

LIBRIS

We know
books

Alexandru Ion

Securitatea cibernetică și drepturile cetățenilor în mediul virtual european



București, 2023

Cuprins

Avertisment (prefață de Mihai Milca)	5
Introducere	13
Capitolul 1. Abordarea teoretică	39
1.1. Definirea termenilor de specialitate ai mediului virtual	48
1.2. Utilizarea teoriilor relațiilor internaționale în mediul cibernetic	59
1.3. Teoria realismului în spațiul cibernetic	64
1.4. Abordarea teoretică neoliberală în mediul cibernetic	71
1.5. Teoria constructivistă în spațiul virtual	78
1.6. Concluzionarea teoretică	85
Capitolul 2. Impactul jurisdicției CEDO și CEJ asupra Europei	97
2.1. Jurisprudența CEDO asupra statelor Consiliului Europei	103
2.2. Jurisprudența CEJ în Uniunea Europeană	119
2.3. Constatări asupra analizei comparative a CEDO și CJE.....	139

2.4. Exportarea modelului UE către statele din vecinătatea sa	158
2.5. Protejarea drepturilor individuale la costul securității colective?	174
Capitolul 3. România ca actor politic în spațiul cibernetice	210
3.1. România și abordarea asupra drepturilor cetățenilor pe internet	218
3.2. Echilibrul între drepturile umane și securitate cibernetică	246
3.2.1. Provocări cibernetice pentru instituțiile române	247
3.2.2. Combaterea amenințărilor cibernetice externe	275
3.2.3. Poziția României asupra spațiului cibernetice în contextul internațional	316
3.3. Potențialul de contribuție cibernetică al țării noastre în mediul internațional	336
Concluzii	350
Anexe	377
BIBLIOGRAFIE	388

Capitolul 1

Abordarea teoretică

Consider acest prim capitol important pentru înțelegerea lucrării, fiind dedicat structurării teoretice, definirii termenilor specifici și în același timp înțelegerii metodelor de cercetare ce le voi folosi în următoarele capitole. De aici decurge necesitatea de împărțire în mai multe subcapitole, justificată prin cantitatea enormă de informații, pentru o mai bună organizare. Am decis astfel să utilizez o structură simplistă de șase subcapitole, în care voi demonstra eficiența bazei teoretice, urmând ca în capitolul următor să testez ipotezele în sistemul relațiilor internaționale din prezent. Cercetarea ce o avem în vedere pornește de la o cantitate mare de surse primare, iar sursele secundare fiind disponibile într-o cantitate limitată, experții acestui domeniu fiind și ei într-un număr limitat, însă de prestigiu internațional. Interpretarea termenilor se va realiza la un nivel general, după cum aceștia au fost acceptați de mai multe națiuni; pe lângă aceștia, vor apărea diferențe de interpretare în anumite cazuri excepționale privind anumite state. Eficiența teoriilor relațiilor internaționale utilizate, dar și a studiilor de calitate realizate va îmbunătăți forma capitolului prezent.

Elementele importante cu care vom lucra în acest capitol sunt de a supune ipotezele cercetării la perspectiva teoretică a relațiilor internaționale, cu privire la conceperea unei strategii de apărare cibernetică și în același timp de respectare a vieții private. Acestea fiind spuse, întrebările de cercetare sunt următoarele: „Este necesară și prioritară adoptarea unei strategii naționale și internaționale privind securitatea cibernetică?” și „Cum putem combate invadarea confidențialității și libertății indivizilor în mediul online, având în vedere că instituțiile acreditate pot face abuz de aceste informații?”. Este necesar în primul rând să înțelegem modul în care se delimitează securitatea colectivă de drepturile individuale ale cetățenilor în mediul virtual. Pentru a putea răspunde la aceste întrebări, ne este necesară studierea atentă atât a mediului internațional, cât și a statelor în mod individual, utilizând metodele de cercetare calitative și cantitative. Interviuul reprezintă metoda calitativă utilizată pentru a răspunde la cele două întrebări ale cercetării, unde voi discuta cu experți în aria multidisciplinară a securității cibernetice și drepturilor în mediul virtual. Această metodă țintește spre a aduce la un loc viziunea tuturor experților din domeniu, pentru a realiza o perspectivă cât mai obiectivă. Dintre metodele de cercetare cantitative, am decis să aleg utilizarea bazelor de date spre a extrage informații suplimentare, în detrimentul chestionarelor. Consider importantă și această metodă, deoarece este o cale eficientă de a înțelege potențialele comparații între actorii politici internaționali. În afară de observațiile de bază pe care le voi consemna, voi aduce argumente și în privința diferitelor conflicte în mediul cibernetic, spre a determina atât agresorul, cât și victima în aceste cazuri.

Cercetarea pe care o efectuez este pentru confirmarea ipotezei susținute de a identifica dreptul la libertate și securitate pe internet drept două bunuri publice destinate cetățenilor. Din punct de vedere valoric, acestea le consider ca două constante direct proporționale unde tendința democrației ideale este a asigura cetățenilor o valoare cât mai mare din ambele. Lipsa unor valori ridicate în ambele cazuri are drept consecință directă incapacitatea de a apăra bunurile propriilor cetățeni și ale statului, iar în cel de-al doilea caz, lipsa parțială sau totală a libertăților civile. Spre deosebire de alte lucrări de cercetare existente în acest domeniu, eu nu voi trata cele două bunuri, libertatea și securitatea, ca pe două valori invers proporționale prin care satisfăcând una se ajunge la subminarea celeilalte. Doresc să caracterizez securitatea cibernetică și drepturile cetățenilor ca fiind două valori constante, nu două valori puse într-o balanță, iar aceasta să încline variabil în direcția uneia sau a alteia. Astfel că democrația ideală, cel puțin la nivel teoretic, reușește să satisfacă criteriul de separare între libertate și securitate, ceea ce se realizează, la rândul ei, printr-o separare a puterilor în stat.

O privire scurtă asupra societății din prezent ne va releva un tablou al fragmentării opiniei publice în ce privește libertățile umane și securitatea cibernetică, prin existența unui clivaj în politica de securizare a internetului, prin suprimarea drepturilor sau prin creșterea drepturilor, cu rezultate ce afectează buna funcționare a securității. Acestea au apărut ca reacție la dezvăluirile lui Edward Snowden privind supravegherea masivă în mediul online de către Agenția Națională de Securitate

a SUA¹³. Cum trusturile media au avut un discurs tendențios față de aceste dezvăluiri, a dus și la împărțirea populației în pro și contra argumentului de securitate națională în mediul virtual. Varianta ce a fost exclusă prezentării și despre care s-a discutat mult mai puțin comparativ cu cele două menționate anterior este aceea de bună funcționare a celor două drepturi fără a fi necesare compromisuri. Această formulă este exact forma inițială de funcționare a drepturilor umane în raport cu securitatea cibernetică. Cu toate acestea, prin intervenția puterii executive această armonie de funcționare a fost perturbată prin încercarea de creștere a securității naționale fără a avea obiective clar definite. Aceste măsuri au apărut într-un moment de criză internațională, subiectul terorismului fiind vehiculat în prim-plan. După depășirea momentului critic, autoritățile nu au mai renunțat la planul de securizare excesivă în mediul virtual, afectând drepturile individuale. Iar cum fiecare acțiune produce și o reacțiune, față de modul de administrare a securității cibernetice a apărut și rezistența împotriva noii politici de supraveghere masivă în mediul online. Lucrarea va aborda într-un mod obiectiv atât securitatea cibernetică, cât și libertatea cetățenilor, cu scopul îmbunătățirii perspectivei actuale asupra acestora.

Cum subiectul abordat în cercetarea curentă se concentrează pe impactul tehnologiei asupra societății în viața de zi cu zi, consider necesară menționarea încadrării acesteia în aria studiilor de știință și tehnologie¹⁴.

¹³ Deena Zaru, *Dilemmas of the Internet age: privacy vs. security*, <http://edition.cnn.com/2015/02/04/politics/deena-zaru-internet-privacy-security-al-franken/>, accesat la data de: 20.05.2015

¹⁴ Staša Milojević, Cassidy R. Sugimoto, Vincent Larivière, Mike Thelwall, Ying Ding, *The role of handbooks in knowledge creation*

Cercetarea și dezvoltarea au avut efecte benefice în trecut, ajutând omul să-și creeze noi condiții de trai, iar odată cu aceasta să adopte noi principii și valori. Ceea ce ne duce la următorul punct important al cercetării, perspectiva tehnologică optimistă, în care, conform ipotezei expuse anterior, omul ajunge să o utilizeze pentru a produce efecte pozitive¹⁵. Internetul s-a transformat dintr-un simplu confort, în urmă cu câteva ani, devenind în prezent o necesitate, fie că vorbim despre o călătorie în afara țării sau de dezvoltarea unei strategii de apărare cibernetică. Fiind considerat un serviciu indispensabil, furnizat fiecărui individ contra cost, devine ușor de înțeles motivul pentru care acesta are obligația de a nu fi utilizat de către autoritățile naționale în scopuri negative. Dar ce ne vom face în momentul în care realizăm că internetul a fost folosit de către guvernele statelor cu o lungă istorie democratică pentru a supraveghea propriii cetățeni? Acțiunea fiind realizată de către agențiile de securitate fără acordul acestora și fără a avea o justificare pentru invadarea spațiului personal. Vom avea o reacție drastică, prin care vom renunța la a mai folosi internetul spre a nu fi afectați? Răspunsul este nu; din moment ce internetul este un serviciu indispensabil în viața noastră, vom identifica metode prin care ne putem proteja viața privată fără a renunța la el.

Ca cercetător și simplu cetățean am vrut să aflăm despre drepturile mele pe internet și despre capacitatea instituțiilor naționale de a-mi apăra datele personale,

and diffusion: A case of science and technology studies, Journal of Informetrics, 2014, p. 694

¹⁵ Jennifer Hochschild, Alex Crabill, and Maya Sen, *Technology Optimism or Pessimism: How Trust in Science Shapes Policy Attitudes Toward Genomic Science*, http://scholar.harvard.edu/files/msen/files/hochschild_crabill_sen.pdf, accesat la data de: 15.07.2015

iar din acest motiv am devenit pasionat de subiect. Nu m-am delimitat la o simplă cercetare la nivel teoretic de pe teritoriul unui singur stat membru al Uniunii Europene, România, ci am studiat și percepția altor state membre: Regatul Unit al Marii Britanii și Irlandei de Nord, Regatul Belgiei, Austria. Trăim într-un secol al informațiilor, toate interacțiunile noastre cu lumea din jur lasă o „amprentă”; după cum este ușor de înțeles, acțiunile noastre în spațiul privat cunosc din ce în ce mai puțină intimitate. Informația a devenit o resursă importantă, iar toate informațiile disponibile prin mijloacele de comunicare ale cetățenilor le numim Big Data, ce constituie adevărate „dosare digitale”¹⁶. Acestea oferă vaste informații disponibile despre o persoană, iar colectarea lor pe termen lung seamănă mai degrabă cu un jurnal personal, având capacitatea de a afla despre un individ informații pe care nici familia sa nu le cunoaște despre acesta. Poate că veți spune că nu este un subiect interesant de dezbatere publică pentru că oricum nu avem ce să ascundem dacă nu facem absolut nimic ilegal pe internet și nu avem de ce ne teme¹⁷. Dar ce ne vom face în momentul în care comitem ceva nu ilegal, ci imoral? Ce ne facem în momentul în care aceste date sunt interceptate de persoane neautorizate sau sunt stocate necorespunzător sau fără un mandat de către instituțiile guvernamentale? Ce se va întâmpla dacă aceste date stocate sunt partajate mai departe către alte instituții neacreditate de a le obține? Consider că acestea sunt

¹⁶ Serge Gutwirth, Ronald Leenes, Paul de Hert, *Reloading Data Protection: Multidisciplinary Insights and Contemporary challenges*, Springer, Dordrecht, 2014, p. 200

¹⁷ David Aspinall, Jan Camenisch, Marit Hansen, Simone Fischer-Hübner, Charles Raab, *Privacy and Identity Management. Time for a Revolution?*, Springer, 2016, pp. 2-3

întrebări pertinente, pe care fiecare cetățean ar trebui să și le adreseze în momentul în care accesează internetul sau vorbește la telefon. Fiecare dintre noi deținem date ce nu sunt destinate publicului larg, fiind de altfel un drept elementar al oricărui individ într-un stat democratic. Conform raportului întocmit de Center for International Governance Innovation din 2014, 64% din totalul utilizatorilor de internet la nivel mondial sunt îngrijorați cu privire la intimitate în mediul online¹⁸. Pornind de la statisticile existente, înțelegem necesitatea respectării drepturilor online și tragerea la răspundere a autorităților în cazul încălcării acestora.

Pentru a beneficia de o formă reală de consens, pe lângă instituțiile naționale ce veghează la respectarea legilor naționale, este necesar ca, într-o democrație, puterea executivă să răspundă pentru acțiunile sale. Controlul acesta va fi exercitat doar în condițiile în care dispunem de un organism intern apolitic sau de un control extern al organizațiilor internaționale¹⁹. Din exterior este dificilă intervenția asupra unui actor politic internațional fără acordul acestuia, iar impunerea prin forță a unei legislații devine o subminare a suveranității naționale. Ne rămâne astfel obligația să observăm modul în care instituțiile naționale exercită o formă de control asupra Guvernului în privința drepturilor umane și a securității pe internet. Modul în care instituțiile naționale funcționează în raport cu valorile unei democrații autentice este răspunsul pe care-l poate oferi doar o organizație internațională ce veghează la

¹⁸ Center for International Governance Innovation, *IPSOS Global Survey on internet security and trust*, GICI, Waterloo, 2014

¹⁹ Human Rights Watch, *UN: Major Step on Internet Privacy*, <https://www.hrw.org/news/2015/03/26/un-major-step-internet-privacy>, accesat la data de: 20.07.2015

respectarea drepturilor cetățenilor. Avem, de asemenea, cazuri în care modul de funcționare al normelor și instituțiilor ajunge să fie adoptat de mediul internațional, ca exemplu având Codul Civil și Penal al Franței în spațiul european. În alte cazuri fiind necesară influența mediului internațional pentru îmbunătățirea modului de funcționare instituțională și de reformare a sistemului intern. Răspunsul căutat nu se regăsește în modul perfect de definire a democrației, ci felul în care acest mod este suficient de bun pentru a nu afecta buna desfășurare a vieții cetățenilor săi. Uneori nu este suficientă perspectiva oferită la nivel național de către un actor politic, pentru a avea o metodologie comparativă este important să analizăm și mediul internațional.

În privința ariei de referință, lucrarea de cercetare nu aduce în discuție doar problema supravegherii în mediul online din partea autorităților statului, ci include și pericolele supravegherii din partea corporațiilor, precum și din partea persoanelor în mod independent. Dreptul la viață privată este încălcat în toate cele trei cazuri amintite mai sus, fiind mai puțin important cine realizează această acțiune, cât este faptul că este permisă de la bun început²⁰. Metoda de sancționare a acestora este diferită, în cazul statului național sau al unei corporații, ele pot fi acționate în justiție, dar dacă este vorba despre un individ, acesta trebuie în primul rând identificat și abia apoi să se acționeze împotriva lui. Diferența constă în modul în care este înțeles și justificat scopul de interceptare a comunicațiilor private, spre exemplu utilizarea în scopuri comerciale, dar nici în condițiile prezentate astfel nu sunt justificabile. Percepția

²⁰ Sophie Stalla-Bourdillon, Joshua Phillips, Mark D. Ryan, *Privacy vs Security*, Springer, London, 2014, p. 94

diferită asupra unor subiecte precum respectarea dreptului la viața privată pe internet, dar și o bună securitate a datelor creează divergențe în opinia publică. Viziunea fragmentată cu privire la mediul online se regăsește și la nivelul leadershipului național, atât din perspective politice diferite, cât și din incapacitatea de înțelegere a unor concepte-cheie.

Spre a nu apărea confuzii pe parcursul acestui capitol, vreau să aduc câteva justificări, prin urmare, deși lucrarea studiază aria interdisciplinară a securității cibernetice și drepturilor online, voi avea o abordare din perspectiva științelor sociale. Din acest motiv consider necesară o interpretare specifică a termenilor tehnici și de transpunere a acestora din perspectiva relațiilor internaționale și a științelor politice. Acești termeni vor juca un rol important și pentru analizarea în profunzime a spețelor din capitolul următor. Prin aceasta am creat o bază teoretică ușor de înțeles atât pentru experți ai mediului virtual, cât și pentru cercetători ai științelor sociale. Cu toate eforturile de a le face mai ușor de înțeles, termenii în sine necesită o cunoaștere elementară a tehnologiei informației. Studiul interdisciplinar deschide noi orizonturi de cercetare, punând astfel bazele definirii unor noi teorii și concepte asupra mediului virtual, concomitent cu reacția societății la adresa schimbărilor aduse de secolul al XXI-lea.

În privința securității cibernetice, statele lumii au o interpretare diferită asupra acestui subiect și din acest motiv voi trata într-un mod cât mai obiectiv informațiile obținute, iar atunci când este cazul voi specifica felul subiectiv de tratare a acestora. Obiectivele naționale în mediul online diferă, prin urmare interesele

sunt adaptate în funcție de aceste condiții²¹. Unele țări au tendința de reprezentare a unor valori democratice și extinderea acestora în afara granițelor sale, altele doresc hegemonie regională, altele văd utilizarea spațiului internetului pentru scopuri comerciale. Deteriorarea relațiilor dintre state este un efect direct al unei strategii agresive în mediul virtual. Colaborarea dintre state în mediul virtual reprezintă calea spre construirea unor alianțe de durată, de îmbunătățire a comerțului, derulare a unor proiecte de cercetare și dezvoltare cu efecte benefice pe termen lung, dar cu toate acestea unele state au ales calea conflictuală.

1.1. Definirea termenilor de specialitate ai mediului virtual

Consider că este esențial ca termenii cu care voi lucra în cadrul cercetării să fie definiți în mod clar, pentru a nu exista o altă formă de interpretare a acestora. Abordarea multidisciplinară între relațiile internaționale și mediul cibernetic aduce o contribuție semnificativă la valorificarea cercetării, astfel că este necesară înțelegerea precisă a termenilor de specialitate. Însă definiția nu se va restrânge la simpla explicație a termenilor printr-o metodologie tehnică, ci voi adăuga și interpretarea acestora și legătura pe care o au cu știința politică. Cei nouă termeni descoperiți utilizând bibliografia de specialitate îi voi folosi în următoarele două capitole ale cărții pentru a înțelege separarea dintre securitate colectivă și drepturile individuale pe internet. După definirea termenilor cu care voi lucra, voi trece la

²¹ Alexander Klimburg, *National Cyber Security Framework Manual*, CCDCOE, Tallinn, 2012, p. 10

analizarea întrebărilor cercetării utilizând teoriile relațiilor internaționale pentru a confirma sau infirma ipoteza de cercetare a lucrării.

Primul termen adus în discuție este **cyberspațiul**, foarte des întâlnit, fiind sinonim cu mediul virtual sau mediul online. Este definit ca fiind aria ce aduce împreună toate infrastructurile ce formează tehnologia informației, nefiind limitat doar la internet, implicând și componenta solidă: rețele de comunicare, sisteme de calculatoare²². Deși cyberspațiul oferă o serie întreagă de avantaje utilizatorilor săi, acesta vine și cu dezavantaje, ce au devenit parte din viața noastră de zi cu zi²³. Conferindu-i termenului un echivalent în știința politică, este cel al mediului internațional, care, deși inițial a fost unul lipsit de reguli, treptat s-a trecut la implementarea norme interstatale. Caracterizat, similar mediului internațional, prin conflicte interne, locale sau internaționale, și prin activități ilegale, cunoaște diferite forme de reglementare pe teritoriul diferitelor state. Mai nou avem o perspectivă de compromis în privința regulilor dintre state, prin tratate negociate și implementate. Dacă aceste reguli ajung să fie respectate sau sunt încălcate, este un alt subiect de discuție pe care îl voi continua în următorul capitol.

Un al doilea termen pe care îl vom discuta, de asemenea relevant, **securitatea cibernetică**, este acțiunea, procesul sau politica prin care informațiile și infrastructura tehnologică sunt protejate de a fi interceptate,

²² Alexander Klimburg, *National Cyber Security Framework Manual*, CCDCOE, Tallinn, 2012, p. 25

²³ Nicholas Tsagourias, Russell Buchan, *Research Handbook on International Law and Cyberspace*, Edward Elgar Publishing, Cheltenham, 2015, pp. 1-2

distruse sau furate de către o entitate neautorizată²⁴. Altfel spus, politica defensivă aplicată de către state pentru a menține în siguranță datele guvernamentale și private. Este de semnalat aici faptul că fiecare actor politic are propria strategie în privința securității cibernetice, termenul fiind din ce în ce mai des utilizat. Adesea această strategie nu se limitează doar la granița națională, fiind o strategie regională, în unele cazuri, cum este Uniunea Europeană, sau o strategie internațională, cum este în cazul NATO. Cu toate că scopul acestor strategii este de a atinge perfecțiunea, fiecare sistem de apărare își are propriile vulnerabilități. Guvernele alocă anual fonduri din ce în ce mai mari pentru îmbunătățirea metodelor de apărare în mediul virtual, precum și pentru cercetarea incidentelor ce au provocat pagube anterior ca să împiedice repetarea acestor greșeli.

Următorul termen pe care îl voi aduce în discuție este **securitatea informației**; după ce în paragraful anterior am discutat despre semnificația securității cibernetice, trebuie să specific că acest concept este parte componentă a securității informației. Definiția termenului de securitate a informației are o tentă subiectivă nu doar în funcție de fiecare actor statal, dar și în funcție și de actorii non-statali. Astfel, conceptul de securitate a informației este metoda prin care se urmărește protecția informațiilor dintr-un sistem, prin integritate, confidențialitate și transparență²⁵. Îndeplinirea acestor trei condiții nu garantează implicit imposibilitatea distrugerii

²⁴ National Initiative for Cybersecurity Careers and studies, *Explore Terms: A Glossary of Common Cybersecurity Terminology*, http://niccs.us-cert.gov/glossary#letter_c, accesat la data de: 05.05.2015

²⁵ Novainfosec, *Cyber Security versus Information Security*, <https://www.novainfosec.com/2014/05/05/cyber-security-versus-information-security/>, accesat la data de: 06.05.2015

sau furtul acestora. Ce doresc să adaug aici este că pe teritoriul fiecărui stat există instituții acreditate cu protejarea informațiilor atât din sfera guvernamentală, cât și din cea privată. Prin urmare, diferă strategia de protecție a datelor disponibile față de persoanele neautorizate și în același timp de păstrare a transparenței față de cetățenii statului. Fiecare actor politic internațional are o percepție diferită asupra metodei de partajare a informațiilor, din acest motiv ajungem la concluzia că numărul statelor este egal cu numărul total al abordărilor.

Cum tehnologia nu ne-a adus doar beneficii, de pe urma acesteia profită și indivizi cu acces la internet ce urmăresc să afecteze bunăstarea celorlalți cetățeni. Al patrulea termen adus în discuție este **cyber-crima**, definit cel mai des ca fiind acționarea în mod neregular sau ilegal în mediul virtual²⁶. O definiție clară în acest sens este imposibil de oferit, din moment ce fiecare stat din mediul internațional percepe într-un mod diferit ce înseamnă o infracțiune pe internet. Astfel că, de-a lungul timpului, termenul de crimă cibernetică a primit o interpretare subiectivă, însă ceea ce are în comun în toate definițiile este că produce un efect dăunător persoanelor, software-ului și hardware-ului. În afară de sectorul informațional, este afectată și starea materială a persoanelor fizice sau juridice, deoarece în unele cazuri se urmărește compromiterea informațiilor legate de sectorul financiar. Cu trecerea timpului, cazurile de criminalitate în mediul online s-au înmulțit, din acest motiv mai multe state au luat inițiativa instruirii cetățenilor săi cu privire la modul de desfășurare a activităților acestora pe internet. În științele sociale cea

²⁶ Alexander Klimburg, *National Cyber Security Framework Manual*, CCDCOE, Tallinn, 2012, pp. 13-14