SECURITATEA STATULUI ȘI RESPECTAREA DREPTURILOR OMULUI ÎN ERA DIGITALĂ

STATE SECURITY AND RESPECT FOR HUMAN RIGHTS IN THE DIGITAL AGE

CZU: 342.7:004.6.056.5:351.751 **DOI:** https://doi.org/10.59295/ssdoed2024.50

Roxana Mihaela MOISOIU[1]

ABSTRACT. *We live in a highly digitized era where access to the latest technologies allows us to access information that we can use both in the sphere of professional concerns and in the sphere of research challenges.*

It is known that Europe as the cradle of civilization in the Balkan Peninsula is the target of a cyber attack every 44 seconds. The statistics are not at all encouraging, as two out of 5 European citizens have experienced cyber security issues, and one out of 8 businesses have been targeted by such attacks.

Romania enjoys a won and confirmed place in the field of digital security. In this sense, our country was chosen to host the European Competence Center in the field of Cyber Security. In the private sector we have one of the largest antivirus companies in the world. But we still have a lot to learn from the highly developed countries that dominate cyber security. Digitization from the perspective of the consequences on the economic level is a particularly complex process because it obviously accelerates the fulfillment of each of the objectives of sustainable development.

However, the advantages and disadvantages of digital technology should not be minimized, especially from the point of view of risks such as the risk of personal data theft, the spread of terrorism and crimes, as well as obvious difficulties regarding the lack of specialization of the global population for new jobs which will be digitized by the disappearance of other jobs.

The use of information technology provides anonymity to users, facilitates the logistical support of criminals and reduces the risk that they will be brought to justice by favoring remote controlled operations.

Analyzing the impact of digitization, both from the point of view of the advantages and the disadvantages it presents, is an obvious necessity, dictated by the economic social political reality existing at the level of the EU as well as at the level of Moldova and Romania. Thus, cyber security must be analyzed and argued in the context of respecting human rights, especially economic rights, which will facilitate a dignified and smooth existence of social welfare.

Keywords: *digital technology, security, cyber security, strategy, social welfare*

REZUMAT. *Trăim într-o eră puternic digitalizată în care accesul la ultimele tehnologii ne permite să accesăm informații pe care le putem folosi atât în sfera preocupărilor profesionale cât și în sfera provocărilor din domeniul cercetării.*

Este cunoscut faptul că, Europa ca leagăn al civilizației din Peninsula Balcanică este ținta unui atac cibernetic la fiecare 44 de secunde. Statistica nu este deloc încurajatoare, deoarece doi

[1] Roxana Mihaela MOISOIU, Drd - U.S.P.E.E. ”Constantin Stere” Moldova – Chișinău, Prof. Colegiul German „Goethe” România – București, ID orcid 0009-0005-0515-0432, roxana_moisoiu@yahoo.com

din 5 cetățeni europeni au avut probleme de securitate cibernetică, iar una din 8 afaceri a fost vizată de asemenea atacuri.

România se bucură de un loc câștigat și confirmat în domeniul securității digitale. Sens în care, țara noastră a fost aleasă să găzduiască Centrul European pentru Competențe în domeniul Securității Cibernetice. În domeniul privat avem una dintre cele mai mari companii antivirus din lume. Însă mai avem multe de învățat de la țările foarte dezvoltate care domină securitatea cibernetică. Digitalizarea din perspectiva consecințelor asupra nivelului economic constituie un proces deosebit de complex deoarece accelerează în mod evident îndeplinirea fiecăruia dintre obiectivele de dezvoltare sustenabilă.

Nu trebuie minimalizate însă avantajele și dezavantajele tehnologiei digitale, mai ales din punctul de vedere al riscurilor precum, risc de furt a datelor personale, de propagarea terorismului și a crimelor, cât și dificultăți evidente privind lipsa de specializare a populației globale pentru noile locuri de muncă care se vor digitaliza prin dispariția altor joburi.

Utilizarea tehnologiei informației oferă anonimatul utilizatorilor, facilitează sprijinul logistic al infractorilor și reduce riscul ca aceștia să fie aduși în fața justiției favorizând realizarea unor operațiuni controlate de la distanță.

Analizarea impactul digitalizării, atât din punctul de vedere al avantajelor cât și al dezavantajelor pe care le prezintă, constituie o necesitate evidentă, dictată de realitatea economică social politică existentă la nivelul UE cât și la nivelul, Moldovei și României. Astfel, trebuie analizată și argumentată securitatea cibernetică în contextul respectării drepturilor omului, în special a drepturilor economice , care să-i faciliteze o existență demnă și lină de bunăstare socială.

Cuvinte-cheie: *tehnologie digitală, securitate, securitate cibernetică, strategie, bunăstare socială*

Motto:

„Noua strategie de securitate cibernetică îi permite, Uniunii Europene să se afirme ca lider în materie de norme și standarde internaționale în spațiul cibernetic și să consolideze cooperarea cu partenerii din întreaga lume pentru a promova un spațiu cibernetic mondial, deschis, stabil și sigur, bazat pe statul de drept, drepturile omului, libertățile fundamentale și valorile democratice.”[1]

Motto:

„The new Cybersecurity Strategy also allows the EU to step up leadership on international norms and standards in cyberspace, and to strengthen cooperation with partners around the world to promote a global, open, stable and secure cyberspace, grounded in the rule of law, human rights, fundamental freedoms and democratic values.”

Viața internațională este într-o perioadă extrem de contradictorie. Manifestarea asimetrică a relațiilor internaționale, complexitatea și dinamismul vieții internaționale a condus la dificultăți ce afectează mediul de securitate. La modul general, securitatea reprezintă unul dintre principiile de bază ale supraviețuirii statului.

În planul securității naționale o atenție deosebită este acordată implementării strategiei de securitate [1, Strategia de securitate cibernetică a României 2022-2027 aprobată prin HG nr 1321- 03.12. 2021] prin actualizarea politicilor publice, cu

[1] https://ec.europa.eu/commission/presscorner/detail/ro/IP_20_2391

scopul realizării unei protecții adecvate valorilor societății în gestionarea riscurilor și vulnerabilităților existente. Pentru o imagine realistă a intereselor naționale și a securității naționale, a contracarării oricăror agresiuni, este imperios necesar să cunoaștem amenințarea.

Politicile publice, ca un garant al democrației trebuie să ofere o abordare interdisciplinară, capabilă să fie aplicată în practică. Liniile de bază ale politicilor publice se reunesc în cadrul strategiilor naționale de apărare, documente ce sunt reevaluate în funcție de mediul politic și social existent, dar și ținând cont de contextul mondial.[2, Legea 58 /14.03.2023 privind securitatea cibernetică a României] Orice eveniment sau conflict în scena actorilor globali, influențează, fără doar și poate, mediul național.

Era digitală a creat virtualizarea politică și socială, a digitalizat relațiile dintre stat și cetățeni, dar și în sfera globală, dintre state. Dacă în trecut conflictele dintre state se dezbăteau în câmpul de luptă, astăzi aceste conflicte se propagă în mediul informatic. Pe măsură ce capacitatea umană a dezvoltat indicatori specifici și tehnologia a căpătat noi însușiri, statul și securitatea națională are noi valențe în domeniul apărării societății.

Noua ordine mondială, polii de putere, conflictele existente, toate acestea arată că ne aflăm la o răscruce a unei noi paradigme de securitate care interacționează în mai multe domenii adaptate la dinamica mediului de securitate.

Războiul este informațional[3, AFD – Actul legislativ privind piețele digitale Consiliul UE 14 septembrie 2022], amenințările emergente au creat premisele evoluției conceptului de cultură de securitate. Cultura de securitate trebuie analizată în contextul în care elementele sale se manifestă în fiecare organizație, în fiecare stat, chiar dacă îmbracă forme specifice. Dezvoltarea societății informaționale a fost creată pentru a crește calitatea vieții.

Un stat funcțional înseamnă o țară sigură care oferă cetățenilor condiții optime pentru un trai decent, în deplină siguranță, care să protejeze valorile și resursele statului de drept.

Securitatea cibernetică, raportată la sectorul tehnologiei informației și telecomunicațiilor în cadrul amplului proces de globalizare și dezvoltare transfrontalieră a mediului online, favorizează și permite derularea sau sprijinirea producerii unor consecințe de natură infracțională. În fapt asistăm, la un atac evident al criminalității cibernetice asupra securității cibernetice ,atât la nivel individual, social, zonal, statal, național, internațional.

Context în care asistăm la dezvoltarea nedorită a structurilor ierarhice clasice ale crimei organizate, ce acționează sub anonimatul utilizatorilor în mediul virtual. Realitatea social economică, juridică și de politică penală își modifică întregul ansamblu de strategii de intervenție și control asupra criminalității cibernetice.

Transformarea societății în era digitalizării (România are un procent de peste 79% dintre cetățeni care utilizează mediul online) securitatea cibernetică preocupă factorii decidenți ai societății. Începând cu anul 2013 securizarea rețelelor și a sistemelor informatice au devenit o prioritate pe agenda statelor europene. [4,https://ec.europa.eu/commission/presscorner/detail/ro/IP_20_2391]

Controlul informațiilor capătă noi dimensiuni, așa cum conflictele transformă raporturile de putere și poziția factorilor de securitate.

În acest mediu complex, securitatea în ansamblul său capătă noi direcții - de reacție și de adaptare.

Strategia națională are ca obiectiv prioritar de asemenea securitatea României, a cetățenilor săi, politicile publice bazându-se pe direcțiile asumate de toate instituțiile publice cu atribuții și responsabilități în domeniul securității țării. Indiferent de riscuri și vulnerabilități putem afirma că o țară funcțională este o țară sigură, chiar și în condițiile în care sunt iminente amenințările cibernetice și de tip hibrid.

În contextul actual instabilitatea din Orientul Mijlociu proiectează amenințări majore în planul securității atât în spațiul european cât și occidental.

Acțiunile informative ostile, canalele de propagandă pro și contra Hamas, respectiv al Israel bulversează opinia publică dând naștere la analize politice continue, a căror derulare in mediul online îmbracă, fără doar și poate, uneori atacuri cibernetice lansate de entități statale și non statale.

Criminalitatea informatică ca și consecință directă a dezvoltării erei digitalizării, înregistrează o tendință ascendentă, evidente fiind activitățile ilicite speciale din aceasta sferă (compromitere de atm- uri, clonarea carduri, acces neautorizate în sistemelor informatice, interceptarea ilegala de date informatice, postare de anunțuri fictive, infectarea sistemelor informatice și chiar utilizarea sau exploatarea criptomonedelor pentru derularea de operațiuni ilicite din zona economică).[5, https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit]

Din perspectiva celor evidențiate mai sus, evoluția în Republica Moldova reprezintă un risc din cauza contrabalansării orientării europene și cea euro-asiatică, facilitând astfel apariția de riscuri în mediul de securitate națională. Un reper asupra căruia trebuie să ne îndreptăm analiza este de ordin economic , în ceea ce privește perpetuarea economică subterană și a corupției, a evaziunii fiscale deoarece toate aceste aspecte au o legătură directă cu precaritatea socială, nivelul de trai scăzut, rata șomajului ridicată, degradarea socială, materială și implicit a demnității umane a fiecărui individ aflat în risc material. Sens în care, capacitatea instituțiilor statului de a evalua și diminua impactul riscurilor și a amenințărilor este limitată de persistența acestor vulnerabilități. Datorită faptului că încă există lacune legislative în domeniul securității naționale din Republica Moldova în contextul agresiunilor informaționale fără precedent asistăm la un fenomen destabilizator cu implicații directe asupra prevenirii contracarării oricărui tip de amenințare.

De asemenea, Moldova se confruntă cu un nivel redus de securitate cibernetică, ca efect direct al vulnerabilităților tehnologice și procedurale ale infrastructurilor deținute de operatorii de comunicații.

O caracteristică evidentă a situației actuale din țara vecină o reprezintă acutizarea decalajului tehnologic și valorificarea insuficientă a noilor tehnologii în domeniile de activitate de ordin strategic.

Decalajele de dezvoltare economică influențează capacitatea statului de a face față schimbărilor climatice și dezvoltării durabile.

Toate aceste aspecte mai sus inserate, afectează atât România cât și statele vecine ei, în următoarele domenii în domeniul educației asistăm la o calitate scăzută a actului educațional, domeniul administrației publice asistăm la deprofesionalizarea datorat unei politizări excesive, iar la nivelul societății civile ne confruntam cu un nivel scăzut al culturii de securitate. Toate acestea au consecință asupra demersurilor conjugate și coerente de modernizare digitalizare și finanțare a proiectelor de infrastructura necesare asigurării armoniei sociale.[6,http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Romanian.pdf]

Este incontestabil avantajul informației electronice și ale sistemului informatic dar există și efecte nocive ale procesului informatic. Infracțiunile informatice sunt acțiuni grave, ce pot pune în pericol valorile apărate de societate, și sunt sancționate de Codul Penal. Acest tip de infracțiuni au un grad ridicat de clandestinitate favorizând câștigul material imediat, în timp ce șansele de a fi descoperiți sunt destul de reduse.

Spațiul virtual a oferit condiții optime pentru o răspândire de amploare a infracționalității. Intervenția neîntârziată a autorităților judiciare în vederea controlului fenomenului se impune ca atare extrem de rapid. [7, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf] Este cunoscut faptul că, prin comiterea de infracțiuni informatice se vizează obținerea unor produse financiare și se pot crea importante prejudicii persoanelor fizice și juridice.[8, Convenția Consiliului Europei privind criminalitatea informatică, Budapesta 2001]

În legislația din Republica Moldova menționăm astfel că prin Legea nr. 6 din 02.02.2009[1] Parlamentul Republicii Moldova a ratificat Convenția Consiliului Europei privind criminalitatea informatică adoptată la Budapesta la 23 noiembrie 2001[2].

În conformitate cu art. 2 al Convenției, Republica Moldova s-a angajat să adopte măsurile legislative și alte măsuri considerate necesare pentru a incrimina ca infracțiune, potrivit dreptului său intern, accesarea intenționată și fără drept. Se poate condiționa incriminarea comiterii infracțiunii.

Prin urmare, legiuitorul din Republica Moldova [9, Codul Penal din Republica Moldova publicat la 14.04 .2009 M.Of nr.72-74] a prevăzut la art. 259 C.P .alin 1 infracțiunea de acces ilegal la informația computerizată(varianta tip).La litera h a aliniatului 2 din art. 259 C.P. legiuitorul a prevăzut a doua variantă tip de infracțiune. În ceea ce privește formele agravante ale acestei infracțiuni sunt prevăzute la b-g alin 2 art.259.

[1] Monitorul Oficial al Republicii Moldova, 2009, nr.37-40.

[2] Convenția Consiliului Europei privind criminalitatea informatică. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Romanian.pdf

În art. 260 C.P. este prevăzută fapta de producere, import, comercializare sau punere la dispoziție în mod ilegal a mijloacelor tehnice sau produselor program.

La art.260 bis C.P. se prevede fapta de interceptare ilegală a unei transmisii de date infoirmatice.260 cu 2 bis se retine fapta de alterarea integrității datelor informatice ținute într-un sistem informatic.

La 260 cu 3 este prevăzută infracțiunea de perturbare a funcționării sistemului informatic. Iar la art.260 cu 4 cp este prevăzută fapta de producere, import, comercializare sau punere ilegală la dispoziție a parolelor codurilor de acces sau a datelor similare. Conform art. 261 C.P. din Republica Moldova legiuitorul prevede fapta de încălcare a regulilor de securitate a sistemelor informatice.

Legiuitorul din Moldova conferă astfel (prin faptele prevăzute la art. mai sus menționate)un spațiu amplu care să apere securitatea informațională prin asigurarea protecției spațiului cibernetic al Republica Moldova. Și nu în ultimul rând interesele de bază ale persoanei, respectiv securitatea informatică individuală constituie un reper care evidențiază preocuparea juridică a legiuitorului prin tragerea la răspundere penală a tuturor acelora care se fac vinovați de săvârșirea acestor infracțiuni.

Dacă analizăm definirea termenilor acestor tipuri de infracțiuni în codul penal român constatăm că nu sunt cuprinse într-o singură grupă, ca în cazul altor infracțiuni ci, se adoptă o anumită logică. În prezent, în Cod penal din România există două grupuri de infracțiuni informatice:

Primul grup - "Fraude comise prin sisteme informatice și mijloace de plată electronice", infracțiunile contra patrimoniului (Titlul II, Capitolul IV din Partea specială) și cuprinde patru infracțiuni, anume "Frauda informatică" (art. 249 C. P.), "Efectuarea de operațiuni financiare în mod fraudulos" (art. 250 C.P.), Operațiuni ilegale cu instrumente de plată fără numerar (art. 250[1]) și ,f"Acceptarea operațiunilor financiare efectuate în mod fraudulos" (art. 251 C.P..).

Al doilea grup, intitulat "Infracțiuni contra siguranței și integrității sistemelor informatice", este inclus printre infracțiunile contra siguranței publice (Titlul VII, Capitolul VI din Partea specială) și cuprinde șase infracțiuni, anume "Accesul ilegal la un sistem informatic" (art. 360 C.P.), "Interceptarea ilegală a unei transmisii de date informatice" (art. 361 C. P.), "Alterarea integrității datelor informatice" (art. 362 C. P..), "Perturbarea funcționării sistemelor informatice" (art. 363 C. P.), "Transferul neautorizat de date informatice" (art. 364 C.P..), "Operațiuni ilegale cu dispozitive sau programe informatice" (art. 365 C.P..).

Aceste infracțiuni au fost prevăzute, inițial, în câteva legi speciale:

 Legea nr.64/2004, pentru ratificarea Convenției Consiliului Europei privind criminalitatea informatică, adoptată la Budapesta, în data de 23 noiembrie 2001;

 Legea nr.161/2003/Titlul III, care cuprinde prevederi referitoare la Prevenirea și Combaterea Criminalității Informatice;

 Legea nr. 365/2002 privind comerțul electronic unde se definesc "infracțiunile săvârșite în legătură cu emiterea și utilizarea instrumentelor de plată electronică și cu utilizarea datelor de identificare în vederea efectuării de operațiuni financiare;

 Legea nr. 455/2001 privind semnătura electronică prin care se stabilește regimul juridic al semnăturii electronice și al înscrisurilor în formă electronică, precum și condițiile furnizării de servicii de certificare a semnăturilor electronice;

 Legea nr.39/2003, privind prevenirea și combaterea criminalității organizate, care reglementează măsuri specifice de prevenire și combatere a criminalității organizate la nivel național și internațional, definindu-se noțiunea de „infracțiune gravă" căruia i se circumscriu mai multe categorii de infracțiuni printre care se nominalizează și "infracțiunile săvârșite prin intermediul sistemelor și rețelelor informatice sau de comunicații";

 Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;

 Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, lege ce se completează cu prevederile Legii nr. 677/2001;

 Legea nr. 544/2001 privind liberul acces la informațiile de interes public;

 Hotărârea nr. 1259/2001 privind aprobarea Normelor tehnice și metodologice pentru aplicarea Legii nr. 455/2001 privind semnătura electronică;

 Ordinul Avocatului Poporului nr. 52/2002 privind aprobarea Cerințelor minime de securitate a prelucrărilor de date cu caracter personal;

 Ordinul Avocatului Poporului nr. 53/2002 privind aprobarea formularelor tipizate ale notificărilor prevăzute de Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;

 Ordinul Avocatului Poporului nr. 54/2002 privind stabilirea unor situații în care nu este necesară notificarea prelucrării unor date cu caracter personal care cad sub incidența Legii nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date, ca elemente de bază ale informației.

Raportul explicativ al Convenției Consiliului Europei privind criminalitatea informatică aduce mai multă claritate cu privire la conceptul de date informatice, arătându-se că: prin expresia apte de a fi procesate folosită de Convenție se înțelege că datele informatice trebuie să se afle într-o anumită formă care să poată fi în mod direct procesată de un sistem informatic computerizat; ii) datele informatice trebuie să fie în formă electronică sau orice altă formă care să poată asigura procesarea lor directă. (HP. Decizia ICCJ nr. 37/2021 [M. Of. nr. 707 din 16 iulie 2021]).

Din analiza comparativă a conceptului de sistem informatic, legiuitorul român s-a raportat la decizia cadru 2005/222/JAI a Consiliului, care include în conceptul menționat atât dispozitivul sau grupul de dispozitive interconectate sau omologate care asigură prin intermediul unui program prelucrarea automată a datelor informatice cât și datele stocate prelucrate, recuperate sau transmise.

În Partea Generală, Titlul X, intitulat "Înțelesul unor termeni sau expresii in legea penala", Capitolul III, "Dispoziții comune", art.181 Cod penal explică înțelesul

termenilor de sistem informatic și date informatice. Astfel prin sistem informatic se înțelege orice dispozitiv sau ansamblu de dispozitive interconectate sau aflate în relație funcțională. Datele informatice sunt reprezentarea unor fapte sau concepte ce pot fi prelucrate într-un sistem informatic.

În Titlul II din Partea speciala, Capitolul IV, Infracțiuni contra patrimoniului, se reglementează "Fraude comise prin sisteme informatice si mijloace de plata electronice".

În art.249 din Codul penal se prezintă următoarele modalități de comitere a infracțiunii:

• introducerea, modificarea sau ștergerea de date informatice;

• restricționarea accesului la aceste date;

• ori împiedicarea în orice mod a funcționării unui sistem informatic ;

în scopul de a obține un beneficiu material pentru sine sau pentru altul, dacă s-a cauzat o pagubă unei persoane.

Efectuarea de operațiuni financiare în mod fraudulos, infracțiune informatica prevăzută in art.250 Cod penal Poate fi comisă prin mai multe modalități.

• efectuarea unei operațiuni de retragere de numerar; încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri;

• prin utilizarea, fără consimțământul titularului, a unui instrument de plată electronică sau a datelor de identificare care permit utilizarea acestuia;

• efectuarea uneia dintre operațiunile prevăzute în alin. (1), prin utilizarea neautorizată a oricăror date de identificare;

• sau prin utilizarea de date de identificare fictive;

• transmiterea neautorizată către altă persoană a oricăror date de identificare, în vederea efectuării uneia dintre operațiunile prevăzute în alin. (1).

Acceptarea operațiunilor financiare efectuate în mod fraudulos Infracțiunea este prevăzută in art.251 din Codul penal si consta in următoarele.

• -acceptarea unei operațiuni de retragere de numerar, încărcare sau descărcare a unui instrument de monedă electronică ori de transfer de fonduri.

• cunoscând că este efectuată prin folosirea unui instrument de plată electronică falsificat sau utilizat fără consimțământul titularului său;

• acceptarea uneia dintre operațiunile prevăzute în alin. (1). Cunoscând că este efectuată prin utilizarea neautorizată a oricăror date de identificare sau prin utilizarea de date de identificare fictive.

Falsul în înscrisuri, ca infracțiune informatică - Infracțiunea de fals informatic, prevăzută de art.325 Cod penal. Constituie fapta de a introduce, modifica sau șterge, fără drept, date informatice; ori de a restricționa, fără drept, accesul la aceste date, rezultând date necorespunzătoare adevărului. Fapta are ca scop de a fi utilizarea datelor în vederea producerii unei consecințe juridice.

- art. 360 C.P. se referă la accesul ilegal la un sistem informatic: accesul, fără drept, la un sistem informatic se pedepsește cu închisoare de la 3 luni la 3 ani sau cu amendă, fapta prevăzută în alin. (1), săvârșită în scopul obținerii de date informatice; dacă fapta a fost săvârșită cu privire la un sistem informatic la care; prin intermediul unor proceduri, dispozitive sau programe specializate; accesul este restricționat sau interzis pentru anumite categorii de utilizatori. Pedeapsa este închisoarea de la 2 la 7 ani.
- art.361 C.P. sancționează interceptarea ilegală a unei transmisii de date informatice interceptarea, fără drept, a unei transmisii de date informatice care nu este publică și care este destinată unui sistem informatic; provine dintr-un asemenea sistem sau se efectuează în cadrul unui sistem informatic; cu aceeași pedeapsă se sancționează și interceptarea, fără drept, a unei emisii electromagnetice provenite dintr-un sistem informatic, ce conține date informatice care nu sunt publice;
- art. 362 C.P. se referă la alterarea integrității datelor informatice fapta de a modifica, șterge sau deteriora date informatice ori dea restricționa accesul la aceste date, fără drept, se pedepsește cu închisoarea de la unu la 5 ani.
- art. 363 C.P. sancționează perturbarea funcționării sistemelor informatice.

Aceasta constau în următoarele:

- fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice;
- sau prin restricționarea accesului la date informatice, se pedepsește cu închisoarea de la 2 la 7 ani".
- art.364 reglementează transferul neautorizat de date informatice, transferul neautorizat de date dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice.
- art.365 C.P. sancționează operațiuni ilegale cu dispozitive sau programe informatice
- fapta persoanei care, fără drept, produce, importă, distribuie sau pune la dispoziție sub orice formă dispozitive sau programe informatice concepute sau adaptate în scopul comiterii uneia dintre infracțiunile prevăzute în art. 360-364; – parole, coduri de acces sau alte asemenea date informatice care permit accesul total sau parțial la un sistem informatic, în scopul săvârșirii uneia din infracțiunile prevăzute în art. 360-364;
- deținerea, fără drept, a unui dispozitiv, a unui program informatic, a unei parole, a unui cod de acces; sau a altor date informatice dintre cele prevăzute în alin. (1), în scopul săvârșirii uneia dintre infracțiunile prevăzute în art. 360-364.

Putem vorbi de asemenea și de reglementarea infracțiunilor informatice la nivel european.(Convenția Consiliului Europei privind criminalitatea informatică) Un as-

pect important îl conferă internetul care creează un imens potențial de dezvoltare în toate domeniile vieții sociale, aplicațiile sale fiind practic inepuizabile.

Ușurința în utilizare, costul scăzut, rapiditatea și asigurarea unui caracter anonim fac din internet un mediu propice infracțiunilor. Din cauza faptului că internetul oferă posibilitatea ascunderii autorului putem spune că este o încurajare a săvârșirii infracțiunii. O reglementare juridică internațională în domeniul criminalității informatice este dată de Convenția Consiliului Europei privind criminalitatea informatică. Prevederile sale și ratificarea acesteia de un număr mare de state conduce la educația celor care utilizează frecvent internetul și la protejarea acestora.

Cu referire la definiția datelor informatice în Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică aceasta se regăsește la punctul 25 în care se specifică că „,,doar datele informatice care sunt procesate automat de sistemul informatic fac obiectul infracțiunilor regăsite în convenție".

Încrederea și securitatea sunt elementele centrale ale Deceniului digital al UE[1]
.

Pentru un grad superior de securitate cibernetică, Comisia propune strategii cu privire la detectarea atacurilor cibernetice, iminente în sectoarele publice și din ce în ce mai complexe, și nu numai, ci și private. Pe măsură ce IA(inteligența artificială) este în continuă evoluție, operațiunile de securitate sunt menite să prevină și să contracareze , să acționeze înainte de producerea unor daune irecuperabile. Se menționează necesitatea unui efort comun prin întărirea rezilienței cibernetice(Directiva NIS revizuită sau „NIS 2"),

Margrethe Vestager, vicepreședintă executivă pentru o Europă pregătită pentru era digitală, a declarat: „*Europa se angajează pe calea transformării digitale a societății și a economiei. Trebuie deci să o sprijinim cu niveluri de investiții fără precedent. Transformarea digitală se accelerează, dar ea va avea succes numai dacă cetățenii și întreprinderile sunt convinși că produsele și serviciile conectate, pe care se bazează, sunt sigure."*

Este lesne de înțeles necesitatea colaborării interumane și interstatale. Transformările în domeniul cibernetic sunt evidente, au un caracter deschis și acest lucru conduce la eforturi și investiții din partea tuturor celor implicați.

Josep Borrell, Înaltul Reprezentant, a declarat: „*Securitatea și stabilitatea internaționale depind mai mult ca niciodată de un spațiu cibernetic global, deschis, stabil și sigur, în care statul de drept, drepturile omului, libertățile și democrația să fie respectate. Strategia de astăzi constituie un demers prin care UE vizează protejarea guvernelor, a cetățenilor și a întreprinderilor sale împotriva amenințărilor cibernetice mondiale și atingerea poziției de lider în spațiul cibernetic și se asigură în același timp că toți cetățenii pot beneficia de avantajele internetului și de utilizarea tehnologiilor."*

[1] https://ec.europa.eu/commission/presscorner/detail/ro/IP_20_2391

Uniunea Europeană își extinde competențele în sfera digitală pentru a îmbunătăți și proteja drepturile și libertățile cetățenilor statelor membre. În condițiile unei schimbări necontenite a politicii și securității mondiale, prin existențe conflictelor deschise și a celor înghețate, securitatea trebuie să fie asigurată pe toate palierele, pentru o viață normală, într-o societate modernă, normală.

Margaritis Schinas, vicepreședintele pentru promovarea modului nostru de viață european, a declarat: „*Securitatea cibernetică este o parte centrală a uniunii securității. Nu mai există distincții între amenințările online și cele offline. Mediul digital și cel fizic sunt acum indisolubil legate între ele. Setul de măsuri de astăzi arată că UE este pregătită să își utilizeze toate resursele și cunoștințele de specialitate cu scopul de a se pregăti pentru amenințările fizice și cibernetice și de a răspunde acestora cu aceeași hotărâre.*"

Prin estimarea numărului de obiecte conectate la internet ce vor fi în folosință până în anul 2024 (22,3 miliarde)Uniunea Europeană nu face altceva decât să anticipeze evoluția tehnologiilor și a criminalității. Costul anual al criminalității cibernetice pentru economia globală este estimat că a ajuns la 5,5 trilioane de euro la sfârșitul anului 2020.Finanțarea U.E. în cadrul financiar multianual 2021-2027 s-ar putea ridica la 2 miliarde EUR în total, plus investițiile statelor membre și din industrie. În acest context, trebuie valorificate și consolidate toate resursele și toate instrumentele pentru ceea ce se dorește a fi un internet global și deschis, sigur, operațional, un internet care să promoveze: Regulamentul UE privind securitatea cibernetică, Regulamentul general privind protecția datelor (GDPR), Regulamentul de identificare electronică (e-IDAS)

Thierry Breton, comisarul pentru piața internă, a afirmat: „*Amenințările cibernetice evoluează rapid și sunt din ce în ce mai complexe și adaptabile. Pentru a asigura protecția cetățenilor și a infrastructurilor, trebuie să gândim în perspectivă. Scutul de securitate cibernetică al Europei, un dispozitiv rezilient și autonom, ne va permite să ne utilizăm calificările și cunoștințele pentru a detecta amenințările și a reacționa mai rapid la acestea, pentru a limita eventualele daune și pentru a ne spori reziliența. Investițiile în securitatea cibernetică sunt investiții în sănătatea viitoare a mediilor noastre online și în autonomia noastră strategică.*"

Unitatea comună cibernetică este o nouă platformă care își propune să consolideze cooperarea între instituțiile, agențiile, organismele și autoritățile UE din statele membre.[1]

În pofida practicii judiciare neunitare referitoare la infracțiuni ce intra în sfera criminalității informatice. identifică o singură hotărâre pentru unificarea practicii judiciare.[2]

Din perspectiva aspectelor de natură teoretică și practică specifice infracționale

[1] https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit

[2] Decizia 15/2013 a ICCJ prin care a fost soluționat un recurs în interesul legii cu privire la interpretarea dispozitiilor art 42 alin 1 -2,3, din L 161/2003

din sfera criminalității informatice în scopul apărării securității inform. prin decizia nr 37/2021 ICCJ „publicarea de anunțuri fictive online care au avut drept consecință producerea unei pagube, fără ca prin această activitate să se intervină asupra sistemului informatic sau asupra datelor informatice prelucrate de acestea realizează condițiile de tipicitate, ale infracțiunii de înșelăciune prevăzute de art. 244 din CP românesc".[10, Codul Penal al României actualizat în 2023]

Amenințările de natură informatică asupra spațiului cibernetic național s-au diversificat, atât din punct de vedere cantitativ cât și din punct de vedere al complexității tehnicii, căpătând un caracter transfrontalier. Investigațiile activității infracționale transfrontaliere implică un volum mare de activități și o strânsă colaborare internațională a celor care desfășoară activități în domeniul asigurării siguranței informaționale.

Concluzionând, criminalitatea informatică ca domeniu aflat în permanentă inovare, dezvoltare și diversificare în era digitalizării -produce consecințe exponențiale atât asupra nr de utilizatori și implicit riscurilor de victimizare.

Nu trebuie minimalizat impactul asupra securității informaționale la nivel strategic de apărare a spațiului terestru aerian maritim, respectiv al suveranității) deoarece o astfel de vulnerabilitate ar determina consecințe devastatoare de natură a bulversa apărarea siguranței și securității naționale, economice sociale și politice.
De aceea fiecare cetățean, entitate socială, statal trebuie să conștientizeze că luarea măsurilor de prevenție este o necesitate obiectivă, fără de care echilibrul n-ar mai exista, ci anarhie, haos global.

Era digitală deschide noi oportunități, promovează valorile unei societăți democratice, deschise care dezvoltă tehnologie aplicativă și permite o economie actuală ancorată în realitatea imediată. Uniunea Europeană prin Comisia Europeană creează premisele unei dezvoltări durabile și a unei ere digitale de încredere.

Acronime:
C.P. Cod Penal
I.A. Inteligența Artificială
I.C.C. J Înalta Curte de Casație și Justiție
U.E. Uniunea Europeană
GDPR Regulamentul general privind protecția datelor
EUR Euro
e-IDAS Regulamentul de identificare electronică

Referințe bibliografice:

1. Strategia de securitate cibernetică a României 2022-2027 aprobată prin Hotărârea de Guvern nr. 1.321 din 30 decembrie 2021,
2. LEGE nr. 58 din 14 martie 2023- privind securitatea și apărarea cibernetică

a României, precum și pentru modificarea și completarea unor acte normative
3. Actul legislativ privind piețele digitale (APD)Consiliul UE 14 septembrie 2022

Site-uri:
4. https://ec.europa.eu/commission/presscorner/detail/ro/IP_20_2391
5. https://digital-strategy.ec.europa.eu/en/policies/joint-cyber-unit
6. http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Convention%20and%20protocol/ETS%20185%20Romanian.pdf
7. https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/roncss.pdf
8. Convenția Consiliului Europei privind criminalitatea informatică Budapesta 2001
9. CODUL PENAL AL REPUBLICII MOLDOVA, Publicat : 14-04-2009 în Monitorul Oficial Nr. 72-74
10. NOUL COD PENAL AL ROMÂNIEI cu modificările ulterioare, actualizat în 2023.