ANALELE ŞTIINTIFICE ALE UNIVERSITATII „AL. I. CUZA" IASI
TOMUL LXIII, ŞTIINTE JURIDICE, 2017, NR. II

DIFICULTĂŢI DE ORDIN CRIMINALISTIC ÎN INVESTIGAREA INFRACŢIUNILOR INFORMATICE

FORENSIC DIFFICULTIES IN INVESTIGATING CYBERCRIME

ANCUŢA ELENA FRANŢ[1]

Rezumat: Societatea actuală îşi desfăşoară majoritatea activităţilor utilizând tehnologia digitală, fapt care aduce numeroase beneficii, dar care, în acelaşi timp, creează premisele unor infracţiuni specifice. Investigarea unor astfel de infracţiuni necesită dezvoltarea unei metodologii criminalistice speciale. Prezenta lucrare îşi propune să identifice modalităţile prin care pot fi descoperite asemenea infracţiuni şi cum pot fi identificaţi infractorii, evidenţiind, în acelaşi timp, dificultăţile cu care se confruntă investigatorii în anchetarea unor astfel de fapte antisociale. Dificultăţile pot apărea, de exemplu, atunci când infractorii îşi ascund adresa de IP, când utilizează o altă adresă de IP sau când îşi atribuie o identitate falsă. De asemenea, este important ca anchetatorii să respecte dispoziţiile legale care prevăd respectarea dreptului la viaţă privată şi să desfăşoare percheziţiile informatice doar în condiţiile prevăzute de lege. Studiul îşi propune să cerceteze şi potenţialul preventiv pe care îl poate avea analiza informaţiilor oferite de internet, în condiţiile în care internetul facilitează comunicarea dintre infractori şi poate oferi indicii despre pregătirea unor activităţi infracţionale.
Cuvinte-cheie: internet, criminalitate informatică, criminalistică, prevenirea infracţiunilor.

Abstract: The modern society carries out most of its activities using digital technology, which brings many benefits but, at the same time, creates the premises of specific crimes. Investigating such crimes requires the development of a special forensic methodology. This paper aims to identify ways in which such offenses can be discovered and how criminals can be identified, while highlighting the difficulties faced by investigators in investigating such antisocial facts. Difficulties may arise, for example, when offenders hide their IP address, use another IP address or assign a false identity. It is also important for investigators to comply with legal provisions regarding the right to privacy and to conduct computer searches only under the

[1] Asistent univ. dr., Facultatea de Drept, Universitatea „Alexandru Ioan Cuza" din Iași, email: ancuta.frant@uaic.ro.

conditions provided by law. The study also aims to examine the preventive potential of internet information analysis, given that the internet facilitates communication between criminals and can provide clues about the preparation of criminal activities.
Key-words: internet, cybercrime, forensic science, crime prevention.

1. Privire generală asupra infracţiunilor informatice

Dezvoltarea tehnologică permanentă reprezintă una din trăsăturile definitorii ale umanităţii.

În prezent, activitatea societăţii se bazează în mare măsură pe tehnologia digitală. Aceasta aduce numeroase beneficii şi facilitează, fără îndoială, viaţa oamenilor, dar, în egală măsură, aduce modificări în modul în care percepem relaţia cu ceilalţi. De asemenea, îi face pe oameni vulnerabili într-un mod care nu fusese cunoscut anterior, deoarece, în paralel cu facilităţile aduse de tehnologie, se dezvoltă şi infracţionalitatea cibernetică.

În special dezvoltarea internetului a modificat radical modul în care se desfăşoară relaţiile sociale în toate domeniile de activitate. Însă această dezvoltare a internetului a atras şi o vulnerabilitate a oamenilor în faţa infracţionalităţii specifice, care s-a dezvoltat în mediul informatic.

Infractorii utilizează internetul în scopuri multiple, de exemplu, pentru a face schimb de informaţii, pentru a-şi ascunde identitatea, pentru a-şi asuma o altă identitate, pentru a descoperi şi a strânge informaţii despre potenţialele victime, pentru a lua legătura cu alţi infractori, pentru a distribui informaţii (adevărate sau false)[2].

Revine criminalisticii, care, prin excelenţă, are rolul de a analiza urmele infracţiunilor, să dezvolte mijloace eficiente pentru a descoperi făptuitorii, astfel încât aceştia să fie pedepsiţi.

Dezvoltarea internetului permite însă şi dezvoltarea laturii preventive a criminalisticii, deoarece pot fi identificate indicii cu privire la pregătirea săvârşirii unor infracţiuni.

În lucrarea de faţă ne propunem să trecem în revistă modalităţile prin care criminalistica poate utiliza caracteristicile specifice mediului informatic, astfel încât să se realizeze combaterea şi prevenirea infracţiunilor cibernetice. Nu avem în vedere neapărat infracţiunile informatice, ci orice

[2] A.R. Gonzales, R.B. Schofield, D.W. Hagy, *Investigations Involving the Internet and Computer Networks*, U.S. Department of Justice, Office of Justice Programs, [Online] la: https://www.ncjrs.gov/pdffiles1/nij/210798.pdf, accesat la data de 18.10.2017, p. 1.

infracţiuni care pot fi sancţionate sau prevenite prin analiza datelor ce pot fi obţinute prin intermediul internetului sau prin alte resurse informatice.

Ceea ce dorim să realizăm este să identificăm şi să clarificăm elementele de bază care permit utilizarea mediului cibernetic pentru a afla informaţii despre comiterea unor infracţiuni şi care permit identificarea autorilor. De asemenea, ne interesează latura preventivă, adică modalitatea în care pot fi prevenite faptele antisociale, prin utilizarea informaţiilor pe care le oferă internetul. Mai ales în ceea ce priveşte infracţiunile săvârşite de grupuri organizate, probabilitatea de a afla informaţii despre pregătirea unor infracţiuni prin intermediul internetului este cu atât mai mare, cu cât membrii reţelelor criminale trebuie să comunice între ei. Însă, evident, nu este uşor de identificat comportamentul infracţional, deoarece persoanele care pregătesc săvârşirea unor infracţiuni şi care comunică prin intermediul internetului în acest scop îşi iau toate măsurile de precauţie pentru a-şi ascunde identitatea şi intenţiile. De exemplu, munca investigatorilor este îngreunată de faptul că persoanele care au intenţii infracţionale utilizează frecvent aşa-numitul „dark web" (internetul întunecat), care este mai greu accesibil, aşa cum vom vedea în prezentul studiu.

În lucrarea de faţă ne propunem să identificăm unele dintre dificultăţile care pot apărea în activitatea de investigare a infracţiunilor informatice, încercând să prefigurăm şi eventuale soluţii, acolo unde este posibil.

2. Modalităţi de utilizare a mediului informatic pentru săvârşirea infracţiunilor

Realitatea arată faptul că sunt foarte multe moduri în care mediul informatic în general şi internetul în special sunt utilizate pentru săvârşirea infracţiunilor. Cunoaşterea acestor modalităţi este un pas important în realizarea activităţii de identificare criminalistică.

Una dintre modalităţile de utilizare a mediului informatic pentru săvârşirea de fapte antisociale este *folosirea internetului pentru a facilita comunicarea între persoanele care pregătesc săvârşirea unor infracţiuni*, inclusiv pentru infracţiuni foarte grave, precum terorism, trafic de persoane, trafic de droguri[3].

[3] A.R. Gonzales, R.B. Schofield, D.W. Hagy, *op.cit.*, p. 1.

De asemenea, internetul este utilizat propriu-zis ca *mediu în care se realizează unele infracţiuni* – de exemplu pornografie infantilă sau trafic de persoane ori de droguri[4].

Larg răspândită este utilizarea internetului pentru realizarea *de fraude fiscale*. Aceste fapte urmăresc fie finanţarea unor organizaţii infracţionale (precum organizaţiile teroriste), fie urmăresc pur şi simplu obţinerea unor bani sau foloase ilicite, pentru uzul personal al infractorilor[5].

Internetul reprezintă mediul ideal pentru *racolarea persoanelor*, în vederea săvârşirii faptelor de trafic de persoane sau de pornografie infantilă.

De asemenea, internetul reprezintă un mediu propice şi pentru săvârşirea faptelor de *spionaj economic*, deoarece permite accesarea sistemelor informatice ale organelor de stat sau ale organismelor private, cu scopul furtului de informaţii[6].

Practica a arătat şi numeroase situaţii în care au fost realizate intruziuni ilegale în sistemele informatice ale unor instituţii cu scopul de a le *îngreuna activitatea*[7].

Nu puţine sunt cazurile hackerilor care săvârşesc fapte ilicite în mediul informatic din *teribilism.* Este mai ales cazul unor hackeri tineri, care săvârşesc faptele doar pentru a arăta că au capacitatea intelectuală de a comite asemenea fapte (de exemplu, cazurile unor hackeri care au spart reţelele NASA ori conturile personale ale unor vedete)[8].

De asemenea, există şi cazuri de hackeri care îşi asumă rolul de *„justiţiari”*, acţionând împotriva celor care săvârşesc infracţiuni (de exemplu, organizaţia Anonymous, care a reuşit destabilizarea unor site-uri care promovau pornografia infantilă)[9].

---

[4] A.R. Gonzales, R.B. Schofield, D.W. Hagy, *op.cit.*, pp. 1-2.

[5] A se vedea C.R. Baker, *An analysis of fraud on the internet*, în Internet Research, Vol. 9, Issue 5, pp. 348-360.

[6] A se vedea K. Davis, *Why Cybercrime Is So Hard To Investigate*, în Computer Crime Research Center, 2015, [Online] la: http://www.crime-research.org/articles/4002/, accesat la data de 20.11.2017.

[7] *Ibidem.*

[8] M. Levinson, *Why Law Enforcement Can't Stop Hackers*, [Online] la: https://www.cio.com/article/2402264/security0/why-law-enforcement-can-t-stop-hackers.html?page=2, accesat la data de 22.11.2017.

[9] A. Cuthbertson, *Anonymous Hacker Takes Down 20 Percent of Dark Web in Child Porn Operation*, 2017, [Online] la: http://www.newsweek.com/anonymous-hacker-dark-web-child-porn-operation-553014, accesat la data de 22.11.2017.

Elementele prezentate mai sus, fără a epuiza totalitatea situaţiilor ce pot fi întâlnite în practică, ilustrează diversitatea modalităţilor în care poate fi utilizat mediul informatic pentru săvârşirea infracţiunilor, ceea ce este de natură să arate amploarea fenomenului infracţiunilor cibernetice. Astfel, devine clar de ce este important demersul de prevenire şi combatere a infracţiunilor informatice.

3. Identificarea dificultăţilor cu care se confruntă anchetatorii în investigarea infracţiunilor de natură cibernetică

Literatura de specialitate arată că, teoretic, identificarea persoanelor care săvârşesc infracţiuni informatice ar trebui să fie relativ simplă, deoarece orice activitate în mediul virtual lasă anumite urme. Astfel, ipotetic vorbind, pornindu-se de la identificarea sistemului atacat (sau accesat), mergând înapoi pe linie temporală, ar trebui să se ajungă la identificarea făptuitorilor[10].

Însă realitatea arată că, din păcate, nu este chiar atât de uşor de identificat infractorii, deoarece apar o serie de dificultăţi care împiedică urmărirea drumului activităţii infracţionale. Dificultăţile referitoare la investigarea criminalistică a infracţiunilor informatice se pot referi fie direct la realizarea anchetei, fie la elemente care, deşi nu ţin efectiv de ancheta penală, au urmări asupra modului în care, în general, este organizată o asemenea investigaţie. În continuare vom prezenta unele dintre problemele cu care se confruntă organele judiciare în demersul de cercetare a infracţiunilor informatice.

O primă piedică este reprezentată de faptul că informaţia din mediul virtual este perisabilă şi foarte uşor se poate altera sau distruge, fie datorită acţiunii intenţionate a infractorilor, fie din neglijenţă în ceea ce priveşte stocarea şi utilizarea datelor[11].

O altă problemă provine din faptul că datele temporale sunt uşor de alterat, ori acestea sunt, de multe ori, esenţiale pentru dovedirea vinovăţiei persoanelor suspectate de săvârşirea infracţiunilor cibernetice[12].

O altă dificultate ţine de faptul că investigarea infracţiunilor informatice necesită personal specializat, cu temeinice cunoştinţe în

[10] M. Levinson, *op. cit*.
[11] A.R. Gonzales, R.B. Schofield, D.W. Hagy, *op. cit.*, pp. 1-2.
[12] *Ibidem*, pp. 1-2.

domeniul informatic. Adesea se observă o veritabilă concurenţă între organele statului care caută specialişti în domeniul cibernetic şi mediul economic privat, care, de asemenea, are nevoie de specialişti în mediul informatic[13]. Cel puţin în România, condiţiile oferite de companiile private sunt de multe ori superioare celor oferite de stat, ceea ce explică de ce specialiştii în informatică preferă să aleagă domeniile private de activitate.

Un alt aspect ţine de percepţia asupra gravităţii infracţiunilor săvârşite în mediul informatic. Astfel, unele infracţiuni care se săvârşesc în mediul virtual şi care sunt considerate mai grave polarizează mult mai multă atenţie din partea organelor de anchetă. De exemplu, infracţiunile de pornografie infantilă sau de trafic de persoane ori de droguri atrag implicarea majorităţii personalului specializat din cadrul poliţiei şi parchetelor, ceea ce, mai ales în lipsa unui număr suficient de cadre, face ca atenţia acordată altor infracţiuni informatice, considerate mai puţin grave, să fie mai mică. De exemplu, faptele prin care se creează fraude financiare sunt considerate de mai mică importanţă, ceea ce face ca atenţia acordată pentru urmărirea şi sancţionarea unor asemenea fapte să fie mai mică, ceea ce duce la un număr mare de infractori nedescoperiţi. Este semnificativ faptul că, în Statele Unite ale Americii, deşi se înregistrează lunar chiar şi sute de mii de plângeri pentru fraude fiscale săvârşite în mediul on-line, foarte multe asemenea fapte rămân nedescoperite[14].

Un alt aspect care îngreunează investigarea infracţiunilor cibernetice este faptul că mulţi hackeri sunt tineri care acţionează din teribilism. Adesea, aceste persoane nu ar săvârşi infracţiuni în afara mediului online, dar tehnologia îi face să nu mai distingă graniţa dintre bine şi rău. De multe ori, ei încep prin a sparge site-uri de pe care descarcă muzică sau filme (care în mod normal sunt contra-cost) şi ajung să săvârşească ulterior fapte mai grave (de exemplu, să spargă conturile NASA). Hackerii care acţionează din teribilism duc la încărcarea agendei investigatorilor, care trebuie să se ocupe şi de anchetarea unor asemenea fapte, în loc să se concentreze asupra altora (precum trafic de persoane sau de droguri). Această dificultate nu ţine propriu-zis de criminalistică, ci mai mult de criminologie, dar trebuie analizată în strânsă legătură cu domeniul criminalisticii, datorită impactului pe care îl are în desfăşurarea anchetelor. S-a arătat în literatura de

[13] K. Davis, *op. cit*.
[14] M. Levinson, *op. cit*.

specialitate că aici este, în primul rând, o problemă de educaţie, deoarece tinerii nu sunt învăţaţi care sunt limitele normale ale utilizării mediului informatic, astfel încât să nu se ajungă la săvârşirea de fapte antisociale. Se vorbeşte chiar despre dezvoltarea unei ramuri a eticii – etica utilizării tehnologiei – care să fie predată în şcoli, pentru a preveni săvârşirea unor asemenea fapte[15].

O altă particularitate a infracţiunilor informatice provine din faptul că, de multe ori, sancţiunile aplicate pentru fapte considerate mai puţin grave (de exemplu, fraude fiscale sau fapte săvârşite din teribilism de hackerii tineri) sunt foarte mici. Mai mult, este important faptul că, dacă nu intervin criptări sau denaturări de date, activitatea desfăşurată de infractori pe internet lasă urme care sunt foarte greu de combătut, iar aceasta deschide calea spre încheierea unui acord de recunoaştere a vinovăţiei, care duce, prin efectul legii, la aplicarea de sancţiuni reduse. Aceste sancţiuni mici creează impresia generală că infracţiunile săvârşite în mediul informatic nu sunt foarte grave, ceea ce încurajează săvârşirea lor în continuare[16].

O altă problemă provine din faptul că investigarea infracţiunilor informatice necesită, de regulă, desfăşurarea unor activităţi complexe şi de durată. De multe ori, infracţionalitatea cibernetică implică făptuitori şi victime aflate în ţări diferite, fiind astfel dificil de obţinut accesul la dispozitivele electronice care pot oferi dovezi cu privire la infracţiunile săvârşite. De asemenea, ancheta poate evidenţia necesitatea de a accesa baze de date deţinute de entităţi care nu au legătură directă cu infracţiunea, precum instituţii de stat sau firme private. În plus, poate fi dificil accesul la servere, routere sau la datele stocate de furnizorii de servicii de internet. Legat de acest aspect, este important de subliniat faptul că unele ţări sunt reticente în ceea ce priveşte cooperarea internaţională referitoare la infracţiunile informatice (de exemplu, Rusia[17]).

[15] M. Levinson, *op. cit*.

[16] *Ibidem*. Autoarea oferă drept exemplu cazul lui Joshua Holly, care a furat datele de la 200 de carduri de credit, dar care nu a făcut nici măcar o zi de închisoare pentru fapta sa.

[17] A se vedea M.A. Vatis, *The Council of Europe Convention on Cybercrime*, în Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy, 2010, [Online] la: https://www.nap.edu/read/12997/chapter/14, accesat la data de 29.11.2017, p. 218.

O dificultate dificil de înlăturat în cercetarea infracţiunilor informatice este faptul că, de multe ori, infractorii folosesc reţele criptate, ceea ce face aproape imposibilă identificarea adresei de I.P. a utilizatorilor.

De asemenea, o adevărată provocare în activitatea investigatorilor o reprezintă faptul că activitatea lor nu trebuie să încalce dreptul la viaţă privată. Altfel spus, toate activităţile de strângere şi analiză a probelor trebuie să se desfăşoare cu respectarea dispoziţiilor legale care garantează respectarea acestui drept.

În cele ce urmează vom detalia două dintre dificultăţile de anchetare prezentate mai sus, şi anume utilizarea reţelelor criptate şi necesitatea de a păstra echilibrul între obţinerea datelor necesare anchetei şi respectarea dreptului la viaţă privată.

4. Dificultăţi în realizarea anchetei penale datorate utilizării reţelelor criptate de către infractori

Investigarea infracţiunilor cibernetice este de multe ori îngreunată de faptul că unii infractori folosesc pentru desfăşurarea activităţilor lor ilegale aşa-numitul *dark web* („internetul întunecat”). Pentru a înţelege cum funcţionează *dark web* trebuie să facem distincţia dintre *dark net, dark web* şi *deep web,* noţiuni între care, adesea, se face confuzie.

Dark net este o reţea de internet ce se poate accesa numai utilizând anumite softuri şi, de multe ori, având şi o cheie care să permită accesarea. De exemplu, reprezintă o reţea de dark net o reţea peer-to-peer criptată sau parolată, prin care un utilizator trimite altui utilizator un fişier[18]. Utilizatorii de *dark net* pot folosi şi softuri speciale, precum Tor sau I2P, care permit ascunderea adresei de IP. Astfel, cei care utilizează *dark net* îşi păstrează anonimitatea şi sunt protejaţi de o eventuală supraveghere sau cenzură[19].

Dark web este constituit din mai multe *dark net*-uri. Practic, *dark web* reprezintă totalitatea site-urilor şi a serviciilor ce activează în *dark net*[20]. Este important de înţeles că, în esenţă, *dark web* poate fi accesibil oricui, de

[18] G. Stanciu, *Care este diferența dintre Deep Web, Darknet și Dark Web*, [Online] la: https://playtech.ro/2017/care-este-diferenta-intre-deep-web-darknet-si-dark-web/, accesat la data de 25.10.2017.

[19] A. Greenberg, *Hacker Lexicon: What is the Dark Web?*, [Online] la: https://www.wired.com/2014/11/hacker-lexicon-whats-dark-web/, accesat la data de 20.10.2017.

[20] G. Stanciu, *op. cit*.

exemplu oricărei persoane care utilizează softul Tor şi cunoaşte adresa url a site-ului pe care doreşte să-l viziteze, însă va fi foarte dificil de identificat adresa de IP a utilizatorilor[21].

Deep web reprezintă colecţia tuturor site-urilor de pe internet care nu pot fi găsite prin utilizarea unui motor de căutare. *Deep web* include, într-adevăr, şi *dark web*, dar este format în principal din pagini cu un conţinut licit. De exemplu, fac parte din *deep web* paginile cu un conţinut dinamic, precum cele care sunt generate de completarea unui formular. Tot din *deep web* fac parte şi conţinuturile video ale unor servicii de streaming (de exemplu, Netflix), deoarece se doreşte ca aceste conţinuturi să poată fi vizualizate doar de către cei care le accesează în mod direct[22]. S-a estimat că *dark web* reprezintă, în esenţă, aproximativ 0,01 din totalul paginilor de internet. Concret, unele studii arată că există aproximativ 10000 de servicii Tor ascunse, faţă de cele câteva mii de milioane de pagini web obişnuite[23].

Utilizarea reţelelor criptate este una dintre cele mai dificile probleme pe care le pot întâlni anchetatorii în investigarea infracţiunilor informatice.

5. Păstrarea echilibrului între dreptul la viaţă privată şi necesitatea obţinerii datelor care să permită cercetarea şi sancţionarea infracţiunilor informatice

O problemă greu de surmontat în investigarea infracţiunilor informatice provine din necesitatea de a păstra echilibrul între oportunitatea unor intervenţii energice pentru accesarea datelor care să permită identificarea infractorilor şi respectarea dreptului la viaţă privată.

Semnificativ în acest sens este textul Convenţiei de la Budapesta[24], prin care s-a încercat trasarea unor reguli menite să faciliteze obţinerea

[21] A. Greenberg, *op. cit*.
[22] G. Stanciu, *op. cit.*
[23] A. Greenberg, *op. cit*.
[24] Convenția Consiliului Europei de la Budapesta, din 23.11.2001, privind criminalitatea informatică, ratificată de România prin Legea nr. 64/2004, publicată în M.Of. nr. 343 din 20.04.2004.

datelor necesare anchetării infracţiunilor cibernetice, în special atunci când este necesară cooperarea judiciară internaţională[25].

Convenţia de la Budapesta a fost primită cu rezervă în multe din ţările semnatare (deşi a fost ratificată de 56 de state), în special de către societatea civilă, care a considerat că prevederile sale duc la o imixtiune nejustificat de mare a statului în viaţa privată[26].

În România, mai multe încercări de a legifera direcţiile trasate de Convenţia de la Budapesta au fost declarate neconstituţionale[27].

Este important de subliniat faptul că Rusia, deşi membră a Consiliului Europei, nu a semnat această Convenţie, considerând că prevederile ei reprezintă o încălcare a suveranităţii sale statale. În special dispoziţiile referitoare la posibilitatea ca anchetatorii din alt stat să poată obţine informaţii doar cu acordul proprietarului computerului sau cu acordul deţinătorului informaţiei au fost considerate de Rusia inadmisibile[28].

Aşadar, este dificil de echilibrat necesitatea anchetatorilor de a obţine informaţii care să ducă la identificarea şi pedepsirea infractorilor cu dreptul cetăţenilor la respectarea intimităţii lor. Apreciem că această dificultate care apare în investigarea infracţiunilor informatice este greu de depăşit, deoarece nu ţine de aspecte tehnice (care pot fi, până la urmă, rezolvate), ci de elemente care implică interpretarea drepturilor. Ori, când este vorba despre interpretarea drepturilor şi despre stabilirea limitelor între

[25] Pentru textul oficial al Convenției de la Budapesta, a se vedea [Online] la: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185, accesat la data de 29.11.2017.

[26] A se vedea K. Rodriguez, *Dangerous Cybercrime Treaty Pushes Surveillance and Secrecy Worldwide*, Electronic Frontier Foundation, 2011, [Online] la: https://www.eff.org/deeplinks/2011/08/cybercrime-treaty-pushes-surveillance-secrecy-worldwide, accesat la data de 29.11.2017.

[27] Legea nr. 82/2012 privind reținerea datelor generate sau prelucrate de furnizorii de rețele publice de comunicații electronice și de furnizorii de servicii de comunicații electronice destinate publicului, precum și pentru modificarea și completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice a fost declarată neconstituțională prin Decizia Curții Constituționale nr. 440 din 8.07.2014. Ordonanța de urgență a Guvernului nr. 111/2011 privind comunicațiile electronice (prin care se dorea furnizarea cartelelor telefonice *prepay* doar pe bază de buletin) a fost declarată neconstituțională prin Decizia Curții Constituționale nr. 461 din 16.09.2014. Legea privind securitatea cibernetică a României a fost declarată neconstituțională prin Decizia Curții Constituționale nr. 17 din 21.01.2015.

[28] A se vedea M.A. Vatis, *op. cit.*, p. 218.

care acestea se pot manifesta, discuţiile pot fi interminabile, iar rezultatele concrete pot fi extrem de greu de obţinut.

6. Concluzii

Cele prezentate mai sus susţin ideea că, în domeniul investigării infracţiunilor informatice, previziunile sunt mai degrabă sumbre. Concret, se pare că infractorii sunt întotdeauna cu un pas înaintea anchetatorilor, ceea ce face ca prevenirea, descoperirea şi sancţionarea infracţiunilor cibernetice să fie extrem de dificil de realizat. Mediul informatic oferă condiţii propice pentru manifestarea intenţiilor infractorilor, iar aceştia vor profita de aceste condiţii. Totuşi, realitatea arată că, prin alocarea unor resurse semnificative, umane şi materiale, pot fi obţinute rezultate în lupta contra infracţiunilor informatice. Rămâne doar să sperăm că, în viitor, investigatorii vor reuşi să depăşească dificultăţile de cercetare a acestor infracţiuni şi vor putea să îi aducă în faţa justiţiei pe majoritatea infractorilor din mediul informatic, în paralel cu realizarea unei activităţi eficiente de prevenire a infracţionalităţii cibernetice.