

# INFRAȚIUNI CIBERNETICE

**Autorul: Eugeniu BACIU**

*Universitatea Tehnică a Moldovei*

**Abstract:** *Securitatea în mediul cibernetic a devenit o componentă a securității tuturor statelor, care se poate realiza prin, cunoașterea, prevenirea și anihilarea atacurilor și amenințărilor, precum și prin diminuarea vulnerabilităților infrastructurilor cibernetică în scopul evitării riscurilor, prevenirea și combaterea infracțiunilor informatice și nu în ultimul rând apărarea cibernetică. Internetul, ca instrument principal al infracțiunilor informatice, prezintă o înfinitate de utilizări din ce în ce mai complexe, ceea ce duce în mod inevitabil la diversificarea formelor de manifestare a fenomenului.*

**Cuvinte cheie:** *spațiu virtual, internet, etică, etichetă, infracțiune cibernetică, terorismul informatic.*

## 1. Introducere

Pe parcursul ultimelor decenii dezvoltarea intensă în domeniului IT a avut un imens impact asupra tuturor componentelor societății umane. Spațiul cibernetic devenind un element de baza a societății contemporane. Comunicațiile și tehnologia informației au devenit coloana vertebrală, manifestându-se în sectoare cheie: economie, energie, transport, cultură etc. Spațiul cibernetic a “rupt” hotarele dintre țări, cetățeni și etnii, permițând relaționarea și schimbul de informații și idei la nivel planetar, devenind un mediu prielnic, ce favorizează procesul de globalizare.

Acest mediu este o parte a societății, fiind asemeni unei societăți însă virtuale, deci un spațiu virtual. El e numit mediu online sau internet. Pentru ca acest mediu să fie unul armonios, liber, deschis altfel zis “sănătos” în el e necesar de aplicat, promovat și apărat valorile, normele și principiile pe care comunitate le urmează.

În ultimii ani s-a observat că în timp ce spațiul cibernetic aduce beneficii enorme, el este, de asemenea, vulnerabil. Incidentele din spațiul cibernetic, intenționate sau neintenționate, sunt în creștere și au efecte negative asupra infrastructurii, telecomunicații, etc. în special asupra domeniului economic. Economia statelor este deja afectată, în proporții diferite din cauza infracțiunilor informatice. Asemenea asigură răspândirea infracțiunilor obișnuite, precum: traficul ființelor umane, vânzarea drogurilor, și alte acțiuni ilegale.

Din cauza acestor factori statele din întreaga lume au început să dezvolte și implementeze strategii de securitate cibernetică și să ia în considerare spațiul cibernetic ca o problemă internațională din ce în ce mai importantă.

## 2. Internet-istoric

Mediul online este de fapt un spațiu virtual în care oamenii pot comunica, acționa etc. Spațiul virtual este întindere limitată, care nu există efectiv, ci ca o posibilitate, limitele între care se desfășoară o acțiune deja reală și cu efecte în realitate. Deci acest spațiu nu este altceva decât internetul. Acest cuvânt își are originea în limba engleză definindu-se ca o rețea interconectată (**interconnected network**).

Internetul a fost inventat în 1969, când Departamentul de cercetare și apărare al Statelor Unite ale Americii (DARPA) a realizat o rețea descentralizată de calculatoare, ceea ce permitea de a dejuca un eventual atac nuclear. Deoarece pierderea unui calculator sau a câtorva nu ar fi însemnat pierderea ireversibilă a tuturor informațiilor. Această rețea le permitea interconectarea calculatoarelor și descentralizarea lor, astfel transferul de informații independent de la un calculator la altul din interiorul rețelei. Internetul a fost introdus ca rețea în comunitatea academică americană începând cu universitățile și apoi răspândindu-se mai departe. În anul 1993 s-a înregistrat s-a dublat numărul de utilizatori, ajungându-se la 400 de milioane.

## 3. Etica în internet

Deci din cele enunțate mai sus putem conchide că internetul reprezintă un spațiu cibernetic, o realitate alternativă liberă, extrem de liberă. Pe internet oamenii comunică, interacționează unul cu altul fiind nevoiți să respecte anumite reguli, principială etc. de conduită morală ca și în realitate. De asemenea spațiul virtual ne oferă posibilitatea de a acționa. Acțiunile noastre pot fi în folosul nostru, în folosul unei persoane sau în folosul comunității sau în detrimentul cuiva ori comunității. Așadar apar principiile morale (bine/rău). Așadar în internet tot e nevoie de respectat etica.

Internetul are propria cultură. Ca rezultat termenul de etică este înlocuit cu Neticheta (Netiquette /net-i-  
ket/). Neticheta este un cod social de comportare și comunicare eficientă într-o rețea iar regulile sale, reprezintă

norme culturale pentru actualizări de stare, mesaje de e-mail, setările de confidențialitate și liste. Neticheta conține următoarele reguli:

- Regula de aur a Netichetei: este de a trata pe alții, așa cum dorești să fii tratat. Fă pentru alții online, așa cum ai face pentru tine.
- 4 reguli de bază:
  - Verificarea ortografică și corectarea mesajelor.
  - Nu scrie totul cu Caps Lock într-un text, deoarece este ca și cum ai țipa la cel care te citește.
  - Onestitatea este o neticheta bună, deoarece comunicațiile în rețea nu sunt valide fără ea.
  - Fii tu însuși online, pentru că nu ești anonim și alți utilizatori sunt oameni reali.
- 7 reguli esențiale pentru o comunicare eficientă:
  - *Regula 1:* Nu scrie totul cu Caps Lock într-un text, deoarece este ca și cum ai țipa la cel care te citește.
  - *Regula 2:* Nu jigni și nu răspunde la jigniri.
  - *Regula 3:* Nu faceți spam și nu urmați link-uri de tip pop-up și spam-ul, deoarece acestea pot duce la viruși, spyware și malware.
  - *Regula 4:* Fii conservator în e-mailul trimis și liberal în e-mailul primit, deoarece calitatea este mai bună decât cantitatea.
  - *Regula 5:* Nu trimite e-mailuri noaptea târziu, deoarece aceasta poate pune în discuție stilul tău de viață.
  - *Regula 6:* Cumpăra de pe site-uri web securizate, deoarece acestea protejează informațiile tale.
  - *Regula 7:* Fii discret în tot ceea ce faci pe internet. Aceasta include crearea de profiluri pe rețelele sociale și postarea de comentarii.

#### 4. Problema eticii în internet

Dezvoltarea internetului ridică numeroase probleme etice cum ar fi: protecția vieții private, securitatea și confidențialitatea informațiilor, drepturile de autor, difuzarea de zvonuri și acuzații, și multe altele. Cele enumerate mai sus prezintă niște probleme etice cât și pericole la care noi suntem supuși ca rezultat a unor acțiuni neetice, și anume infracțiuni obișnuite în internet.

Astfel avem un mare număr de surse dar majoritatea din ele nu sunt de încredere cum ar fi, o mare parte din jurnalism ca dezinformare. Asemenea circulă și informații ce pot dăuna-canaluri pe youtube.com. Un pericol aparte informația cu caracter personal, aici se includ: datele personale; conversații personale care pot fi folosite pentru a provoca daune materiale. Un caz aparte sunt copiii. Fiind foarte naivi, pe rețele de socializare ei deseori comunică cu oameni necunoscuți, și nici măcar nu pot presupune real cine e la acel capăt.

Aici ar fi cazul de adăugat că cauzele constituie libertatea extrem de mare, posibilitatea de a rămâne într-un mod oarecare anonim și alte facilități ale internetului. Astfel mulți oameni trec de limita binelui spre rău, provocând daune și alte fărâdelegi. Astăzi problemei etice în internet îi este acordată o atenție deosebită fiind discutată la multe forumuri internaționale pe lângă alte probleme globale cu scopul de a găsi măsuri de soluționare.

În soluționarea problemei eticii în internet s-a încadrat și religia. În anul 2001, Papa Ioan Paul al II-lea și-a exprimat susținerea privind proiectul Consiliului Pontifical pentru Comunicații Sociale de a scrie un document despre „Etica Internetului“. Acest document venea după „Etica în Comunicațiile Sociale“ (2000) și „Etica în Publicitate“ (1997).

#### 5. Infracțiuni cibernetice-repere teoretice

Din cele expuse mai sus, infracțiunea cibernetică reprezintă o acțiune neetică săvârșită în spațiul cibernetic ce are consecințe negative în societatea reală, punând sub pericol oameni. Pentru a defini mai concret această îmbinare de cuvinte îl vom explica pe cuvinte. Conform dicționarului explicative al limbii române, prin noțiunea de “infracțiune” se înțelege o faptă care prezintă pericol social, constând în încălcarea unei legi penale, în săvârșirea, cu vinovăție, a unei abateri de la legea penală, și care este sancționată de lege. Iar cibernetic în contextual dat are semnificația de spațiul virtual, calculatorul precum și tot ce e legat de ele. Astfel Infracțiunea informatică va avea următoarea definiție, o faptă social periculoasă, prevăzută de Codul penal, comisă cu vinovăție, asupra unui calculator sau cu ajutorul lui precum și accesorii, în spațiul virtual pentru care se aplică pedeapsa penală.

O formă acută a acestui fenomen reprezintă terorismul informatic. Este o nouă amenințare la adresa ordinii publice. Sunt multe definiții pentru acest termen dintre care cea mai reușită definiție este a F.B.I-ului: "un atac premeditat, motivat politic, împotriva informațiilor, sistemelor de calculatoare, programelor și

operărilor de date, ce conduce la violente împotriva obiectivelor civile și necombatantilor, atac exercitat de grupări subnaționale sau agenți clandestini".

Infrațiunile cibernetice pot fi clasificate după tipuri de infracțiuni, și anume după acțiunile întreprinse:

- infracțiunea de fraudă informatică - *fapta de a cauza un prejudiciu patrimonial unei persoane prin introducerea, modificarea sau ștergerea de date informatice, prin restricționarea accesului la aceste date ori prin împiedicarea în orice mod a funcționării unui sistem informatic, în scopul de a obține un beneficiu material pentru sine sau pentru altul.*
- infracțiunea de fals în informatică - 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, în scopul de a fi utilizate în vederea producerii unei consecințe juridice.
- infracțiunea de prejudiciere a datelor sau programelor informatice;
- infracțiunea de sabotaj informatic - acțiune având ca scop împiedicarea calculatorului și a sistemelor sale, în special frânarea desfășurării normale a activității sale în scopul de a obține un beneficiu material.
- infracțiunea de interceptare neautorizată;
- infracțiunea de reproducere neautorizată a unui program informatic protejat de lege;
- infracțiunea de alterare fără drept a datelor sau programelor informatice;
- infracțiunea de spionaj informatic;
- infracțiunea de utilizare neautorizată a unui calculator, program informatic protejat de lege;
- Etc.

## 6. Cauzele infracțiunilor cibernetice

Desigur sunt multe motive din domeniu social, economic, cultural dar să evaluăm problema prin prisma tehnologiilor. Ușurința în utilizare, costul scăzut, rapiditatea și asigurarea unui caracter anonim fac din Internet un mediu propice infracțiunilor. Datorită caracterului global al rețelei și uriașei complexități, posibilitățile de a rămâne într-un mod oarecare anonim a autorului sunt practic nelimitate, încurajând și din acest motiv săvârșirea de infracțiuni.

Alte tipuri de cauze sunt:

- Dependența de tehnologia informației și comunicațiilor-spațiul cibernetic "a pătruns" în sectoarele cheie a societății, oamenii depinzând multe de tehnologiile informaționale.
- Numărul de utilizatori - numărul de utilizatori, este în continuă ascensiune, depășind 1,5 miliarde. Chiar dacă numai 0,1% din utilizatori ar comite infracțiuni, numărul total al infractorilor ar depăși 1,5 milioane.
- Disponibilitatea dispozitivelor și accesului-pentru a comite o infracțiune cibernetică e voie de: echipament hardware, software și acces la internet.
- Disponibilitatea informațiilor - Internetul conține, în prezent, aproape 240 milioane de pagini web, un infractor liber găsește informația detaliată de care are nevoie
- Pierderea mecanismelor de control-este greu de controlat internetul luând în considerare mărimea spațiului cibernetic și numărul imens de utilizatori.
- Viteza de dezvoltare-permite infractorilor de a săvârși infracțiuni utilizând metode din ce în ce mai complexe.

## 7. Structuri specializate în prevenirea și combaterea criminalității informatice

Un exemplu de structuri specializate în luptă cu infracțiunile cibernetice, pe baza unui stat cu o practică vastă în acest domeniu. În S.U.A sunt următoarele structuri: Secțiunea privind criminalitatea informatică și proprietatea intelectuală, F.B.I., Serviciul Secret al Statelor Unite, Direcția de Imigrări și Vămi a Statelor Unite, Serviciul de Inspecție Poștală a Statelor Unite.

Asemenea și U.E întreprinde acțiuni eficiente în combaterea cu infracțiunile cibernetice, a înființat Centrul European pentru Criminalitate Informatică, la 23.11.2001 C.E a adoptat Convenția de la Budapesta împotriva criminalității informatice, precum se adoptă un șir de legi, recomandări și rezoluții etc.

## 8. Infracțiunile cibernetice în Republica Moldova

În R. Moldova infracțiunile cibernetice au următoarele caractere:

- caracter predominant financiar: produse de credit și plată oferite de instituții financiare;
- organizarea grupărilor care acționează, structurarea și specializarea membrilor acestora;
- folosirea unor tineri cu abilități în a utiliza computerele și noile tehnologii

- trecerea de la fraudele informatice, în domeniul tranzacțiilor, la fraude în care predomina folosirea de programe informatice în fraudare;
- caracterul transnațional al acestor fapte, în sensul că sunt vizate victime din alte țări, anumite activități sunt derulate de pe teritoriul altor state sau sunt folosite sisteme informatice din alte state;

Un caz aparte îl prezintă pirateria. Potrivit studiului Business Software Alliance cu privire la pirateria software pentru computere personale, Republica Moldova face parte din grupul de state cu cea mai mare rată a pirateriei, ocupând locul 4 din lume (după Georgia, Bangladesh și Zimbabwe). Se constată că, ponderea produselor program ilegale din totalul software-ului utilizat este de 91%, ceea ce constituie, în opinia BSA, 28 milioane de dolari SUA, și, totodată, cel puțin 70 milioane de lei venit național (reieșind din achitarea TVA și a taxelor de import).

### 9 Măsurile de combatere în R. Moldova

În trecut aceste cazuri erau anchetate de ofițeri de urmărire penală obișnuiți, astăzi prin hotărârea Parlamentului din 4 mai 2010, s-a creat Secția tehnologiei informaționale și investigații ale infracțiunilor în domeniul informaticii. De asemenea s-au introdus schimbări în codul penal al R.M, capitolul XI” Infracțiuni informatice și infracțiuni din domeniul telecomunicațiilor”, ce prevede următoarele categorii de infracțiuni cibernetice:

- Accesul ilegal la informația computerizată (art. 259);
- Interceptarea ilegală a unei transmisii de date informatice (art. 260);
- Alterarea integrității datelor informatice ținute într-un sistem informatic (art. 260);
- Perturbarea funcționării sistemului informatic (art. 260);
- Falsul informatic (art. 260);
- Frauda informatică (art. 260);
- Etc.

Pedepsele sunt variante de la amenzi de la 200 u.c. până la privarea de libertate pe o perioadă de până la 9 ani.

### 10. Exemple de infracțiuni cibernetice și impact acestora

Doi tineri din orașele Chișinău și Cimișlia sunt cercetați penal pentru infracțiuni cibernetice. Potrivit procurorilor, în ultimele două luni, suspectii au spart sistemul de securitate al unei agenții de turism și au furat informații ce conțin secret comercial pentru a vinde datele unor companii din străinătate. Ei riscă 7 ani de închisoare.

Forțele de poliție internaționale au destructurat o grupare de români care sunt acuzați celei mai mare fraude cu carduri bancare din Australia, de la nivelul anului 2013. Un număr de șapte persoane din România au fost acuzate de furt informatic de pe 30.000 de carduri de credit australiene, potrivit polițiștilor din acest stat.

Echipa Național Computer Crime aparținând FBI estima într-un studiu al său că încercările de fraudă pe computer nu sunt nici măcar detectate în proporție de 85-97%

### 11. Abordarea problemei infracțiunilor cibernetice pe plan mondial

Problema infracțiunilor informatice a fost pusă în discuții la sfârșitul summit-ului G8 din 1997, comunicarea prezentată la acel summit cuprindea 10 principii și direcții de acțiune pentru combaterea acestui fenomen.

În prezent această temă asemenea este discutată pe scară largă. Luna Europeană a Securității Cibernetice (ECSM) ediția 2016 a demarat oficial fiind o campanie a UE de promovare a securității cibernetice în rândul cetățenilor și urmărește schimbarea percepției asupra amenințărilor informatice, prin intermediul promovării conceptului de securitate a datelor și a informațiilor, prin educație, schimbul de bune practici și competiții. Au fost abordate temele: securitatea în domeniul bancar (3-7 octombrie), siguranța cibernetică (10-14 octombrie), educația de securitate cibernetică (17-21 octombrie), malware-ul pentru dispozitivele mobile (24-28 octombrie).

### 12. Concluzia

Concluzionând tema abordată aș dori să menționezi că la baza tuturor tipurilor de infracțiuni cibernetice este comportamentul neetic, care în ultimele decenii crește. O întrebare la această temă ar fi: ”Mai are oare loc etica în internet, dacă și religia a s-a implicat în soluționarea problemei etice?”.

Desigur o altă mențiune este că odată cu dezvoltarea tehnologiilor informaționale ele vor căpăta utilizări mai vaste în societatea noastră, făcându-ne mai dependenți de ea, supunându-ne unui risc și mai mare căci și

metodele infractorilor vor deveni mai complexe, iar infracțiunile lor ne vor afecta mai grav. Astfel afirmația:” Teroristul zilei de mâine ar putea fi capabil să provoace daune mai mari cu un Keyboard decât cu o bombă” a devenit deja un adevăr și o realitate.

Nu și în ultimul rând evidențezi faptul că nu doar statul și structurile speciale se combat cu acest fenomen dar și întreaga comunitate. Această problemă a căpătat nuanțe globale, fiind o problemă de zi discutată la multe conferințe internaționale, În cadrul cărora se iau măsuri necesare de combatere eficientă. De asemenea și comunitatea se implică în rezolvarea acestei probleme, cum ar fi introducerea netchitei.

#### **Bibliografie:**

<http://gandeste.org/general/activismul-hacker-ilor-dezobedienta-civila-sau-infraciune-cibernetica/26117>  
<http://www.canal3.md/ro/news/doi-tineri-sunt-cercetati-penal-pentru-infraciuni-cibernetice>  
<http://infoeuropa.md/criminalitatea-informatica/>  
<http://lex.justice.md/index.php?action=view&view=doc&lang=1&id=330752>  
<http://legi-internet.ro/blogs/index.php/infraciuni-informatic-noul-cod-penal>  
<http://www.legi-internet.ro/articole-drept-it/2007/aspecte-privind-urmarirea-penala-in-cazul-infraciunilor-informatic-prevezute-de-legea-nr161-din-2003.html>  
<http://www.legi-internet.ro/articole-drept-it/infraciunea-de-interceptare-ilegala-a-unei-transmisii-de-date-informatic.html>  
[http://drept-md.com/wp-content/uploads/2014/02/Raport\\_-Criminalitatea-informatica.pdf](http://drept-md.com/wp-content/uploads/2014/02/Raport_-Criminalitatea-informatica.pdf)  
<http://drept-md.com/raport-criminalitatea-informatica/>  
<http://www.criminalitate.info/>  
<http://www.criminalitatea-informatica.ro/infraciuni-informatic/>  
<https://dexonline.ro/>  
<http://www.legi-internet.ro/insulta.htm>  
[https://www.realitatea.net/infraciuni-cibernetice-12-arestari-in-mai-multe-tari-printre-care-si-romania\\_1849651.html](https://www.realitatea.net/infraciuni-cibernetice-12-arestari-in-mai-multe-tari-printre-care-si-romania_1849651.html)  
[http://www.economica.net/conferinta-despre-etica-terorismului--a-eugeniei-si-a-internetului--sustinuta-de-cercetatori-ai-universitatii-din-oxford\\_110994.html](http://www.economica.net/conferinta-despre-etica-terorismului--a-eugeniei-si-a-internetului--sustinuta-de-cercetatori-ai-universitatii-din-oxford_110994.html)  
<http://www.cnet.ro/2002/02/22/etica-in-internet/>  
<http://www.cnet.ro/2002/02/22/etica-in-internet/2/>  
<http://www.info-portal.ro/articol/impactul-internetului-in-cultura-societate-si-economie/276/1/etica/>  
<http://www.scribd.com>  
<https://timotintatiana.wordpress.com/2011/12/05/etica-in-spatiul-virtual/>  
<http://prbeta.ro/blog/etica-online/>  
<http://www.prietenulpc.ro/10-reguli-de-comunicare-pe-internet/>  
<http://www.magisteriu.ro/etica-in-internet-2002/>  
<http://www.ziare.com/articole/frauda+online>