UNIVERSITATEA BABEŞ-BOLYAI

FACULTATEA DE DREPT

TEZĂ DE DOCTORAT

Accesul neautorizat la un sistem informatic, frauda și falsul informatic

(cuprins și rezumat)

Conducător de doctorat:

Prof. univ. dr. Sergiu BOGDAN

Student-doctorand:

George Michail Rudolf ZLATI

CUPRINS

TITLUL II
ACCESUL NEAUTORIZAT
LA UN SISTEM INFORMATIC
(ART. 360 COD PENAL)

TITLUL III

FRAUDA INFORMATICĂ

(ART. 249 COD PENAL)

TITLUL IV
FALSUL INFORMATIC
(ART. 325 COD PENAL)

CUVINTE CHEIE

Acces neautorizat, fraudă informatică, fals informatic, sistem informatic, mijloc de stocare, date informatice, instrument de plată electronică, clonare pagini web, phishing, furt de identitate, fraude pe Internet.

REZUMAT

În această teză sunt analizate trei infracțiuni informatice: accesul neautorizat la un sistem informatic [art. 360 Cod pen.], frauda informatică [art. 249 Cod pen.] și falsul informatic [art. 325 Cod pen.]. În afara acestor trei infracțiuni, este analizat conceptul de criminalitate informatică și aspecte terminologice relevante, precum noțiunea de sistem informatic, instrument de plată electronică etc.

Infracțiunile informatice **au făcut obiectul a cel puțin câtorva monografii**,[1] inclusiv la momentul în care acestea erau cuprinse doar în legislația specială (Legea nr. 161/2003[2] și Legea nr. 365/2003[3]). În prezent, lucrările de specialitate ce analizează partea specială a noului Cod penal abordează automat și infracțiunile ce fac obiectul prezentei teze deoarece acestea au fost preluate din legislația specială în conținutului Codului penal – art. 249 [frauda informatică], art. 250 [efectuarea de operațiuni financiare în mod

[1] **Cu titlu de exemplu enumerăm următoarele lucrări:** I. Vasiu, *Criminalitatea informatică*, Ed. Nemira, Bucureşti, 1998; I. Vasiu, L. Vasiu, *Totul despre hackeri*, Ed. Nemira, Bucureşti, 2001; I. Vasiu, L. Vasiu, *Informatica juridică şi Drept informatic*, Ed. Albastră, Cluj, 2002; T. Amza, C.-P. Amza, *Criminalitatea informatică*, Ed. Lumina Lex, București, 2003; I. Vasiu, L. Vasiu, *Prevenirea criminalităţii informatice*, Ed. Hamangiu, Bucureşti, 2006; M. Dobrinoiu, *Infracţiuni în domeniul informatic*, Ed. C.H. Beck, Bucureşti, 2006; Ş. Prună, I.-C. Mihai, *Criminalitatea informatică*, Ed. Sitech, 2008; M. Dobrinoiu, *Criminalitatea informatică,* Ed. Academiei Naţionale de Informaţii, Bucureşti 2009; A. Trancă**,** I. Vasiu, L. Vasiu, *Criminalitatea în cyberspaţiu*, Ed. Universul Juridic, 2011; D.C. Trancă, *Infracţiunile informatice în noul Cod penal*, Ed. Universul Juridic, Bucureşti, 2014. **La nivel de drept comparat am putea enumera următoarele lucrări:** P.F., Cabana, *Las nuevas tecnologías en los delitos contra el patrimonio y el orden socioeconómico*, Ed. Tirant lo Blanch, Valencia, 2009; L. Cuomo, E. Razzante, *La nuova disciplina dei reati informatice*, Ed. Giappichelli, Torino, 2009; M. Quéméner, Y. Charpenel, *Cybercriminalité. Droit pénal appliqué*, Ed. Economica, Paris, 2010; A. Amato G. Saraceni, *I reati informatici. Elementi di teoria generali e principali figure criminose*, Ed. Giappichelli, Torino, 2015; G.B. Hoyos, *El delito de estafa informática*, Ed. Leyer, Bogotá, 2009; A. Cadoppi, S. Canestrari, A. Manna, M. Papa M. (dir.), *Cybercrime* [Kindle], Ed. UTET Giuridica, Milano, 2019; J. Clough, *Principles of Cybercrime*, second edition, Cambridge University Press, UK, 2015.

[2] Privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției (publicată în M.Of. nr. 279 din 21 aprilie 2003).

[3] Privind comerțul electronic republicată (publicată în M.Of. nr. 403 din 10 mai 2006).

fraudulos], art. 325 [falsul informatic], art. 360-365, art. 374 [pornografia infantilă] ș.a. Cod pen.

În ciuda existenței acestor analize doctrinare, în literatura de specialitate autohtonă **se simte în continuare nevoia unei analize aprofundate** în domeniu. Într-o abordare critică, s-ar putea susține că în ceea ce privește criminalitatea informatică nu ducem lipsă de literatură de specialitate, dar literatura de specialitate existentă până în momentul de față evidențiază nevoia unor completări. Iar aici ne referim la o analiză în profunzime asupra unor probleme relevante din perspectiva practicii judiciare și nu doar o prezentare generală și schematică a conținutului textelor de incriminare.

Un prim argument vizează problemele evidențiate în practica judiciară. În acest sens, în practica judiciară se observă adesea cum infracțiunile informatice ridică **probleme majore la nivel de interpretare** iar atât raporturile juridice dintre acestea (de exemplu, relația dintre falsul informatic şi frauda informatică), cât și raporturile dintre infracțiunile informatice și alte infracțiuni considerate ca fiind tradiționale (de exemplu, relația dintre frauda informatică și infracțiunea de înșelăciune), au generat o **practică judiciară neunitară**.

Or, o analiză a criticilor ce pot fi aduse numeroaselor soluții de practică judiciară ne determină să concluzionăm că acestea își găsesc de mult prea puține ori răspunsul în literatura de specialitate. Tocmai de aceea ne-am propus ca în prezenta teză să efectuăm o analiză amplă a practicii judiciare și identificarea unor soluții juridice concrete pentru fiecare problemă în parte ce a generat controverse ori dificultăți la nivel de interpretare și aplicare a textelor de incriminare.

Un alt doilea argument este acela că de prea multe ori analizele doctrinare – îndeosebi cele autohtone – vizează aspecte generale ori deja clarificate și de prea puține ori se concentrează pe chestiuni cu adevărat controversate ce ridică deja probleme ori care ar putea să apară în viitor. Având în vedere că rolul literaturii de specialitate nu este doar de a oferi răspuns la probleme actuale, ci și acela de a preîntâmpina discuții în vederea evitării unei viitoare practici judiciare neunitare, apreciem că prezenta teză este necesară și oportună.

În acest context, credem că inclusiv **o analiză aprofundată la nivel de drept comparat** devine o necesitate. Or, o recenzie a literaturii de specialitate autohtone ne arată că metoda abordării comparative este de prea puține ori folosită, iar atunci când este folosită trimiterile sunt făcute îndeosebi la dreptul american.

În ceea ce ne privește, nu avem vreo rezervă în a susține că dreptul american reprezintă un punct de referință în domeniul criminalității informatice. Totuși, raportat la prevederile naționale ce fac obiectul prezentei teze, dreptul american devine cu adevărat relevant doar din perspectiva infracțiunii de acces neautorizat la un sistem informatic [art. 360 Cod pen.], acolo unde literatura de specialitate[4] și jurisprudența este vastă și de o ținută științifică remarcabilă.[5] Credem așadar că pentru clarificarea noțiunilor de „acces" și „fără drept"[6] o incursiune în dreptul american este un pas important în orice cercetare științifică în domeniu.

În schimb, din perspectiva fraudei informatice și a falsului informatic credem că acest sistem de drept nu reprezintă cu adevărat un model pentru legiuitorul național. Dincolo de o analiză amplă cu privire la furtul de folosință [în engleză, *identity theft*] în general și conduitele tip *phishing*[7] în particular, nu credem că literatura de specialitate ori jurisprudența americană este în măsură să ofere răspunsuri relevante pentru problemele ce pot fi identificate în dreptul național în legătură cu aceste două infracțiuni.

De aceea, credem că atenția trebuie îndreptată și înspre alte sisteme de drept, precum cel spaniol, italian, german etc. În literatura de specialitate din aceste țări ori referitoare la aceste sisteme de drept, pot fi identificate analize ample la nivel conceptual pentru a delimita infracțiunea de fraudă informatică (art. 248.2 Cod pen. spaniol, art. 640-ter Cod pen. italian și secțiunea 263a Cod pen. german) de înșelăciunea tradițională.

Având în vedere că în jurisprudența națională majoritatea covârșitoare a cauzelor privind infracțiunea de fraudă informatică evidențiază o regretabilă confuzie între această infracțiune și înșelăciunea tradițională,[8] o asemenea incursiune în dreptul comparat

---

[4] Ne referim aici îndeosebi la materialele profesorului Orin Samuel Kerr ce reprezintă un punct de referință la nivel internațional în materia criminalității informatice. A se vedea cu titlu de exemplu, O.S., Kerr, *Cybercrime's scope: interpreting „access" and „authorization" in Computer Misuse Statues*, în „New York University Law Review", vol. 78, 2003; O.S. Kerr, *Norms of Computer Trespass,* în „Columbia Law Review", vol. 116, 2016; O.S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, în „Minnesota Law Review", vol. 94, 2010.

[5] Remarcabilă nu datorită faptului că ne-a determinat să achiesăm soluțiilor de practică judiciară, ceea ce nu a fost cazul, ci datorită faptului că orice concluzie la care s-a ajuns a avut în spate un întreg raționament logico-juridic ce de multe ori lipsește în motivarea instanțelor.

[6] În dreptul american făcându-se vorbire despre „lipsa autorizării".

[7] A se vedea cu titlu de exemplu L.L. Sullins, *„Phishing for a solution": domestic and international approaches to decreasing online identity theft*, în „Emory International Law Review", vol. 20, 2006.

[8] Astfel, în ipoteze de înșelăciuni prin mijloace informatice (licitații online ori vânzări de bunuri online) **unele instanțe rețin infracțiunea de înșelăciune:** C. Ap. București, secția a II-a penală, dec. nr. 421/2015; C. Ap. Piteşti, secția penală, dec. nr. 689/R/2008; C. Ap. Ploieşti, secția penală, dec. nr. 1084/2016; C. Ap. Ploieşti, secția penală, dec. nr. 804/2015. În schimb, **alte instanțe rețin infracțiunea de fraudă informatică:** C. Ap. Bacău, secția penală, dec. nr. 128/2011; C. Ap. Piteşti, secția penală, dec. nr. 496/2014; C. Ap. Piteşti, secția penală, dec. nr. 672/2013, C. Ap. Craiova, secția penală, dec. nr. 1113/2015; C. Ap.

reprezintă un demers util și necesar. Tocmai de aceea, așa cum urmează a se vedea pe parcursul tezei, trimiterile făcute la alte sisteme de drept sunt numeroase. Pe lângă dreptul spaniol, italian ori german s-au făcut trimiteri inclusiv la dreptul elvețian, francez, olandez etc.

Studiul falsului informatic din perspectiva dreptului comparat se dovedește într-o bună măsură problematic. Aceasta întrucât, în ciuda art. 7 din Convenția privind criminalitatea informatică, sistemele de drept de referință pentru dreptul național (dreptul italian, spaniol, german sau francez) nu au incriminat falsul informatic ca o infracțiune autonomă ori au avut o abordare cu totul diferită față de cea a legiuitorului român.

De asemenea, se observă că literatura de specialitate ezită în general să propună soluții concrete pentru soluționarea unor probleme reale la nivel de interpretare ori aplicare a textelor de incriminare.

În context, apreciem că în urma unei analize aprofundate a legislației naționale, prin raportare la elemente de drept comparat și ținând cont de dreptul european în materie, **se pot formula propuneri concrete de reformare a infracțiunilor informatice** supuse analizei ori a altor infracțiuni cu care acestea se află într-un raport problematic din punct de vedere juridic. Rolul literaturii de specialitate nu este doar acela de a aduce clarificări ori de a tranșa discuții controversate, ci și acela de a propune **soluții pentru simplificarea legislației penale** în contextul în care ne aflăm într-o continuă expansiune cantitativă și calitativă a dreptului penal, ce tinde să devină îngrijorătoare din perspectiva principiilor generale de drept.

La nivel de conținut, teza se va axa pe **analiza a trei infracțiuni informatice** şi anume accesul neautorizat la un sistem informatic (*Titlul II*), frauda informatică (*Titlul III*) şi falsul informatic (*Titlul IV*), fiecare infracțiune în parte urmând a beneficia de un **titlu distinct în cadrul tezei** pentru o mai bună sistematizare a materiei. Aceste trei titluri vor prezenta unele asemănări și anume: existența unui capitol referitor la raportul dintre reglementarea națională și prevederile anumitor instrumente juridice supranaționale, analizarea rațiunii și necesității incriminării și tratarea într-un capitol distinct a relației

---

București, secția a II-a penală, dec. nr. 637/2017; C. Ap. Alba Iulia, secția penală, dec. nr. 171/2015; C. Ap. Bacău, secția penală, dec. nr. 128/2011; C. Ap. Cluj, secția penală, dec. nr. 1801/2011; C. Ap. București, secția I penală, dec. nr. 938/2016; C. Ap. București, secția I penală, dec. nr. 1189/2016; C. Ap. București, secția a II-a penală, dec. nr. 1472/2017; C. Ap. Craiova, secția penală, dec. nr. 279/2017. Există chiar **instanțe chiar rețin un concurs de infracțiuni între înșelăciune și fraudă informatică:** ÎCCJ, secția penală, dec. nr. 3764/2013; C. Ap. Bacău, secția penală, dec. nr. 1012/2014, C. Ap. Bacău, secția penală, dec. nr. 1170/2015; C. Ap. București, secția a II-a penală, dec. 854/2016; C. Ap. Pitești, secția penală, dec. nr. 295/2011.

dintre infracțiunea ce face obiectul analizei și alte infracțiuni informatice, tradiționale, prevăzute în Codul penal sau în legislația specială.

De asemenea, având în vedere că toate infracțiunile informatice ce au făcut obiectul analizei se subsumează noțiunii de "criminalitate informatică" și reprezintă o transpunere în dreptul intern a unor instrumente juridice europene (Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice[9] ori Directiva 2013/40/EU privind atacurile împotriva sistemelor informatice și de înlocuire a Deciziei-cadru 2005/222/JAI a Consiliului[10]) ori internaționale (Convenția Consiliului Europei privind criminalitatea informatică[11]), a fost dedicat un titlu introductiv prin care s-a analizat **conceptul de criminalitate informatică** (Titlul I, Capitolul I) și **terminologia folosită** în cuprinsul textelor de incriminare ce vor face obiectul analizei (Titlul I, Capitolul II).

Primul titlu (intitulat „Aspecte introductive") a fost structurat în două capitole. Primul capitol a fost dedicat conceptului de „criminalitate informatică", iar cel de al doilea terminologiei folosite de legiuitor în cuprinsul unor texte de incriminare.

În **Capitolul I** (intitulat „Criminalitatea informatică") ne-am propus să evidențiem dificultatea definirii conceptului de „criminalitate informatică"[12] și riscurile utilizării unui asemenea concept în legislație. În primul rând, au fost identificate exemple de acte normative naționale ori europene în care se face trimitere la conceptul de „criminalitate informatică" (spre exemplu, Legea nr. 302/2004[13], Directiva 2018/1673/UE[14] etc.).

În context, s-a încercat a se puncta că utilizarea unui concept vag în conținutul unor instrumente juridice care ar trebui să exceleze la nivel de claritate și previzibilitate ar putea pune în discuție respectarea principiului legalității. De asemenea, s-a evidențiat riscul unor interpretări abuzive printr-o extindere nejustificată a sferei de aplicabilitate a normei penale, cu riscul încălcării principiului proporționalității.

În continuare, s-a procedat la o prezentare succintă a principalelor orientări legate de definirea conceptului de „criminalitate informatică". În acest sens, s-a insistat asupra

[9] Publicată în JOUE L 069/67.

[10] Publicată în JOUE L 218/8 din 14.08.2013.

[11] Ratificată prin Legea nr. 64/2004 pentru ratificarea Convenției Europei privind criminalitatea informatică, adoptată la Budapesta la 23 noiembrie 2001 (publicată în M.Of. nr. 343 din 20 aprilie 2004).

[12] În acest sens și S. Gordon, R. Ford, *On the definition and classification of cybercrime*, în „Journal of Computer Virology", nr. 2/2006, p. 13.

[13] Privind cooperarea judiciară internațională în materie penală republicată (M.Of. nr. 707 din 21 septembrie 2015).

[14] Privind combaterea prin măsuri de drept penal a spălării banilor (JOUE L 284 din 12 noiembrie 2018).

definiției larg răspândite[15] ce stabilește conținutul criminalității informatice prin raportare la trei categorii de infracțiuni: **(1)** infracțiuni îndreptate împotriva sistemelor ori datelor informatice – acestea fiind „ținta" conduitei infracționale; **(2)** infracțiuni unde sistemul informatic este doar un mijloc pentru a comite infracțiunea – caz în care sistemul informatic este doar o „unealtă" pentru realizarea conduitei infracționale; **(3)** activități infracționale ce sunt incidentale pentru comiterea altor infracțiuni tradiționale.

Tot cu privire la conținutul conceptului de criminalitate informatică a fost identificată practică judiciară națională la nivelul Înaltei Curți de Casație și Justiție,[16] în care fie s-a încercat definirea conceptului fie au fost incluse anumite infracțiuni ori conduite infracționale în acest concept.

În **Capitolul II** (intitulat „Aspecte terminologice") ne-am propus să analizăm *in extenso* noțiunea de „sistem informatic". Analiza a avut ca premisă instrumentele juridice supranaționale ce au reprezentat un izvor de drept pentru legiuitorul național. Ne referim în acest sens la Convenția Consiliului Europei privind criminalitatea informatică, Decizia-cadru 2005/222/JAI privind atacurile împotriva sistemelor informatice și Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice.

În continuare, s-a analizat definiția sistemului informatic în dreptul intern [art. 181 alin. (1) Cod pen.] în încercarea de a identifica și explica criteriile legale pentru calificarea unui anumit dispozitiv drept sistem informatic. Ne-am referit în acest sens la sistemul informatic ca dispozitiv [componenta hardware] și la prelucrarea automată a datelor informatice prin intermediul unui program informatic [componenta software]. S-au făcut trimitere inclusiv la elemente de drept comparat, încercând a se evidenția două modele de abordare: cel în care sistemul informatic beneficiază de o definiție legală (SUA, Canada,

[15] A se vedea în acest sens J. Clough, *Principles of Cybercrime...*, precit., p. 10-11; S. Fafinski, *Computer Misuse. Response, regulation and the law*, Willian Publishing, UK, 2009, p. 5; J. Clough, *Cybercrime*, în „Commonwealth Law Bulletin", vol. 37, nr. 4/2011, p. 672; S.W. Brenner, *U.S. Cybercrime Law: Defining Offenses*, în „Information Systems Frontiers", vol. 6, nr. 2/2004, p. 117; J. Müller, *La cybercriminalité économique au sens étroit. Analyse approfondie du droi suisse et aperçu de quelqyes droits étrangers*, Ed. Schulthees Médias Juridiques, Zurich, 2012, p. 12; H. Lu, B. Liang, M. Taylor, *A Comparative Analysis of Cybercrimes and Governmental Law Enforcement in China and the United States*, în „Asian Criminology", vol. 5, 2010, p. 126; I. Vasiu, L. Vasiu, *The Cybercrime Challenge: Does the Romanian Legislation Answer Adequately*, în „Law Review", vol. III, nr. 2/2013, p. 45-46; D. Chilstein, *Législation sur la cybercriminalité en France*, în „Revue internationale de droit comparé", nr. 2/2010, p. 553; S.W. Brenner, *Cybercrime. Criminal Threats from Cyberspace*, Ed. Praeger, SUA, 2010, p. 39-47.

[16] A se vedea în acest sens, ÎCCJ, secția penală, dec. nr. 1415/2014 (despre definirea conceptului); ÎCCJ, secția penală, dec. nr. 1396/2013 (despre apartenența conduitelor tip phishing la conceptul de criminalitate informatică); ÎCCJ, secția penală, dec. nr. 2346/2012 (despre infracțiunile ce fac parte din conceptul de criminalitate informatică).

Olanda, Austria etc.) și cel în care interpretarea noțiunii a fost lăsată în sarcina literaturii de specialitate și a jurisprudenței (Regatul Unit, Italia, Franța, Spania etc.).

Centrul de greutate al analizei noțiunii de „sistem informatic" vizează o analiză *in concreto* a numeroase exemple de sisteme informatice ori exemple problematice din perspectiva calificării juridice, inclusiv prin raportare la practica judiciară. Cu titlu exemplificativ, au fost avute în acest sens următoarele dispozitive: servere prin care se furnizează anumite servicii ori pe care sunt găzduite anumite pagini web; sistemul electronic de tranzacționare pe piața de capital; bancomatele, terminalele POS, ceasurile inteligente, televizoarele inteligente, aparatele de jocuri de noroc, dispozitivele din categoria *Internet of Things*, dispozitivele tip skimmer, autovehicule moderne etc. În afara acestor dispozitive au fost mai analizate bazele de date, paginile web, Internetul, rețeaua de comunicații electronice, cartelele SIM, instrumentele de plată electronică etc. Toate acestea în încercarea de a clarifica sfera de aplicabilitate a noțiunii „sistem informatic" și de a evidenția eventualele controverse ce pot apărea în legătură cu această noțiune.

După identificarea tuturor acestor probleme a fost avută în vedere inclusiv o posibilă reconceptualizare a noțiunii, începând de la o redefinire a acesteia. S-a analizat în acest sens posibilitatea de a introduce elemente suplimentare în conținutul definiției precum funcția principală a sistemului informatic, caracterul autonom ori anumite criterii negative care să limiteze în mod rezonabil sfera de aplicabilitate a noțiunii. Nu în ultimul rând, s-a propus o interpretare restrictivă a definiției actuale în încercarea de a rezolva posibilele controverse ce ar putea apărea în legătură cu utilizarea unor aparate casnice, a unui televizor inteligent, a unei multifuncționale etc.

În afara noțiunii „sistem informatic" au fost analizate noțiunile „program informatic", „date informatice" și „instrument de plată electronică". Toate aceste analize au urmărit în cele din urmă clarificarea unor noțiuni ce fac parte din elementele constitutive ale unor infracțiuni sau prezintă o relevanță aparte din perspectiva dreptului procesual penal.

În ceea ce privește instrumentul de plată electronică a fost analizată inclusiv Directiva (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar și de înlocuire a Deciziei-cadru 2001/413/JAI a Consiliului.[17] Cu toate că instrumentul de plată electronică este avut în vedere în mod expres doar de art. 250 Cod pen. [efectuarea de operațiuni financiare în mod fraudulos],

[17] JOUE L 123/18 din 10 mai 2019.

Directiva (UE) 2019/713 se referă inclusiv la monedele virtuale. Or, acestea nu sunt incluse de *lege lata* în noțiunea de instrument de plată electronică ceea ce implică necesitatea de a testa aplicabilitatea infracțiunii prevăzute de art. 249 Cod pen. [frauda informatică] în vederea acoperirii acestui aparent „vid legislativ".

Al doilea titlu al tezei (intitulat „Accesul neautorizat la un sistem informatic") reprezintă o analiză amplă a infracțiunii prevăzute la art. 360 Cod pen., cu trimiteri repetate la elemente de drept comparat și la o vastă jurisprudență națională și din dreptul comparat.

Pornind de la sursa de inspirație a legiuitorului național și continuând cu modul de transpunere în dreptul intern a Convenției privind criminalitatea informatică și a Directivei 2013/40/UE, au fost evidențiate probleme de interpretare și controverse ce ar putea apărea în practica judiciară raportat la reglementarea actuală. Au fost analizate de asemenea atât decizii ale Curții Constituționale identificate în legătură cu infracțiunea de acces neautorizat la un sistem informatic,[18] cât și recursul în interesul legii soluționat de către Înalta Curte de Casație și Justiție prin decizia nr. 15/2013.[19]

Înainte de a se analiza propriu-zis conținutul infracțiunii s-a încercat clarificarea rațiunii incriminării. Prin acest demers nu ne-am propus doar justificarea introducerii unui text de incriminare autonom care să acopere accesul neautorizat la un sistem informatic, ci s-a urmărit inclusiv evidențierea unor posibile asemănări cu infracțiunea de violare de domiciliu [art. 224 Cod pen.]. Scopul unui asemenea demers a fost acela de a identifica anumite puncte de legătură care, în ciuda diferenței la nivel conceptual, să ajute la tranșarea unor aspecte în legătură cu infracțiunea de acces neautorizat la un sistem informatic. Ne referim aici la identificarea subiectului pasiv, delegarea autorizării din partea titularului sistemului informatic, raportul dintre accesul neautorizat și depășirea limitărilor autorizării ori păstrarea neautorizată a accesului etc.

Din perspectiva conținutului infracțiunii analiza a fost una *in extenso*, încercându-se clarificarea tuturor aspectelor problematice ce ar putea să apară în legătură cu acest text de incriminare. Spre exemplu, în ceea ce privește subiectul pasiv ne-am propus elaborarea unei teorii pentru identificarea titularului sistemului informatic, prin raportare la existența unui drept de folosință consolidat, încercând de asemenea lămurirea raportului dintre pluralitatea de subiecți pasivi și pluralitatea de sisteme informatice accesate.

[18] A se vedea în acest sens, decizia Curții Constituționale nr. 183/2018 (publicată în M.Of. nr. 486 din 13.06.2018) și decizia Curții Constituționale nr. 353/2018 (publicată în M.Of. nr. 650 din 26.07.2018).

[19] A se vedea în acest sens, ÎCCJ, Completul competent să judece recursul în interesul legii, dec. nr. 15/2013 (publicată în M.Of. nr. 760 din 6.12.2013).

Analiza laturii obiective a avut ca premisă tipologia accesului neautorizat la un sistem informatic în dreptul comparat pentru a se evidenția discrepanțele majore cu privire la reglementarea acestei infracțiuni. În continuare, s-a încercat în primul rând clarificarea raportului dintre accesul la un sistem informatic și accesul la un mijloc de stocare a datelor informatice, prin raportare la diverse ipoteze problematice. Aceasta pentru a evidenția o posibilă problemă legată de sfera de aplicabilitate a infracțiunii având în vedere omisiunea legiuitorului de a incrimina nu doar accesul la un sistem informatic, ci și accesul la un mijloc de stocare a datelor informatice.

Analiza conduitei incriminate (accesul) s-a bazat inclusiv pe o vastă literatură de specialitate și jurisprudență relevantă cu privire la semnificația noțiunii de acces. Printr-un asemenea demers s-a încercat identificarea unor exemple clare de acces și exemple susceptibile să genereze controverse.

Au fost avute în vedere în acest sens o gamă largă de ipoteze precum: folosirea de la distanță a unui sistem informatic prin intermediul *Team Viewer*; accesarea unu cont bancar online; autentificarea (accesul) fără drept la interfața de administrare a unei pagini web; accesarea unui bancomat prin intermediul unui instrument de plată electronică; alterarea fără drept a unei pagini web prin înlocuirea ori modificarea modului în care aceasta este afișată; transmiterea unui e-mail; atacurile de tip *denial-of-service* [*DoS attack*]; scanarea porturilor [*port scanning*]; obținerea de date informatice prin *phishing*; contrafacerea de pagini web [*web spoofing*]; punerea în vânzare pe Internet a unor bunuri fictive; interacțiunea fizică cu un bancomat; efectuarea de plăți la un terminal POS; efectuarea de plăți online; accesarea unor adrese URL (nepublice) ale unor pagini web (publice); copierea fără drept de date informatice din sistemul informatic aparținând unei terțe persoane; utilizarea unui program informatic tip *keylogger* pentru a intercepta datele introduse de la tastatură de către victimă; infectarea unor sisteme informatice cu un program malițios (virus) etc.

Concluzia cu privire la noțiunea de „acces” a fost aceea că aceea că aceasta trebuie să aibă în vedere o interacțiune la nivel logic prin intermediul căreia agentul să poată beneficia de resursele ori/și funcțiile respectivului sistem informatic.

Lipsa autorizării, prin raportare la noțiunea „fără drept”, a făcut de asemenea obiectul unei analize *in extenso* în încercarea de a tranșa anumite controverse. Similar analiza noțiunii de acces au fost avute în vedere numeroase ipoteze identificate în practică judiciară. Cu titlu de exemplu, facem trimitere la următoarele: lipsa autorizării exprese a

administratorului de rețea; utilizarea fără drept a unui card de carburant; introducerea de anunțuri fictive pe platforma eBay; crearea de conturi fictive pe platforma eBay; accesarea unei pagini web restricționate de către angajat cu un scop fraudulos; utilizarea unui laptop bun comun al soților; accesarea contului de Internet banking de către unul dintre soți; accesarea unui cont de e-mail prin folosirea unui parole primite anterior; verificarea situației fiscale a unor contribuabili din altă jurisdicție etc.

Pentru a evidenția cât mai bine complexitatea analizei acestei noțiuni a fost analizată inclusiv jurisprudența Curții de Casație italiene care a extins în mod excesiv sfera de aplicabilitate a infracțiunii de acces neautorizat [acces abuziv în dreptul italian] și teoriile apărute în dreptul american cu privire la lipsa autorizării (teoria contractuală, teoria încălcării unei obligații de loialitate, teoria depășirii unor măsuri de securitate și teoria revocării autorizării). Ulterior tuturor acestor analize s-a încercat identificarea unui *framework* rezonabil prin stabilirea limitelor noțiunii „fără drept" raportat la o serie de criterii obiective adjuvante.

Momentul consumării infracțiunii și delimitarea dintre tentativă și simplele acte de pregătire fără semnificație penală au făcut de asemenea obiectul unei analize detaliate. În context, dincolo de încercarea de a identifica momentul consumării infracțiunii și de a analiza desistarea și împiedicarea producerii rezultatului, au fost avute în vedere ipoteze concrete care ar putea ridica probleme din perspectiva calificării juridice a acestora drept acte de executare ori acte pregătitoare.

Formele agravate ale infracțiunii de acces neautorizat la un sistem informatic (în scopul obținerii de date informatice [art. 360 alin. (2) Cod pen.] și prin depășirea măsurilor de securitate [art. 360 alin. (3) Cod pen.]) beneficiază de o secțiune distinctă. În ceea ce privește agravanta prevăzută la art. 360 alin. (2) Cod pen. s-a analizat conținutul scopului special și relația cu alte infracțiuni. În schimb, agravanta prevăzută la art. 360 alin. (3) Cod pen. a beneficiat de o analiză mai detaliată, fiind atinse aspecte precum: rațiunea incriminării formei agravate, natura măsurilor de securitate (fizice, organizaționale ori logice) ori caracteristici ale acestora.

Cu privire la caracteristicile măsurilor de securitate s-a punctat inclusiv pe diferențierea dintre efectivitatea și fiabilitatea (eficacitatea) măsurilor de securitate, în încercarea de a oferi criterii adjuvante pentru stabilirea unor limite rezonabile de aplicabilitate a acestei agravante. De asemenea, au fost descrise anumite proceduri specifice de interzicere ori de restricționare a accesului (spre exemplu, utilizarea unor

elemente biometrice ori setarea adreselor MAC), împreună cu clarificarea dispozitivelor ori a programelor informatice prin intermediul cărora se poate atinge același scop.

Nu în ultimul rând, au fost analizate modalitățile prin care se poate ajunge la depășirea măsurilor de securitate, aspect ce a generat pe alocuri inclusiv o practică judiciară neunitară. În context, a fost avută în vedere obținerea frauduloasă a datelor de autentificare de la victimă, folosirea acestora după pierderea autorizării sau utilizarea unor date reale în vedere autentificării.

Ultimele două capitole (Capitolul VI și Capitolul VII) ale Titlului II se referă la relația infracțiunii de acces neautorizat la un sistem informatic cu alte infracțiuni prevăzute în Codul penal sau în legislația specială și reformarea art. 360 Cod pen. Cea mai relevantă discuție ține de soluționarea raportului dintre accesul neautorizat la un sistem informatic și violarea secretului corespondenței [art. 302 Cod pen.]. În acest sens, s-a argumentat *in extenso* în sensul reținerii doar a infracțiunii prevăzute de art. 360 Cod pen. în ipoteza accesării corespondenței electronice, în ciuda unor opinii doctrinare și jurisprudențiale în sens contrar.

Al treilea titlu al tezei (intitulat „Frauda informatică") reprezintă de asemenea o analiză amplă a infracțiunii prevăzute la art. 249 Cod pen., cu trimiteri la elemente de drept comparat.

Dincolo de analiza sursei de inspirație a legiuitorului național, modalitatea de transpunere în dreptul intern a art. 8 din Convenția privind criminalitatea informatică și analiza necesității de a transpune în viitor prevederile Directivei (UE) 2019/713 privind combaterea fraudelor și a contrafacerii în legătură cu mijloacele de plată fără numerar, a fost analizată *in extenso* rațiunea și necesitatea incriminării fraudei informatice. S-a analizat în acest sens posibilul conflict la nivel conceptual între frauda informatică și înșelăciunea tradițională în încercarea de a concluziona în ce măsură înșelăciunea tradițională poate acoperi conduitele specifice fraudei informatice.

Din perspectiva analizei conținutului infracțiunii de fraudă informatică accentul a fost pus pe o analiză *in concreto* a fiecărei modalități de comitere a faptei, cu trimiteri la ipoteze ce au fost avute în vedere în practica judiciară ori în literatura de specialitate. Astfel, cu privire la fiecare modalitate de comitere în parte, dincolo de a clarifica conținutului respectivei modalități, au fost analizate ipoteze care se pliază pe conceptul de fraudă informatică și ipoteze care ar trebui să se afle sub incidența altor texte de incriminare.

În context, în ceea ce privește **modalitatea introducerii de date informatice** au fost analizate ipoteze precum furtul de monede virtuale, reîncărcarea unei cartele prepay, mărirea „artificială” a soldului contului bancar, licitațiile online frauduloase, activitățile de *phishing* și *pharming*, efectuarea de tranzacții offline, folosirea unui *spyware dialer*, „minarea” de monede virtuale (*crypto-jacking*) etc.

Pentru **modalitatea modificării de date informatice** au fost avute în vedere ipoteze precum efectuarea unui transfer de fonduri, modificarea soldului într-un cont bancar, menținerea ca activat a unui anumit serviciu în vederea facturării suplimentare, alterarea conținutului unei pagini web etc. Cu toate că **modalitatea ștergerii de date informatice** nu este des întâlnită în practica judiciară au fost analizate ipoteze problematice legate de utilizarea unui magnet asupra unui mijloc de stocare a datelor informatice sau ștergerea unor debite din baza de date. În ceea ce privește **modalitatea restricționării accesului la datele informatice** a fost analizată îndeosebi prin raportare la ipoteza restricționării accesului la anumite conturi prin schimbarea parolei de acces la la conduitele de tip *ransomware*. Nu în ultimul rând, **modalitatea împiedicării în orice mod a funcționării unui sistem informatic** a scos în evidență problematica manipulării jocurilor electronice de noroc, a interacțiunii logice cu un bancomat fără a se utiliza un instrument de plată electronică, interacțiunea fizică cu un bancomat (metoda „furculița”), dezactivarea unor dispozitive electronice de protecție pentru sustragerea unui anumit bun etc.

Dincolo de analiza acestor conduite comisive ori posibilitatea de a reține comisiunea prin omisiune prin raportare la instituția poziției de garant (art. 17 Cod pen.), a fost analizată urmarea constând în producerea unei pagube și beneficiul material din conținutul scopului special prevăzut de art. 249 Cod pen.

Din perspectiva momentului consumării infracțiunii de fraudă informatică, principala analiză a vizat identificarea actelor preparatorii care nu sunt susceptibile să intre în sfera tentativei. Au fost analizate în acest sens îndeosebi accesul neautorizat la un sistem informatic și activitatea de phishing.

Similar cu infracțiunea de acces neautorizat la un sistem informatic ultimele două capitole sunt dedicate relației infracțiunii de fraudă informatică cu alte infracțiuni prevăzute în Codul penal sau în legislația specială și reformarea art. 249 Cod pen.

Al patrulea titlu al tezei (intitulat „Falsul informatic”), similar cu frauda informatică și accesul neautorizat la un sistem informatic reprezintă o analiză amplă a

infracțiunii prevăzute la art. 325 Cod pen., cu trimiteri la elemente de drept comparat. Studiul falsului informatic din perspectiva dreptului comparat a fost totuși limitat de faptul că, în ciuda art. 7 din Convenția privind criminalitatea informatică, sistemele de drept de referință pentru dreptul național (dreptul italian, spaniol, german sau francez) nu au incriminat falsul informatic ca o infracțiune autonomă ori au avut o abordare cu totul diferită față de cea a legiuitorului român.

În încercarea de a conceptualiza infracțiunea de fals informatic s-a pornit de la conceptul de înscris tradițional și s-a efectuat o paralelă între funcțiile acestuia și datele informatice relevante din perspectiva falsului informatic. A fost avută așadar în vedere funcția de perpetuare, probatorie și de garanție pentru a încerca efectuarea unei corespondențe între datele informatice asupra cărora intervine agentul și conceptul de document electronic ca echivalent al înscrisului tradițional.

Analiza laturii obiective a infracțiunii de fals informatic a urmat aceeași abordare precum în cazul fraudei informatice și a accesului neautorizat la un sistem informatic. S-a insistat așadar asupra unor ipoteze din practica judiciară, acestea fiind analizate astfel încât să se poată concluziona în ce măsură și-ar putea găsi aplicabilitatea art. 325 Cod pen. ori este incident un alt text de incriminare.

În ceea ce privește **modalitatea introducerii de date informatice** au fost analizate ipoteze precum contrafacerea de pagini web (*web spoofing*), simularea poștei electronice (e-mail *spoofing*), utilizarea fără drept a unei semnături electronice, introducerea de date informatice (informații) false în sistemul ECRIS, crearea de profile (conturi) false sau fictive pe rețelele de socializare, clonarea unei cartele SIM, publicarea de anunțuri fictive pe diverse platforme online, crearea unui duplicat după un document informatic etc. **Modalitatea modificării de date informatice** a fost analizată prin raportare la ipoteze precum modificarea notei de la BAC într-un catalog digital, modificarea numărului de telefon asociat unui cont bancar, modificarea denumirii și prețului unui produs, modificarea numărului de telefon (*caller ID spoofing*), falsificarea unei adrese IP (IP *spoofing*) etc. În ceea ce privește **modalitatea ștergerii de date informatice** a fost avută în vedere în primul rând ștergerea unor debite dintr-o bază de date. Nu în ultimul rând, referitor la **modalitatea restricționării accesului la datele informatice**, a fost analizată situația dezactivării opțiunii de Home Banking sau restricționarea accesului procurorului la anumite documente electronice prin parolarea acestora.

Spre deosebire de frauda informatică și accesului neautorizat la un sistem informatic, în Titlul IV dedicat infracțiunii de fals informatic se regăsesc două capitole dedicate relației dintre falsul informatic și falsurile tradiționale și relevanța falsului informatic în contextul furtului de identitate.

În ceea ce privește relația dintre falsul informatic și falsul tradițional s-a evidențiat în primul rând paralelismul deficitar din perspectiva limitelor de pedeapsă, sancționării tentativei, incriminării uzului de fals etc. Având drept premisă aceste discrepanțe existente între cele două categorii de infracțiuni au fost analizate diferite ipoteze deosebit de problematice printre care: contrafacerea sau alterarea unui înscris tradițional pe un sistem informatic; continuarea acțiunii de alterare după tipărirea conținutului documentului electronic pe suport hârtie; contrafacerea sau alterarea unei facturi electronice etc.

Toate aceste ipoteze analizate atât din perspectiva falsului informatic cât și a falsului tradițional au avut scopul de a evidenția dificultatea identificării momentului în care putem discuta despre un înscris tradițional ori a actului de executare ori consecințele juridice problematice ale metamorfozei falsului informatic într-un fals tradițional.

În ceea ce privește furtul de identitate, s-a încercat clarificarea acestui concept prin raportare la trei faze acceptate la nivel doctrinar[20] și anume: faza obținerii datelor personale; faza interacțiunii cu datele personale obținute în primă fază; faza utilizării efective a datelor personale. Având în vedere aceste trei faze ce înglobează conceptul de furt de identitate s-a analizat relevanța infracțiunii de fals informatic. În context, a fost analizată activitatea de phishing și alte activități conexe susceptibile de a atrage aplicabilitatea art. 325 Cod pen.

Similar cu infracțiunea de acces neautorizat la un sistem informatic ultimele două capitole sunt dedicate relației infracțiunii de fraudă informatică cu alte infracțiuni prevăzute în Codul penal sau în legislația specială și reformarea art. 325 Cod pen.

Summa summarum, prezenta teză reprezintă un studiu aprofundat cu privire la infracțiunea de acces neautorizat la un sistem informatic, frauda și falsul informatic. Analiza se axează în principal pe analiza unor probleme de drept ignorate în mare parte de

[20] A se vedea în acest sens S. Schjolberg, *The History of Cybercrime 1976-2014,* Cybercrime Research Institute, Cologne, 2014 p. 128; M. Gercke, *Internet-related identity theft,* Discussion Paper (Council of Europe), 2007, p. 13; J. Clough, *Principles of Cybercrime, second edition, precit.*, p. 238; A.N. Martín, *Identity theft and international criminal policy: manufacturing consent,* în „Cahiers de défense sociale", nr. 36/2009-2010, p. 25.

în literatura de specialitate autohtonă, dar care au ridicat probleme deosebite în practica judiciară.