Cyberspaţiul şi teritorialitatea legii penale

Cyberspace and the territoriality principle of the criminal law

Conf. univ. dr. ***Laura Maria STĂNILĂ****
Universitatea de Vest din Timişoara
Facultatea de Drept

Abstract

The extension of the criminal phenomenon in the area of cyberspace leads to a paradigm shift in the application of criminal law in space, with the consequence of a reconfiguration of the principles governing criminal jurisdiction. In this study, the author proposes an analysis of the principle of territoriality of criminal law from the perspective of conflictual criminal legal relationship with cybernetic element, offering arguments for a change of vision in the sense of diluting territoriality as the main rule of criminal law.

Keywords: *principle of territoriality, principle of ubiquity, application in space of criminal law, mutual cooperation, cybercrime*

Rezumat

Extinderea fenomenului infracţional în sfera cyberspaţiului determină o schimbare de paradigmă în ceea ce priveşte aplicarea legii penale în spaţiu, cu consecinţa reconfigurării principiilor care guvernează jurisdicţia penală. În prezentul studiu, autoarea îşi propune o analiză a principiului teritorialităţii legii penale din perspectiva raportului juridic penal de conflict cu element cibernetic, oferind argumente în sensul unei schimbări de viziune şi al unei diluări a teritorialităţii ca regulă principală a aplicării legii penale.

Cuvinte-cheie: *principiul teritorialităţii, principiul ubicuităţii, aplicarea legii penale în spaţiu, cooperare mutuală, infracţionalitate cibernetică.*

I. Aspecte introductive privind necesitatea unei schimbări de paradigmă în privinţa aplicării în spaţiu a legii penale în cazul infracţiunilor cibernetice. Cyberspaţiul – ultima frontieră

Criminalitatea cibernetică reprezintă o ameninţare serioasă pentru valorile de bază ale societăţii, punând în pericol evident drepturile omului, democraţia şi statul de drept. Aproape orice tip de infracţiune poate fi comisă în cyberspaţiu, existând la ora actuală inclusiv forme specifice de criminalitate organizată cibernetică, extrem de greu de controlat şi combătut de către organele judiciare. Utilizarea de către infractori a Tehnologiei informaţiilor şi a comunicării (TIC) în demersurile lor antisociale a dus la apariţia unei ramuri distincte a fenomenului infracţional – criminalitatea cibernetică sau informatică – care prezintă trăsături specifice suplimentare faţă de fenomenul infracţional „clasic". Un *modus operandi* prin utilizarea serverelor, adreselor IP, reţelelor şi sistemelor răspândite pe întreg teritoriul geografic al mapamondului reclamă o reacţie socială adaptată noilor vremuri care să utilizeze la rândul său noile tehnologii, pregătire specializată a investigatorilor şi a organelor judiciare şi un cadrul legal pe măsură care să vină în întâmpinarea acestor noi realităţi. În afara adaptării mijloacelor şi metodelor de investigaţie infracţională, una dintre cele mai mari provocări o reprezintă interpretarea şi aplicarea

* laura.stanila@e-uvt.ro

principiul teritorialităţii legii penale şi, în consecinţă, determinarea certă a jurisdicţiei penale aplicabile unor cazuri concrete de infracţionalitate cibernetică.

Doctrina internaţională a semnalat deja că ameninţările din ce în ce mai mari prezentate de digitalizare a aproape a oricărei activităţi umane necesită noi modalităţi de abordare a problemei teritorialităţii şi că este extrem de important a se face distincţia între ceea ce este „aici" şi „acolo" într-o formă electronică[1].

Internetul nu este un spaţiu de nondrept, în ciuda exprimării unor opinii contrare izolate[2]. Cu toate acestea, este dificil de conturat la ora actuală un drept al internetului sau măcar un drept penal al internetului. Pe cale de consecinţă, internetul se supune normelor juridice existente şi principiilor jurisprudenţiale din realitatea obiectivă, însă mediul digital exercită o acţiune corozivă asupra dreptului, iar sistemul juridic se află acum în punct de cotitură.

Termenul „cyberspațiu" a fost utilizat pentru prima oară de scriitorul SF William Gibson în lucrarea *Neuromantul*, autorul imaginându-şi un spațiu populat de milioane de utilizatori conectați la o „halucinație consensuală"[3].

Realitatea virtuală devine „noua realitate", o realitate alternativă unde regulile realităţii obiective suferă mutaţii. Cyberspaţiul ne-a promis un tip de societate pe care spaţiul realităţii noastre nu l-ar permite niciodată: libertate fără anarhie, control fără guvernare, consens fără putere[4]. În vreme ce reţeaua *www*[5] e globală, transnaţională, dreptul în general şi dreptul penal în special rămân tradiţionale şi naţionale, deşi există interferenţe tot mai multe, un exemplu elocvent fiind cel al cooperării mutuale în materie penală.

Prin urmare, principiile aplicării legii penale în spaţiu nu prea mai sunt compatibile cu dimensiunea paralelă a cyberspaţiului a spaţiului virtual care nu se suprapune peste spaţiul fizic. Din această cauză, unii autori vorbesc despre o „limitare a teritorialităţii jurisdicţiei subiective" în contextul infracţionalităţii cibernetice[6].

Fireşte că o introducere în problematica aplicării legii penale în spaţiu în cazul particular al infracţiunilor cibernetice presupune o incursiune în principiile aplicării legii penale în spaţiu astfel cum sunt ele prevăzute în dreptul intern, însă abordarea corectă şi eficientă necesită focusarea demersului ştiinţific pe elementele de transnaţionalitate ale fenomenului infracţional cibernetic. Altfel spus, aplicarea legii penale în spaţiu în cazul infracţiunilor cibernetice trebuie să ţină seama de natura transnaţională a ariei „online". În acest spaţiu virtual, regula clasică a teritorialităţii stabilite de dreptul internaţional nu poate aduce soluţii clare. În acelaşi timp, fiind o manifestare a suveranităţii naţionale, regula teritorialităţii nu se lasă uşor abandonată. Eventualele soluţii la care statele suverane ar putea ajunge în lupta lor pentru combaterea infracţionalităţii cibernetice nu pot fi însă limitate la spaţiul Uniunii Europene şi nici la Consiliul Europei, ci vor trebui să aibă un caracter global. De departe, Convenţia de la Budapesta a Consiliului Europei privind criminalitatea cibernetică[7] la care au aderat 65 de state părţi de

---

[1] J. Kleijssen, P. Perri, *Cybercrime, Evidence and Territoriality: Issues and Options*, în M. Kuijer, W. Werner (eds.), *Netherlands Yearbook of International Law 2016*, Netherlands Yearbook of International Law 47, p.169, DOI 10.1007/978-94-6265-207-1_7.

[2] A se vedea John Perry Barlow, *Declaraţia de independenţă a cyberspaţiului,* 1996, http://web.archive.org/web/20010603162041/www.eff.org/~barlow/Declaration-Final.html.

[3] W. Gibson, *Neuromantul*, Ed. Paladin, Bucureşti, 2017.

[4] L. Lessig, *Code version 2.0.,* Basic Books, New York, 2006, p. 30.

[5] *„world wide web".*

[6] J.-B. Maillart, *The limits of subjective territorial jurisdiction in the context of cybercrime*, ERA Forum 19: 375-390, 2019, https://doi.org/10.1007/s12027-018-0527-2.

[7] *Convenţia Consiliului Europei cu privire la criminalitatea informatică (Convention on cybercrime),* adoptată la Budapesta, la 23 noiembrie 2001. Convenţia a fost ratificată de România *prin Legea nr.64/2004 şi publicată în Monitorul Oficial, Partea I nr. 343 din 20 aprilie 2004.* Convenţia de la Budapesta este primul tratat internaţional cu privire la infracţiunile comise prin internet şi alte reţele de calculatoare, care se ocupă în special de încălcările drepturilor de autor, fraudele legate de computer, pornografia infantilă şi încălcările securităţii reţelei. De asemenea, conţine o serie de puteri şi proceduri, cum ar fi căutarea reţelelor de calculatoare şi interceptarea. Obiectivul său principal, stabilit în preambul, este urmărirea unei politici penale comune care vizează protecţia societăţii împotriva criminalităţii cibernetice, în special prin adoptarea legislaţiei adecvate şi încurajarea cooperării internaţionale.

pe tot mapamondul[8], inclusiv SUA, rămâne în prezent cel mai bun cadru pentru a oferi soluţiile de urgenţă necesare pentru realizarea justiţiei penale, respectând în acelaşi timp drepturile omului şi principiile stabilite ale jurisdicţiei statului.

II. Cyberspaţiul – între teritorialitate şi ubicuitate

Principiul teritorialităţii legii penale este considerat cel mai important dintre principiile aplicării legii penale în spaţiu, fiind consacrat de toate legislaţiile penale. Spre exemplu[9], art. 8 C. pen. român statuează că „legea penală română se aplică infracţiunilor săvârşite pe teritoriul României". Textul consacră regula că legea penală română se aplică tuturor infracţiunilor săvârşite pe teritoriul României, indiferent de naţionalitatea infractorului. Legea penală este teritorială, fiindcă rostul ei este de a realiza, menţine şi restabili ordinea pe teritoriul statului căruia îi aparţine. În literatura de specialitate s-a subliniat că principiul teritorialităţii legii penale reflectă cel mai bine principiul constituţional fundamental, referitor la suveranitatea statului român[10]. De aceea, în cazul infracţiunilor săvârşite pe teritoriul României nu se pune problema vreunui conflict de competenţă între legea penală a statului nostru şi legile penale ale altor state ai căror cetăţeni săvârşesc infracţiuni pe teritoriul României.

Aplicarea legii penale faţă de infracţiunile săvârşite pe teritoriul naţional este, în principiu[11], exclusivă şi necondiţionată, cu alte cuvinte, calificarea faptei ca infracţiune, condiţiile tragerii la răspundere penală, stabilirea, aplicarea şi executarea sancţiunilor penale pentru infracţiunile săvârşite pe teritoriul naţional au loc toate exclusiv în temeiul legii penale române, fără a se ţine seama de reglementările cuprinse în legea penală a statului al cărui cetăţean este eventual făptuitorul. De asemenea, dacă un cetăţean străin sau o persoană fără cetăţenie a fost judecată şi condamnată în străinătate pentru fapte comise în ţara noastră, hotărârile pronunţate de instanţele străine nu au autoritate de lucru judecat. Dacă persoana care a comis o infracţiune pe teritoriul ţării noastre a fost judecată şi condamnată pentru acea infracţiune în străinătate, ar fi judecată şi condamnată pentru aceeaşi faptă şi de instanţele române, în baza principiului *non bis in idem*, partea din pedeapsă, precum şi reţinerea şi arestarea preventivă, executate în afara teritoriului ţării, se scad din durata pedepsei aplicate pentru această infracţiune de instanţele române. Regula teritorialităţii a fost extinsă în sensul unei interpretări largi a noţiunii de „teritoriu" şi a celei de „infracţiune comisă pe teritoriu", dispoziţiile art. 8 alin. (4) C. pen. consacrând aşa-numita regulă a ubicuităţii: *„Infracţiunea se consideră săvârşită pe teritoriul României şi atunci când pe acest teritoriu ori pe o navă sub pavilion românesc sau pe o aeronavă înmatriculată în România s-a efectuat un act de executare, de instigare sau de complicitate ori s-a produs, chiar în parte, rezultatul infracţiunii".*

---

[8] Lista statelor care au semnat şi ratificat Convenţia de la Budapesta disponibilă la https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=TyQ7bjRy.

[9] Codul penal francez consacră regula teritorialităţii în art. 113. Legea penală italiană reglementează principiul teritorialităţii în art. 3 alin. (1) şi art. 6 C. pen. italian, iar în art. 4 alin. (2) defineşte noţiunea de „teritoriu", în care sunt incluse navele şi aeronavele italiene oriunde s-ar găsi, în afară de cazul în care, după dreptul internaţional, sunt supuse legilor străine (a se vedea G. Fiandaca, E. Musso, *Diritto penale, parte generale*, Bologna, 1995, p. 114; F. Mantovani, *Diritto Penale. Parte generale*, CEDAM Padova, 1993, p. 911). Codul penal german reglementează principiul teritorialităţii legii penale în Titlul I par. 3, în baza căruia legea penală germană se aplică faptelor penale ce au fost comise pe teritoriul german, ca şi în legislaţia noastră penală. În par. 4, legiuitorul german a prevăzut aplicarea legii penale germane şi faptelor săvârşite pe navele sau aeronavele autorizate să arboreze pavilionul german sau însemnele naţionale ale Germaniei. Codul penal portughez, în art. 45, consacră principiul teritorialităţii legii penale. Astfel, potrivit acestui articol, „cu excepţia cazului în care există un tratat sau o convenţie internaţională contrară, legea penală portugheză este aplicată faptelor săvârşite: a) pe teritoriul portughez, indiferent de naţionalitatea autorului; sau b) la bordul navelor sau aeronavelor portugheze". În legea penală spaniolă, conceptul juridic de teritoriu include, în primul rând, spaţiul care cuprinde teritoriul în sens geografic, mai precis, spaţiul terestru, maritim şi aerian supus suveranităţii spaniole. Şi, de asemenea, include în sens juridic spaţiile acoperite de dreptul pavilionului, şi anume navele şi aeronavele spaniole, indiferent unde s-ar găsi acestea, sub rezerva ca tratatele internaţionale să nu prevadă altfel (a se vedea F. Munoz Conde, M. Garcia Aran, *Drept penal – Partea generală*, Ed. Tirant la Blanch, Valencia, 2002, p. 152).

[10] V. Dongoroz, *Drept penal, Reeditarea din 1939*, Editura Academiei, p. 131.

[11] Spunem „în principiu" deoarece, potrivit art. 12 C. pen., teritorialitatea legii penale române este înlăturată dacă se dispune altfel printr-un tratat internaţional la care România este parte. Cu alte cuvinte, normele de drept internaţional ratificate de România, dacă există, se vor aplica cu prioritate infracţiunilor comise pe teritoriul naţional.

Această regulă a ubicuităţii ar putea fi de fapt salvarea teritorialităţii ca principiu de aplicare a legii penale în cyberspaţiu, majoritatea legislaţiilor penale prevăzând-o. Rezultă că, potrivit reglementării din art. 8 alin. (4) C. pen., nu numai faptele care au fost comise în întregime pe teritoriul ţării noastre, de către participanţii la infracţiune, vor cădea sub influenţa legii penale române, ci şi acelea care au fost începute în ţară şi finalizate în străinătate sau începute în străinătate şi finalizate pe teritoriul României. De asemenea, vor cădea sub incidenţa legii penale române fapte care nu au fost comise în România, dar al căror rezultat s-a produs pe teritoriul ţării noastre. Regula ubicuităţii are meritul de a înlătura neajunsurile celorlalte principii de aplicare a legii penale în timp[12] şi de a reţine avantajele pe care fiecare le prezintă pentru activitatea practică a statelor, în ocrotirea propriilor valori sociale şi în lupta contra infracţiunilor.

După cum spuneam, regula ubicuităţii este consacrată de majoritatea legislaţiilor penale moderne, fiind o regulă modernă, universal recunoscută[13], fiind „cea mai largă aplicare a principiului teritorialităţii calificate”[14]. În sistemul *common-law*, un stat îşi poate exercita jurisdicţia asupra unei infracţiuni atunci când comportamentul infracţional (jurisdicţie teritorială subiectivă) sau rezultatul (jurisdicţie teritorială obiectivă) au avut loc/s-au produs pe teritoriul său. Aplicaţiile subiective şi obiective ale principiului teritorialităţii s-au dezvoltat pentru prima dată la sfârşitul secolului al XIX-lea şi începutul secolului al XX-lea, ca principii independente şi exclusive ale jurisdicţiei. În primul rând, acolo unde a avut loc conduita criminală, se găsesc cele mai utile dovezi pentru investigarea unei infracţiuni. În al doilea rând, în comparaţie cu teritorialitatea obiectivă, se presupune că teritorialitatea subiectivă ar asigura mai bine respectarea principiului legalităţii, conform căruia cetăţenii trebuie în primul rând avertizaţi că o anumită faptă este incriminată. În al treilea rând, jurisdicţia teritorială subiectivă se bazează pe ideea că, din punct de vedere criminologic, este mai important ca statele să sancţioneze exteriorizarea unei voinţe infracţionale pe teritoriul lor decât să restabilească ordinea publică încălcată sau periclitată (raţiunea principală a jurisdicţiei teritoriale obiective). Potrivit lui Foucault, scopul jurisdicţiei teritoriale este într-adevăr „nu atât acela de a restabili un echilibru, cât mai ales acela de a pune în joc, în punctul său extrem, disimetria dintre subiectul care a îndrăznit să încalce legea şi atotputernicul suveran care îşi manifestă puterea”[15]. Statele nu pot interpreta teritorialitatea subiectivă într-un mod mai larg, astfel încât să o poată aplica unei infracţiuni care a fost comisă de cineva din străinătate, deoarece acest lucru ar fi contrar celor trei principii menţionate anterior, care, împreună, constituie raportul dintre jurisdicţia teritorială subiectivă. Cele mai relevante dovezi se găsesc într-adevăr numai pe teritoriul statului unde a avut loc comportamentul infracţional. De asemenea, numai pe teritoriul statului respectiv se exprimă voinţa penală a făptuitorului, iar principiul legalităţii este cel mai bine protejat.

Această definiţie restrânsă a teritorialităţii legii penale determinate pe baza localizării conduitei criminale este recunoscută pe scară largă de doctrină, în special în ceea ce priveşte infracţiunile cibernetice. Statul din care a acţionat infractorul îşi va aplica propria jurisdicţie, deoarece şi dispozitivele implicate în comiterea faptei au fost amplasate pe teritoriul său atunci când au fost utilizate în acest fel. Doctrina germană a arătat că o persoană care încarcă date pe internet din afara Germaniei nu îndeplineşte exigenţa teritorialităţii în Germania. În acest caz, numai teritoriul statului în care făptuitorul este prezent fizic la momentul încărcării datelor defineşte *locus delicti* – locul în care a acţionat făptuitorul *(„Handlungsort”)* şi care determină jurisdicţia aplicabilă[16].

III. Infracţiuni cibernetice. Prin ce se deosebesc de infracţiunile „comune”?

---

[12] Principiul teritorialităţii – art. 8 C. pen., Principiul personalităţii – art. 9 C. pen., Principiul realităţii – art. 10 C. pen., Principiul universalităţii – art. 11 C. pen.

[13] Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice*, International Journal of Cyber Criminology, vol. 9 Issue 1, ianuarie-iunie 2015, p. 67.

[14] J. B. Maillart, *op. cit.*, p. 376.

[15] M. Foucault, *Discipline and Punish: The Birth of the Prison*, Random House, New York, 1995, p. 48-49.

[16] Ulrich Sieber, *Cybercrime and jurisdiction in Germany: the present situation and the need for new solutions*, în S.W.Brenner, B-J. Koops, (eds.), *Cybercrime and Jurisdiction*, Asser Press, The Hague, 2006, p. 189.

Infracţiunile cibernetice se deosebesc de infracţiunile „comune” sau de cele care au un caracter transnaţional prin metodele şi instrumentele utilizate pentru a comite faptele, pentru a disimula adresele IP sau pentru a ascunde urmele electronice.

Doctrina[17] a arătat că există cinci elemente definitorii care caracterizează criminalitatea cibernetică şi care reprezintă principalele elemente de diferenţiere faţă de infracţionalitatea „comună”:

a) schimbarea „scenei” infracţionale, care devine intangibilă;

b) apariţia unor tipuri complet noi de infracţiuni *(ex. phishing);*

c) impactul asupra procedurilor de aplicare a legii, care necesită cooperare internaţională între agenţiile de aplicare a legii şi o abordare multipartită;

d) descentralizarea controlului asupra reţelelor digitale, care are consecinţe majore pentru identificarea ţării, a companiei sau a locului unde sunt transmise sau stocate dovezile;

e) deschiderea şi interdependenţa internetului, care creează vulnerabilităţi comune ce afectează toate persoanele care accesează o reţea digitală specifică;

f) infracţiunile cibernetice sunt urmărite penal cu dificultate din cauza aspectelor legate de natura reţelei şi a dovezilor electronice, care necesită acces imediat la date, precum şi cooperarea dintre agenţiile de aplicare a legii şi furnizorii. În această ordine de idei, dovezile referitoare la comiterea infracţiunilor informatice sunt, într-o covârşitoare majoritate, disponibile doar în format electronic pe sisteme de calculatoare sau dispozitive de stocare şi trebuie păstrate pentru proceduri penale. Investigaţiile penale care nu se bazează pe dovezi electronice constituie o excepţie în cazul criminalităţii cibernetice. Problematica dovezilor electronice este pe cât de importantă, pe atât de sensibilă, imposibilitatea producerii probelor esenţiale ducând la impunitatea infractorilor informatici. O problemă majoră este că dovezile electronice adesea nu sunt localizate pe teritoriul autorităţii care investighează fapta. Datele sunt stocate pe diferite servere, sunt oglindite sau fragmentate ori se deplasează între servere „undeva în cloud”, în jurisdicţii multiple sau necunoscute, în timp ce autorităţile judiciare sunt limitate de principiul teritorialităţii. Chiar dacă datele sunt stocate pe teritoriul statului unde se realizează investigaţia penală, autorităţile judiciare din acel stat putând dispune confiscarea sau percheziţia informatică, aceste măsuri procesuale nu vor fi suficiente dacă persoana fizică sau juridică care deţine sau controlează datele – adică persoana care deţine „cheia” accesului la date – se află pe teritoriul unui alt stat. În acelaşi timp, nu trebuie să uităm faptul că justiţia penală trebuie realizată într-un cadru restrictiv, urmărind scopul combaterii infracţiunilor şi tragerii la răspundere penală a infractorilor, însă respectând în acelaşi timp drepturile omului şi cerinţele statului de drept şi respectând principiile suveranităţii statale.

IV. Aplicarea legii penale în spaţiu în cazul infracţiunilor informatice. Diluări sau limitări ale regulii teritorialităţii în cyberspaţiu?

Este evident că regula teritorialităţii stricte este imposibil de aplicat în cyberspaţiu, argumentele pentru o regândire a acesteia fiind uşor de identificat.

În primul rând, este extrem de dificil din punct de vedere tehnic de identificat şi urmărit infractorii cibernetici şi, prin urmare, de identificat locului în care s-a produs comportamentul infracţional. Fiecărui sistem informatic (computere, telefoane inteligente, tablete etc.) conectat la internet i se atribuie o adresă unică de protocol Internet (IP), care constă din patru (IPv4) până la şase (IPv6) numere, între 0 şi 255. Spaţiul de adrese IP este administrat la nivel global de Corporaţia Internaţională pentru Nume şi Numere Atribuite[18] (ICANN). ICANN nu rulează sistemul, dar ajută la coordonarea modului în care sunt furnizate adresele IP pentru a evita repetarea sau suprapunerea acestora. ICANN este, de asemenea, depozitul central pentru adresele IP, din care sunt furnizate intervale către cele cinci Registre Regionale de Internet (RIR) care, la rândul lor, sunt responsabile în teritoriile lor desemnate pentru alocarea utilizatorilor finali şi a Registrelor Locale de Internet, cum ar fi furnizorii de servicii internet. În prezent,

---

[17] J. Kleijssen, P. Perri, *op. cit.*, p. 148-149.

[18] *International Corporation for Assigned Names and Numbers* (ICANN).

există cinci RIR-uri: RIPE-NCC (Europa şi Orientul Mijlociu), ARIN (America de Nord), APNIC (Asia-Pacific), LACNIC (America Latină şi Caraibe) şi AfriNIC (Africa).

Având în vedere că adresa IP a unui computer indică o adresă fizică[19] ce determină locul de origine al unei infracţiuni cibernetice, nu pare, la prima vedere, să ridice vreo problemă tehnică întrucât teritorialitatea ar presupune doar identificarea locaţiei adresei IP a sistemului informatic utilizat de infractorul cibernetic. Cu toate acestea, niciun atacator nu comite o infracţiune utilizând direct propria sa adresă IP. Există o gamă de tehnici, programe software şi site-uri web disponibile sau accesibile pe internet care permit utilizatorilor individuali să ascundă cine sunt sau unde sunt. Autorul unei infracţiuni cibernetice poate înlocui cu uşurinţă adresa IP a sistemului informatic pe care îl foloseşte cu cea alocată unui alt sistem informatic, astfel încât infracţiunea să pară că este comisă într-o altă locaţie. Există multe proxy-uri deschise pe internet care pot fi accesate de orice persoană[20], această tehnică, denumită „spoofing IP", fiind relativ uşor de implementat. O altă tehnică este utilizarea serverelor proxy, publice sau private, care permite infractorilor de criminalitate cibernetică să stabilească o conexiune la o reţea printr-un server intermediar şi astfel să-şi ascundă activitatea online. Acest sistem informatic, despre care se spune că este „zombificat", este adesea ultima verigă dintr-un lanţ foarte lung care implică numeroase sisteme informatice şi jurisdicţii. Infractorii cibernetici pot ascunde astfel adevărata origine a atacului, făcând urmărirea atacatorilor o sarcină extrem de dificilă. Mai mult, anonimatul inerent activităţilor de pe internet contribuie foarte mult la dificultatea tehnică de a urmări infractorii în spaţiul cibernetic.

Prin urmare, internetul serveşte ca mediu de conectare a *host*-urilor („gazde") din întreaga lume. Uneori este de dorit să ştim unde este localizată geografic o anumită gazdă. În mod informal, geolocalizarea internetului este problema determinării locaţiei fizice (la un anumit nivel de granularitate) a unui utilizator de internet. Aceasta se numeşte adesea şi geolocalizare IP, deoarece fiecare gazdă conectată direct la internet este identificată printr-o adresă IP unică. Un număr tot mai mare de companii (de exemplu, Akamai, Digital Envoy, MaxMind, Quova şi Verifia) întreţin şi licenţiază baze de date care mapează adresele IP la locaţiile geografice[21].

Geolocalizarea pune însă importante probleme juridice. În două cauze a fost evidenţiată incertitudinea în ceea ce priveşte capacităţile tehnologiei de geolocalizare a internetului şi dificultăţile pe care aceasta le pune instanţelor. În afară de problema confidenţialităţii, s-a analizat utilizarea tehnologiei de geolocalizare pentru a cenzura descărcarea conţinutului. *Cazul Yahoo! v. Liga împotriva rasismului şi antisemitismului*[22] soluţionat de Tribunalul din Paris a implicat vânzarea de obiecte naziste pe internet. Experţii consultaţi în cauză au arătat că Yahoo! nu putut restricţiona accesul cetăţenilor francezi la materialele ilicite din mai multe motive, inclusiv: (1) cetăţenia bazată pe adresa IP este corectă doar pentru 70% dintre cetăţenii francezi şi (2) acest lucru este uşor eludat. Cu toate acestea, grupul de experţi a raportat primirea mai multor comunicări de la organizaţii comerciale care afirmau că tehnologia lor ar putea pune în aplicare cererea de cenzură a instanţei franceze.

Un alt caz, Nitke v. Ashcroft[23], a pus în discuţie legea privind decenţa în comunicaţii şi a analizat problema postării pe web a imaginilor considerate de unele comunităţi ca fiind obscene. Obscenitatea este determinată de „standardele comunităţii locale"; astfel, s-a arătat că locaţia clientului care descarcă materialele este relevantă.

---

[19] A. Klip, *XIXe International Congress of Penal Law* (Information Society and Criminal Law), Section IV, General report, Revue International de Droit Pénal, 2014, p. 387.

[20] J. A. Muir, P. C. Van Oorschot, *Internet geolocation and evasion*, ACM Computer Survey, 2009, https://www.ccsl.carleton.ca/paper-archive/muir-computingsurveys-09.pdf.

[21] J. A. Muir, Van Oorschot, *op. cit.*, p. 1.

[22] *Yahoo! Inc. v. Liga contra rasismului şi antisemitismului*, Tribunal de Grande Instance din Paris, 20 noiembrie 2000, http://www.eff.org/legal/Jurisdiction_and_sovereignty/LICRA_v_Yahoo/.

[23] *Barbara Nitke and the national Coalition for Sexual Freedom v. John Ashcroft*, Attorney General (U.S.A.), U.S. District Court, Southern District of New York, case no. 01 Civ. 11476 (RMB), 2003-2004, http://www. sethf.com/nitke/ashcroft.php.

Anonimatul este de fapt „principala problemă" în geolocalizarea sursei infracţiunilor cibernetice[24]. Practic autorităţile de pot stabili locul de comitere a unei infracţiuni cibernetice doar dacă l-ar putea identifica anterior pe autorul acesteia. Cu toate acestea, există multe instrumente, cum ar fi Tor[25], Anonymouse[26], The CloakFootnote[27] sau software-ul de criptare a e-mailurilor, care permit menţinerea anonimatului online.

Obligaţiile negative ce derivă din legislaţia drepturilor omului limitează autorităţile publice în acţiunile şi scopurile lor şi creează o arie de libertăţi individuale care este protejată împotriva oricărei ingerinţe statale. De aceea stabilirea jurisdicţiei aplicabile este o chestiune extrem de importantă care trebuie analizată şi prin prisma standardului dreptului la un proces echitabil şi a componentelor acestuia.

Regulile jurisdicţionale se bazează pe relaţia dintre state, iar jurisdicţia se fundamentează pe principiul teritorialităţii, expresia suveranităţii şi independenţei statale.

Cyberspaţiul modifică aceste reguli şi le impune adaptarea[28].

Astfel, Convenţia cu privire la Criminalitatea Electronică consacră principiul jurisdicţiei teritoriale – cu alte cuvinte, infracţiunilor cibernetice li se aplică legea locului unde a acţionat făptuitorul *(regula lex loci delicti).* Art. 22 al Convenţiei de la Budapesta stabileşte faptul că fiecare stat parte va adopta măsurile legislative şi alte măsuri care se dovedesc necesare pentru a stabili competenţa sa cu privire la orice infracţiune informatică atunci când infracţiunea este comisă într-unul dintre următoarele cazuri, enumerate alternativ:

a) pe teritoriul său;

b) la bordul unui vas sub pavilionul acestui stat-parte;

c) la bordul unei aeronave înmatriculate în conformitate cu legislaţia acestui stat-parte;

d) de către unul dintre cetăţenii săi, dacă infracţiunea poate atrage răspunderea penală în locul în care aceasta a fost comisă sau dacă infracţiunea nu este de competenţa teritorială a niciunui stat.

Statele-părţi îşi pot rezerva dreptul de a nu aplica sau de a aplica doar în cazuri ori în condiţii specifice regulile de competenţă indicate mai sus, cu excepţia cazului de teritorialitate exclusivă.

Totodată se va aplica jurisdicţia statului pe al cărui teritoriu este prezent autorul prezumat al infracţiunii dacă acesta nu poate fi extrădat spre un alt stat decât în baza naţionalităţii sale, în urma unei cereri de extrădare.

În cazul în care mai multe părţi îşi revendică jurisdicţia cu privire la o infracţiune stabilită în informatică la care face referire convenţia, statele-părţi implicate se vor pune de acord, atunci când acest lucru este oportun, în scopul de a determina care dintre ele este cel mai potrivit pentru a exercita urmărirea.

Comitetul de Miniştri al Consiliului Europei a stabilit că jurisdicţia unui stat se aplică nu numai în cazul în care atât persoana care atacă un sistem informatic, cât şi victima se găsesc pe teritoriul său, ci şi dacă sistemul informatic atacat se află pe teritoriul său, chiar dacă făptuitorul este localizat în altă parte. Nu este clar dacă aceleaşi reguli se aplică în cazul în care conţinutul vătămător este publicat pe internet, deoarece în principiu o pagină web e accesibilă de oriunde în lume[29]. Această interpretare a primit denumirea de „doctrina efectelor calificate"[30] şi a dus la o extindere a regulii teritorialităţii în sensul că se va aplica legea statului de unde procurorul a accesat pagina web[31]. Evident că această doctrină este

---

[24] L. Greenemeier, *Seeking address: why cyber attacks are so difficult to trace back to hackers*, 2011. Disponibil la http://www.scientificamerican.com/article/tracking-cyber-hackers/.

[25] http://www.torproject.org.

[26] http://anonymouse.org.

[27] http://www.the-cloak.com/anonymous-surfing-home.html.

[28] R. Uerpmann-Wittzac, *Principles of International Internet Law,* German Law Journal, vol. 11 nr. 11: 1246-1263, 2010, p. 1254.

[29] Consiliul Europei, Comitetul de Miniştri, *Convenţia cu privire la criminalitatea cibernetică, Raport explicativ* din 8 noiembrie 2001, paragr. 233, disponibil la: http://conventions.coe.int/treaty/en/reports/ html/185.htm.

[30] R. Uerpmann-Wittzac, *op. cit*., p. 1255.

[31] A se vedea cauza Perrin – CEDO, *Perrin v. United Kingdom*, Judgment of 18 October 2005, www.echr.coe.int.; Cauza Toeben – Curtea Federală Germană 2000, http://www.bundesgerichtshof.de/; Yahoo – Tribunalul Superior din Paris 2000, *Tribunal de Grande Instance de Paris, UEJF et Licra c/ Yahoo! Inc.*, Ordonnance de Référé of 20 November 2000, available at: http://www.juriscom.net/txt/jurisfr/cti/tgiparis 20001120.htm.

foarte dificil de aplicat deoarece teoretic ar putea veni în concurs toate cele peste 190 de jurisdicţii naţionale, conform principiul ubicuităţii cyberspaţiului.

De aceea şi practica judiciară a diferitelor instanţe naţionale sau internaţionale este neunitară sub acest aspect. Există o tendinţă de a utiliza anumite criterii pentru a alege o jurisdicţie aplicabilă, cum ar fi: limba, conţinutul sau publicitatea ca indicând un anumit stat. De exemplu, dacă conţinutul este intenţionat a fi preluat dintr-un anumit stat, atunci se va aplica jurisdicţia acelui stat.

În *cauza Perrin v. UK* care a fost soluţionată de CtEDO, instanţele britanice au condamnat un cetăţean francez pentru publicarea de materiale obscene pe un site web din SUA, deoarece un ofiţer de poliţie englez a luat act de acele materiale într-o secţie de poliţie din Londra. În *cauza Toeben* instanţele germane au condamnat un cetăţean australian pentru negarea holocaustului pe un site australian. În *cauza Yahoo* amintită mai devreme, Tribunalul de Mare Instanţă din Paris a constatat că oferirea de memorii naziste pe un server american a încălcat legea penală franceză. De vreme ce nu există o reglementare clară a regulii teritorialităţii care să împiedice conflictul de jurisdicţii, conţinutul *world wide web* ar trebui să respecte dispoziţiile legale de peste 190 de state.

Doctrina străină[32] a arătat că trebuie găsit un echilibru echitabil între principiile conflictuale ale jurisdicţiei teritoriale şi ale libertăţii internetului. Din perspectiva drepturilor omului, s-a avansat şi ideea că jurisdicţia străină trebuie să fie previzibilă pentru utilizatorii internetului.

V. Codul domeniului de ţară ca spaţiu cyberteritorial. Extinderea teritorialităţii

Devine tot mai clar faptul că porţiuni ale cyberspaţiului tind să devină extensii ale teritoriului statal. Codul domeniului de ţară (ex. .uk, .ro, .fr etc.). Domeniul de ţară a fost creat de Jon Postel (*Top Level Domains* – TLD), care s-a referit la o listă de coduri de ţară stabilite de organizaţia Internaţională de Standardizare în 1998. Postel a delegat administrarea TLD unor organizaţii ştiinţifice sau alte instituţii care şi-au manifestat intenţia de a funcţiona ca registre. Începând cu 1998, crearea şi atribuirea TLD-urilor este realizată de Internet Corporation for Assigned Names and Numbers (ICANN) despre care am făcut vorbire mai devreme, o organizaţie nonprofit care acţionează în baza legii din California. Acest lucru este valabil pentru *ccTLD*-uri (*country code TLD* – coduri ale domeniului de ţară), cât şi pentru *gTLD*-uri (*generic TLD*-uri – coduri generice), cum ar fi *.com* sau *.info.* Prin urmare, *ccTLD*-urile provin dintr-o sferă care era greu controlată de state. Atât domeniile de ţară, cât şi domeniile generice (.com, .info) sunt în principal create şi controlate de organizaţii private (cum e cazul în UK, Germania), dar constituie şi obiectul impunerii unui control statal eficient (cazul Franţei).

Domeniul *.eu* al Uniunii Europene a fost creat prin Regulamentul (EC) 733/2002[33] al Parlamentului European şi al Consiliului şi face obiectul unui contract de concesiune încheiat între EURid şi Comisia Europeană. Prin Regulamentul (EC) 874/2004[34], Comisia Europeană a adoptat reguli de politică publică pentru administrarea domeniului *.eu.*

Summitul Mondial cu privire la Societatea Informaţională – WSIS (Geneva 2003 şi Tunis 2005)[35] a stabilit că statele nu se pot implica în decizii referitoare la domeniul de ţară al unui alt stat şi că fiecare guvern este suveran asupra domeniului ţării sale, care se va supune jurisdicţiei acelui stat. Un draft WSIS din 30 septembrie 2005 a mers şi mai departe statuând că fiecare guvern va avea suveranitatea asupra codului domeniului său de ţară[36]. Deoarece există o veritabilă legătură între ccTLD şi statul respectiv, un stat poate reclama jurisdicţia deplină asupra propriului său ccTLD. CcTLD devine teritoriu statal în spaţiul cibernetic. Prin urmare, spre exemplu, România ar putea exercita jurisdicţie penală asupra oricărei infracţiuni comise sub domeniul său de ţară ccTLD *.ro*.

Putem spune deci că cyberspaţiul nu înfrânge total principiul jurisdicţiei teritoriale. Mai degrabă, principiul teritorialităţii suferă o adaptare la situaţia specifică a internetului.

---

[32] R. Uerpmann-Wittzac, *op. cit*., p. 1256.

[33] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002R0733.

[34] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32004R0874.

[35] World Summit on the Information Society (WSIS), http://www.itu.int/net/wsis/basic/about.html.

[36] Doc. WSIS-II/PC-3/DT/10 (Rev.4)-E, paragr. 54; disponibil la: http://www.itu.int/wsis/docs2/pc3/ working/dt10rev4.pdf.

VI. Concluzia: teritorialitatea excesivă e desuetă. Regula cooperării mutuale corectează deficienţele şi dificultăţile investigaţiei penale a infracţiunilor informatice.

În 2015, secretarul de stat John Kerry a afirmat că „regulile de bază ale dreptului internaţional se aplică în spaţiul cibernetic" şi „statele ar trebui să colaboreze pentru a descuraja şi a răspunde eficient la ameninţările online". De asemenea, el a elogiat Convenţia de la Budapesta ca fiind „cel mai bun (…) cadru legal pentru a coopera peste graniţe, pentru a defini ce este criminalitatea informatică şi pentru a stabili cum ar trebui prevenite şi urmărite penal încălcările legii". Cu toate acestea, în lipsa unei convenţii universale privind criminalitatea cibernetică sau măcar a unui cadru internaţional general acceptat care să stabilească clar regulile aplicării legii penale naţionale în cyberspaţiu, conflictul între jurisdicţiile penale rămâne încă o problemă delicată.

Criminalitatea cibernetică solicită imperativ mecanisme de cooperare care nu sunt prevăzute în cadrul instrumentelor juridice existente creează dificultăţi semnificative pentru poliţie şi agenţiile de urmărire penală[37]. Există următoarele instrumente multilaterale şi bilaterale care sunt capabile să ofere soluţii numai în anumite contexte[38]:

• Convenţia de la Budapesta;

• Convenţia Naţiunilor Unite împotriva criminalităţii transnaţionale organizate (2000) şi cele trei protocoale adiţionale ale sale;

• Convenţia europeană privind asistenţa reciprocă în materie penală (1959);

• Convenţia interamericană privind asistenţa reciprocă în materie penală (1992);

• Proiectul Convenţiei internaţionale Stanford pentru îmbunătăţirea protecţiei împotriva criminalităţii cibernetice şi terorismului (1999);

• Proiectul Convenţiei Uniunii Africane privind instituirea unui cadru juridic credibil pentru securitatea cibernetică în Africa (2011);

• Legea model a Commonwealth-ului privind infracţiunile informatice şi conexe computerelor (2002).

Atunci când organele judiciare naţionale primesc o sesizare la nivel local cu privire la comiterea unei infracţiuni cibernetice, trebuie îndeplinite o serie de condiţii înainte de a putea fi iniţiată o anchetă formală. Pentru a avea competenţa teritorială necesară, fapta trebuie să fie incriminată de legea statului în cauză. Principiul teritorialităţii din dreptul penal stabileşte că o infracţiune comisă pe teritoriul unui stat va fi urmărită şi judecată de acel stat. Totuşi, în cyberspaţiu, teritorialitatea dreptului penal nu coincide întotdeauna cu suveranitatea teritorială. Mulţi infractori cibernetici au evitat consecinţele penale din cauza slăbiciunilor legilor penale de fond care nu abordează mijloacele tehnologice, altfel spus, legislaţia naţională nu ţine pasul cu Tehnologia Informaţiei şi a Comunicării (TIC) tot mai utilizată în sfera infracţionalităţii. de a ofensa[39]. Determinarea locului în care a fost comisă o infracţiune *(locus delicti)* şi depăşirea conflictului pozitiv şi negativ de competenţă teritorială poate prezenta dificultăţi pentru organele judiciare atunci când efectuează acte procedurale (ex. emit mandate, redactează citaţii etc.).

Foarte interesant este şi faptul că infracţionalitatea cibernetică nu poate fi urmărită în toate cazurile în baza principiului universalităţii[40]. De asemenea, doctrinele consacrate într-un sistem juridic nu pot

---

[37] Cameron S. D. Brown, *Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice,* International Journal of Cyber Criminology, Vol. 9 Issue 1: 55-119, ianuarie- iunie 2015, p. 62.

[38] Ibidem.

[39] R. W. Downing, *Shoring Up the Weakest Link: What Lawmakers Around the World Need to Consider in Developing Comprehensive Laws to Combat Cybercrime* în Columbia Journal of Transnational Law, nr. 43, 2005741-762.

[40] Art. 11 C. pen. român

Universalitatea legii penale

„(1) Legea penală română se aplică şi altor infracţiuni decât celor prevăzute în art. 10, săvârşite în afara teritoriului ţării de un cetăţean străin sau o persoană fără cetăţenie, care se află de bunăvoie pe teritoriul României, în următoarele cazuri:

a) s-a săvârşit o infracţiune pe care statul român şi-a asumat obligaţia să o reprime în temeiul unui tratat internaţional, indiferent dacă este prevăzută sau nu de legea penală a statului pe al cărui teritoriu a fost comisă;

b) s-a cerut extrădarea sau predarea infractorului şi aceasta a fost refuzată.

impune obligaţii şi nici nu se pot aplica în jurisdicţii străine. „Egalitatea suverană" existentă între statele naţionale este un principiu fundamental al dreptului internaţional, care cere respectarea autonomiei legiuitoare a altor ţări. În cele din urmă, legea penală este pur şi simplu un instrument pentru guvernare şi protecţie vizate a moravurilor publice într-o anumită localitate.

Art. 23 din Convenţia de la Budapesta stabileşte că statele părţi vor coopera între ele, în conformitate cu dispoziţiile convenţiei şi în aplicarea instrumentelor internaţionale relevante cu privire la cooperarea internaţională în materie penală, a acordurilor încheiate pe baza legislaţiilor uniforme sau reciproce şi a dreptului lor intern, în cea mai largă măsură posibilă, în scopul investigărilor sau al aplicării procedurilor privind infracţiunile în legătură cu sisteme şi date informatice sau pentru a culege dovezile unei infracţiuni în format electronic.

Totodată Convenţia stabileşte şi un set de principii generale referitoare la asistenţa mutuală[41]:

1. Părţile îşi vor acorda asistenţă mutuală într-o măsură cât mai largă posibil, în scopul investigărilor sau al aplicării procedurilor privind infracţiunile în legătură cu sisteme şi date informatice sau pentru a culege dovezile unei infracţiuni în format electronic.

2. De asemenea, fiecare parte va adopta măsurile legislative, precum şi măsurile care se dovedesc necesare pentru a-şi îndeplini obligaţiile stabilite în convenţie.

3. În caz de urgenţă, fiecare parte va putea formula o cerere de asistenţă mutuală sau comunicările care se raportează acesteia prin mijloace rapide de comunicare, precum faxul sau poşta electronică, cu condiţia ca aceste mijloace să ofere condiţii suficiente de securitate şi de autentificare (inclusiv folosirea codării atunci când este necesar), cu o confirmare oficială ulterioară dacă partea solicitată va revendica acest lucru. Partea solicitată va accepta cererea şi va răspunde prin oricare dintre mijloacele sale rapide de comunicare.

4. Cu excepţia unei dispoziţii contrare expres prevăzute în prezentul capitol, asistenţa mutuală va fi supusă condiţiilor fixate de dreptul intern al părţii solicitate sau de tratatele de asistenţă mutuală aplicabile, inclusiv în ceea ce priveşte motivele pe baza cărora partea solicitată poate refuza cooperarea. Partea solicitată nu îşi va exercita dreptul de a refuza asistenţa mutuală privind infracţiunile vizate la art. 2-11 doar din motivul că cererea vizează o infracţiune pe care aceasta o consideră de natură fiscală.

5. În cazul în care, în conformitate cu dispoziţiile prezentului capitol, părţii solicitate îi este permis să condiţioneze asistenţa mutuală de existenţa dublei incriminări, această condiţie va fi considerată îndeplinită dacă fapta care constituie infracţiunea pentru care asistenţa mutuală este solicitată este calificată drept infracţiune de dreptul său intern, indiferent dacă dreptul intern include sau nu infracţiunea în cadrul aceleiaşi categorii de infracţiuni ori dacă o defineşte sau nu prin aceeaşi terminologie ca dreptul părţii solicitante.

Suntem de părere că, până la o intervenţie de reglementare clară a regulii teritorialităţii în cyberspaţiu care să rezolve problema competenţei teritoriale de investigare, urmărire şi judecare a infracţiunilor cibernetice, doar cooperarea mutuală poate salva aparenţele şi poate rezolva conflicte jurisdicţionale delicate care ar putea apărea în combaterea acestora.

---

(2) Dispoziţiile alin. (1) lit. b) nu se aplică atunci când, potrivit legii statului în care s-a săvârşit infracţiunea, există o cauză care împiedică punerea în mişcare a acţiunii penale sau continuarea procesului penal ori executarea pedepsei sau când pedeapsa a fost executată ori este considerată ca executată.(3) Când pedeapsa nu a fost executată sau a fost executată numai în parte, se procedează potrivit dispoziţiilor legale privitoare la recunoaşterea hotărârilor străine".

[41] Art. 25 Convenţia de la Budapesta.