trăsăturilor criminalității cibernetice, ci o analiză aprofundată a modului în care aceasta reconfigurează paradigmele tradiționale ale dreptului penal și contravențional. Este un apel la conștientizarea imperativului adaptării continue a cadrului juridic – atât în plan normativ, cât și instituțional – pentru a face față provocărilor generate de digitalizare.

Referințe:

1. ZLATI, G. Tratat de criminalitate informatică, vol. 1. București: Ed. Solomon, 2020. 336 p.
2. CĂLUGĂRU, A. Inteligența artificială și impactul ei asupra domeniului juridic. În: next.juridice.ro [accesat: 16 februarie 2025]. Disponibil: https://next.juridice.ro/ai-si-dreptul
3. SHEHLIZA, S. Legal Challenges of Emerging Technologies. arXiv preprint, 2024 [accesat: 16 februarie 2025]. Disponibil: https://arxiv.org/abs/2408.17302
4. ENESCU, F. Criminalitatea informatică: între globalizare și reglementare. Teză de doctorat. București: Universitatea „Nicolae Titulescu”, 2017. 278 p.
5. Council of Europe. Convention on Cybercrime (Budapest Convention). Budapest, 2001. [accesat: 17.02.2025]. Disponibil: https://www.coe.int/en/web/conventions/full-list?module=treaty-detail& treatynum=185

Recomandat
***Alina ȘAVGA**, dr., conf. univ.*