IN DUBIO PRO REO: APĂRAREA CAL TROIAN ÎN CAUZELE DE CRIMINALITATE INFORMATICĂ

IN DUBIO PRO REO: THE TROJAN HORSE DEFENSE IN CYBERCRIME CASES

Lect. univ. **Svetlana PURICI**[1]
Facultatea de Drept
Universitatea de Stat din Republica Moldova

Abstract

Internet connectivity, the ability to remote control a computer system and the automation of crimes committed through or against the information systems by means of malware programs, without the knowledge of the rightful owner, raises a whole series of difficult challenges for the investigators and for the legal practitioners în establishing beyond any reasonable doubt the real author of a computer crime in cases where the defendant claims that someone else has committed the crime, especially given the high statistical occurrence în real life of such malware infections.

Rezumat

Conectarea la Internet, capacitatea de a controla de la distanță sisteme informatice precum și automatizarea cu ajutorul programelor malițioase a comiterii de activități din sfera ilicitului penal prin intermediul sistemelor informatice, fără știrea utilizatorului sau proprietarului de drept al acestora, ridică o serie întreagă de probleme atât investigatorilor cât și practicienilor dreptului în stabilirea dincolo de orice îndoială rezonabilă a autorului real al unei fapte penale din sfera criminalității informatice în cauzele în care învinuitul neagă comiterea faptei, aceasta mai cu seamă în lumina statisticilor îngrijorătoare privind frecvența cu care se întâlnesc în societate sisteme informatice infectate ce sunt utilizate în comiterea de infracțiuni.

[1] Autorul este Lector universtar la Departamentul Drept Procedural, Facultatea de Drept, Universitatea de Stat din Republica Moldova, disciplina Criminalistica. E-mail: purici.svetlana@gmail.com

CUPRINS

I. PREAMBUL

Interconectarea și frecvența mare a infectării sistemelor informatice cu programe capabile să desfășoare în mod automatizat activități dintre cele mai diverse, inclusiv din sfera ilicitului penal, ori să ofere control de la distanță unei terțe persoane, fără știrea deținătorului sau utilizatorului de drept al sistemului informatic, ridică probleme deosebite atât organelor de urmărire penală cât și practicienilor la stabilirea făptuitorului real cu un grad de certitudine dincolo de orice îndoială rezonabilă.

Simpla prezență într-un sistem informatic conectat la rețeaua Internet a unor materiale ilegale, spre exemplu fotografii înfățișând minori în ipostaze sexuale explicite, nu poate justifica prezumția[2] că deținătorul ori utilizatorul de drept al sistemului informatic, chiar dacă este singura persoană care a avut acces fizic la sistem, este și făptuitorul real, fiind necesară eliminarea prin probe a ipotezelor alternative de comitere a faptei penale de către terțe persoane, ori în mod automatizat prin acțiunea unui program malițios de tipul virușilor informatici.

II. APĂRAREA CAL TROIAN. NOȚIUNE

Una din cele mai frecvent întâlnite strategii de apărare în cazul infracțiunilor informatice o constituie apărarea tip Cal Troian[3], în care inculpatul sau suspectul neagă faptul că ar fi autorul faptei și susține că infracțiunea a fost săvârșită, fie de către un terț prin controlul de la distanță a sistemului informatic infectat cu un program malițios de tip Virus sau Cal Troian ce oferea acces (*back door*)[4] atacatorului real, fie, că fapta a fost comisă în mod automat de către un astfel de program malițios care executa automat un set predefinit de instrucțiuni, în ambele situații, fără știrea utilizatorului sau deținătorul legitim al sistemului informatic.

O variantă a acestei apărări, la fel de frecvent întâlnită o constituie invocarea nepriceperii utilizatorului care susține, spre exemplu, că nu a avut și intenția de a pune la dispoziție materialele ilegale descărcate prin sistemele de partajare de fișiere și nu a știut că programul de partajare punea automat la dispoziție în rețea documentele descărcate, apărare întâlnită în special în cauze în care punerea la dispoziție constituie agravantă.[5]

Prin invocarea acestei posibilități, se induce îndoiala rezonabilă asupra făptuitorului real, ori se urmărește reliefarea reprezentării pe care inculpatul a avut-o asupra faptei, în special în cauze privitoare la descărcarea sau deținerea de materiale ilegale (ex. pornografie infantilă) ori în cazul accesării fără drept a unui sistem informatic, al transferului fără drept de date informatice precum și în cazul perturbării sistemelor informatice

---

[2] C. Driga, S. Purici, *Fighting the classical crime-scene assumptions. Critical aspects în establishing the crime-scene perimeter în computer-based evidence cases*, în "CKS-Challenges of the Knowledge Society", "Nicolae Titulescu" University Publishing House (2016), ISSN 2359-9227, documentul este disponibil online la adresa http://cks.univnt.ro/download/156_cks_2016_online_journal.pdf, ultima accesare 1 oct 2016.

[3] Calul Troian este o aplicație malițioasă, de tip backdoor, disimulat într-un program legitim și care, odata lansat în execuție, instalează pe computerul țintă încărcătura logică dăunătoare (ex. viruși, keylogger etc.). http://e-crime.ro/ecrime/site/index.php/acasa/glosar/, ultima accesare 1 oct 2016,

[4] Backdoor este unul dintre cei mai periculoși cai troieni. Adesea, este transmis ca un atașament atractiv pentru utilizatorul vizat, putând fi „camuflat" drept joc video, aplicație multimedia sau documente. În general, se instalează automat la vizitarea unui website infectat și oferă celui care l-a trimis posibilitatea de a accesa de la distanță sistemul de operare al mașinii de calcul atacate și de a intra în posesia datelor personale ale utilizatorului, mesajelor de email, documentelor stocate etc. Specialiștii apreciază destul de dificilă eliminarea din sistem a acestui tip de Troian.

5 United States v. Dodd, 598 F.3d 449, 451-53 (8th Cir. 2010). Documentul este disponibil online la adresa: https://casetext.com/case/us-v-dodd-21#p451, ultima accesare 25 noiembrie 2016 și United States v. Creel783 F.3d 1357, 1357 (11th Cir. 2015). Documentul este disponibil online la adresa: https://casetext.com/case/united-states-v-creel-7, ultima accesare 25 noiembrie 2016.

(cazul atacurilor DDoS[6]).

Denumirea de Apărare Cal Troian își are aparent originea în primele cauze documentate la nivelul anului 2003 în Marea Britanie și SUA[7] în care inculpații au negat comiterea faptelor, susținând că acestea au fost comise de programe malițioase de tip Cal Troian, o serie dintre inculpați fiind achitați în urma constatării prezenței în sistemul informatic a astfel de programe informatice, neputându-se identifica dincolo de orice îndoială rezonabilă făptuitorul real în aceste condiții, relevante fiind pentru Marea Britanie cauzele Karl Schofield (aprilie 2003), Julian Green (iulie 2003), Aaron Caffrey (octombrie 2003) iar pentru SUA cauzele Eugene Pitts (august 2003), Brian Bass (septembrie 2003), Michael Aaron O'Keefe (noiembrie 2004)[8]. Cu toate acestea, denumirea este una generică, acțiunile ilegale putând fi comise și de alte programe malițioase precum virușii ori viermii informatici (*computer worm)*[9].

Programele tip Cal Troian sunt acele programe informatice care au aparent o funcție utilă, inofensivă, pe care utilizatorul le instalează pentru utilitatea aparentă și care maschează funcționalități dăunătoare precum descărcarea de viruși, criptarea documentelor și cererea subsecventă de plată a unei răscumpărări (*ransomware*), descărcarea sau traficul de materiale ilegale, lansarea unor atacuri informatice asupra altor sisteme informatice ori oferirea controlului total de la distanță asupra sistemului informatic în care au fost instalate, fără știrea utilizatorului legitim al sistemului.

Apărarea Cal Troian urmărește aplicarea regulii "in dubio pro reo" ca și complement al prezumției de nevinovăție contestând identificarea făptuitorului și având în practica judiciară șanse de succes doar în măsura înțelegerii de către practicieni și instanțe a realităților societății digitale, mai cu seamă în cauzele în care trimiterea în judecată s-a făcut exclusiv pe baza probelor digitale incriminatoare prelevate din sistemul informatic al suspectului ori inculpatului (ex. fotografii cu minori în ipostaze sexuale explicite) și fără a adresa corespunzător și elimina aspectele de posibil control de la distanță asupra sistemului informatic, ori virușii existenți care ar fi putut comite fapta în mod automatizat, precum și în cauzele în care percheziția informatică nu este completată și de alte procedee probatorii precum supravegherea operativă, documentarea profilului persoanei investigate, operațiuni financiare în legătură cu fapta și altele similare menite a-l plasa pe inculpat "la tastatură" la momentul comiterii faptei, ori a proba distinct fapta sub aspectul laturii subiective, așa cum o indică de altfel manualele de bune practici în investigarea infracțiunilor de criminalitate informatică.

III. O ÎNDOIALĂ REZONABILĂ CONFORM REALITĂȚILOR TEHNICE ȘI A STATISTICILOR

Realitatea socială ne arată faptul că toate aceste situații sunt posibile și plauzibile având o frecvență foarte mare în societate, realitate care impune luarea lor în considerare de către organele de urmărire penală și de către instanțe și acordarea unei atenții sporite identificării făptuitorului real, neputându-se prezuma din simpla prezență a materialelor ilegale în sistemul informatic aparținând suspectului ori inculpatului că acesta se face vinovat de comiterea faptei, în lipsa unor probe suplimentare pe cât posibil de altă natură decât informatică. În același context a fost chiar semnalată și o formă de șantaj ce consta în ,,plantarea" unor date

[6] DDoS - În condițiile unui refuz al serviciului în mod distribuit (Distributed Denial of Service), mai multe mașini de calcul atacă simultan computerul țintă. Numărul covârșitor de mesaje (date) primite determină blocarea sistemului atacat și rejectarea drepturilor de acces ale utilizatorilor legitimi. Un atacator poate iniția un atac DDoS exploatând vulnerabilitățile unui singur computer, pe care îl transformă în unitate principală, iar cu ajutorul acestuia caută și comunică cu alte computere vulnerabile pe care ulterior instalează anumite aplicații dedicate. După crearea grupului de computere controlate la distanță (BotNet) atacatorul poate, printr-o singura comandă, să lanseze un atac distribuit asupra mașinii de calcul țintă. http://e-crime.ro/ecrime/site/index.php/acasa/glosar/ Ultima accesare: 1 Oct 2016.

[7] Susan W. Brenner, Brian Carrier, și Jef Henninger, *The Trojan Horse Defense în Cybercrime Cases*, 21 Santa Clara High Tech. L.J. 1 (2004). Documentul este disponibil online la adresa: http://digitalcommons.law.scu.edu/chtlj/vol21/iss1/1, Ultima accesare 1 oct 2016,

[8] S Bowles, J Hernandez-Castro, The first 10 years of the Trojan Horsedefence, Computer Fraud & Security, Elsevier, 2015. Documentul este disponibil online la adresa: http://azlaha.com/papers/The%20first%2010%20years%20of%20the%20Trojan%20Defence.pdf, ultima accesare 30 nov 2016.

[9] Viermele informatics (*computer worm*) este o aplicație sau cod malițios capabil să se autoreproducă prin Internet sau alte sisteme conectate și care poate cauza daune în mai multe moduri. Deoarece au capacitatea de a se reproduce, viermii se pot înmulți foarte repede într-o rețea precum Internet. http://e-crime.ro/ecrime/site/index.php/acasa/glosar/, ultima accesare 25 noiembrie 2016.

informatice conținând pornografie infantilă pe un sistem informatic vulnerabil și constrângerea ulterioară a titularului respectivului sistem de a transfera o suma de bani[10].

Stabilirea în urma percheziției informatice a succesiunii de evenimente ce au avut loc în cadrul sistemului informatic se efectuează de regulă prin coroborarea înregistrărilor din jurnalele sistemului de operare (*computer logs*) privitoare la activitățile programelor informatice instalate, dacă aceste jurnale există, cu datele de creare, accesare, deschidere a documentelor identificate în sistem, crescând gradul de certitudine cu privire la stabilirea succesiunii de evenimente în situația în care sunt identificate astfel de jurnale de activitate a unui anumit program din sistem. Însă, situația programelor malițioase de tip virus este cu totul alta, acestea fiind de regulă create să opereze fără a lăsa urme în jurnalele de sistem, fiind documentate chiar cazuri de viruși dotați cu funcția de autodistrugere care va iniția ștergerea atât a virusului cât și a urmelor activității acestuia din jurnale, declanșată fie automat la momentul realizării scopului, fie în urma primirii unei comenzi de la distanță, pentru a împiedica depistarea și analiza[11], situație în care "presupunerea" doar în baza datelor prelevate de la documentele identificate, că utilizatorul sistemului informatic a comis fapta, poate conduce la erori judiciare grave.

Îndoiala cu privire la făptuitorul real, indusă de prezența programelor informatice dăunătoare (de tip virus informatic, Troian etc) în sistemul informatic al suspectului sau inculpatului devine cu atât mai rezonabilă în lipsa altor probe, cu cât statisticile Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO relevă în cadrul incidentelor de securitate procesate, implicarea unui număr impresionant de sisteme informatice aparținând populației, atât ca număr de IP-uri publice ori ca număr de sisteme infectate cu programe malițioase capabile să ofere acces de la distanță atacatorilor (*back door*), cât și ca număr de sisteme infectate facând parte din rețelele Botnet prin intermediul cărora se comit în mod automatizat atacuri informatice și alte fapte antisociale în mediul digital[12].

Realitățile sociale relevate de statisticile amintite justifică astfel pe deplin cerința ca instanțele să analizeze distinct și temeinic probatoriul referitor la identificarea suspectului ori inculpatului, chiar în lipsa unor prevederi specifice investigării mediului digital în legislația procedurală, făcând, acolo unde probele sunt insuficiente, aplicarea regulii *in dubio pro reo*.

IV. DIFICULTĂȚI ÎN INVESTIGARE ȘI JUDECARE

În cazul invocării apărării Cal Troian în fața instanței, ținând cont de realitățile expuse mai sus, instanța este pusă în fața a doar două posibilități: să condamne pe inculpat în baza posesiei materialelor incriminate identificate pe mediile de stocare, cu riscul ca acesta să nu fi fost făptuitorul real, ori să achite pe inculpat, cu riscul ca acesta în mod intenționat să-și fi infectat sistemul informatic cu programe malițioase, pentru a beneficia de aplicarea regulii "*in dubio pro reo*", în lipsa probării de către organele de urmărire penală a lipsei raportului cauzal dintre infectarea sistemului informatic și faptă.

Ținând cont de ușurința cu care se pot crea și insera probe digitale precum și de dificultățile tehnice și de costurile investigării acțiunilor concrete intreprinse de un virus într-un sistem informatic, sarcina aflării adevărului în cauzele de acest tip devine una deosebit de grea și de multe ori aproape imposibilă.

Apărarea tip Cal Troian este în mod evident o adaptare la epoca digitală a apărării clasice în care se susține că "altcineva a comis fapta", sarcina eliminării dubiului revenind organelor de urmărire penală cărora le revine sarcina probei în procesul penal și care se văd puse în situația de a proba contrariul afirmației, o sarcină deosebit de dificilă în condițiile în care virușii informatici actuali au capabilități sporite de deghizare a activităților desfășurate într-un sistem, iar acțiunile acestora rareori se înregistrează în jurnalele sistemului

[10] D. Haagman, B. Ghavalas, *Trojan defense: A forensic view,* în "Digital Investigation", nr. 2, 2005, p. 24.

[11] *Flamer: Urgent Suicide.* "Symantec Official Blog". (06 iunie 2012) Documentul este disponibil online la adresa http://www.symantec.com/connect/blogs/flamer-urgent-suicide. Ultima accesare: 1 Oct 2016.

[12] *Report on Cybersecurity Alerts Processed by CERT-RO în 2015*, în "IJISC – International Journal of Information Security and Cybercrime", Volume 5, Issue 1, Year 2016, ISSN: 2285-9225, DOI: 10.19107/IJISC.2016.01. Documentul este disponibil online la adresa: http://www.ijisc.com/year-2016-issue-1-article-9/, ultima accesare pe 1 oct 2016. Conform raportului, 20,78% (14 mil) dintre alertele de securitate colectate și procesate în anul 2015 se refereau la sisteme informatice infectate cu diverse programe dăunătoare, având drept caracteristică oferirea către atacatori a controlului de la distanță a sistemului informatic infectat; Conform raportului, 64% (3 milioane) din numărul total de incidente de securitate, identificate ca atare din procesarea alertelor, se refereau la sisteme informatice infectate și facând parte din rețelele de tip botnet existând șansa să fie utilizate în atacuri informatice și comitere automatizată de fapte penale din gama infracțiunilor informatice.

informatic (*computer logs*), nelăsând urmele digitale clasice pe care le lasă programele informatice utilizate în mod uzual în sistem, situație în care, percheziția informatică este rareori în măsură să releve comiterea faptei de către un terț.

Presiunea pusă pe acuzare este cu atât mai mare cu cât expertizarea acțiunilor desfășurate de anumite programe malițioase este una costisitoare, necesitând analiza acestora în condiții dinamice, în timpul funcționării, în laboratoare specializate, pentru a determina activitățile exacte ale virusului în sistemul informatic, neputându-se determina aceste activități doar din rezultatele raportului de percheziție informatică.

Raportul de percheziție informatică relevă de regulă doar situația statică a sistemului, așa cum se desprinde din datele stocate la un moment dat în timp, permițând o reconstituire parțială a anumitor evenimente, doar în măsura în care programele informatice ori sistemul de operare efectuau jurnalizări ale activităților desfășurate. Spre exemplu, datele de creare, ștergere, accesare ale unui fișier indică acțiunile cu privire la acel document, însă nu pot indica și dacă activitatea respectivă a fost desfășurată de utilizator de la tastatură, de către un utilizator clandestin de la distanță, ori în mod automat de către un program informatic malițios de tip virus.

În schimb, constatarea printr-un obiectiv al expertizei tehnice în specialitate informatică a infectării sistemului informatic cu un virus, chiar în lipsa expertizării în laboratoare specializate, poate fi completată sub aspectul documentării, cu lista de funcții / activități cunoscute a fi desfășurate de către virusul identificat. Dacă printre acestea se regăsește capacitatea de a oferi controlul de la distanță atacatorului sau autorului virusului, consecința juridică a constatării o reprezintă îndoiala privind numărul real de utilizatori ai sistemului informatic, alții decât utilizatorul legitim care avea acces fizic la sistemul informatic, impunând verificări suplimentare, ori, în lipsa acestora, aplicarea regulii in dubio pro reo.

În contextul prezentei teme este important a se defini și înțelege de către actorii implicați în procesul penal noțiunea de infectare a sistemului informatic cu un program malițios de tip virus sau cal troian și a stărilor în care acesta poate fi identificat în sistem, pe bună dreptate afirmându-se în doctrină faptul că nu este suficientă simpla depistare în sistem a fișierului conținând programul malițios, fiind necesară verificarea rulării acestuia la un moment dat în timp și eventuala corelare cu datele de creare și accesare de la documentele și fișierele incriminate precum și cu alte urme ale activității programului malițios[13].

Astfel, considerăm că un sistem informatic este infectat cu un program malițios în măsura în care programul respectiv se regăsește în sistemul informatic în zone de unde poate fi executat (spre exemplu nu este localizat în zona de carantină a programului antivirus și nu a fost dezactivat de acesta) iar funcția de pornire automată a acestuia se regăsesc între instrucțiunile care se execută în mod automat de către sistem, spre exemplu la pornirea sistemului, la executarea unui alt program sau periodic ori la o anumită dată, de regulă aceste instrucțiuni fiind localizate în regiștrii sistemului de operare, putând fi identificate în cadrul percheziției informatice.

Vom denumi în cele ce urmează această stare de fapt a programului malițios drept ”stare activă”, acesta fiind pornit sau rulat în mod activ de către sistemul de operare, putându-se determina, prin analize avansate inclusiv în timpul funcționării acestuia, dacă deschide căi de acces din exterior (*back door*) sau dacă desfășoară în sistemul informatic anumite activități din sfera de interes a cauzei, precum accesarea adreselor din internet identificate ca punând la dispoziție materiale pornografice cu minori, accesarea locațiilor de pe disc unde sunt stocate documentele relevante cauzei, etc. Cu toate acestea, așa cum arătam mai sus, o atare analiză implică proceduri suplimentare percheziției informatice, costisitoare și desfășurate în laboratoare specializate. În lipsa acestor analize suplimentare însă, rămâne pentru instanță întrebarea dacă programul avea capacitatea de a deschide căi de acces din exterior ori dacă conținea instrucțiuni de comitere a faptei.

În egală măsură însă, un program malițios poate fi identificat ca inactiv, fie în zona de carantină a programului antivirus din sistem (neexistând în regiștrii sistemului instrucțiuni de rulare a programului), situație care însă nu elimină posibilitatea ca programul să fi fost activ și să fi funcționat ca instrument la momentul comiterii faptei, fie pur și simplu în orice locație din sistem dar fără a regăsi instrucțiuni de rulare în regiștri.

Opinăm că situația identificării ca inactiv a programului malițios, cu cele două variante ale sale nu poate sta singură la baza concluziei că fapta a fost comisă de către deținătorul sau utilizatorul legitim al sistemului

[13] G. Zlati, Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (II), în “Caiete de drept penal”, nr. 4/2014.

informatic, în lipsa identificării unor date care să probeze cu certitudine apariția în sistem a programului după data comiterii faptei ori a documentării imposibilității ca programul malițios să nu fi avut capacitățile necesare comiterii faptei prin intermediul său, în contextul în care, dubiul cu privire la funcționarea programului malițios nu poate prima în fața dubiului cu privire la făptuitorul real, probarea dincolo de orice îndoială rezonabilă a comiterii faptei căzând în sarcina acuzării.

Așa cum realitatea socială o arată, în condițiile în care unele dintre programele malițioase sunt create cu capabilități de a nu lăsa urme ale activităților lor în sistem, iar în anumite situații fiind dovedită chiar capabilitatea de a șterge urmele, mergând până la funcția de autodistrugere pentru a împiedica depistarea, în cazul invocării apărării Cal Troian sistemul judiciar este pus în situația dilemei aparent fără ieșire de a alege între a condamna pe inculpat în baza posesiei materialelor incriminate identificate în sistemul informatic, cu riscul ca acesta să nu fi fost făptuitorul real, ori a achita pe inculpat, cu riscul ca acesta în mod intenționat să-și fi infectat sistemul informatic cu programe dăunătoare, pentru a beneficia de aplicarea regulii "in dubio pro reo", în situația în care învinuitul sau inculpatul invocă acest tip de apărare în instanță.

V. PREZUMȚII SPECIFICE MEDIULUI DE COMITERE A FAPTEI

La această dificultate se adaugă noutatea și specificitatea mediului digital, în special cu privire la necesitatea de a elimina anumite prezumții aplicabile în mod normal în spațiul fizic la investigarea infracțiunilor și încetățenite în rândul practicienilor și instanțelor. Ca exemplu, un set de prezumții des utilizat în stabilirea perimetrului investigației criminalistice în spațiul fizic este dat de asa-numita situație a "crimei comise în camera închisă" prin opoziție cu situația "crimei comise în piața publică".

În cazul unei crime în spațiu închis (o cameră) se poate prezuma cu un grad destul de ridicat de probabilitate că în spațiul respectiv se pot identifica mai multe probe în stare intactă, iar cercul de suspecți poate fi restrâns la persoanele care se aflau înăuntru sau care au intrat ori ieșit din clădire. La polul opus, o crimă comisă în piața publică va avea, cel mai adesea, probele contaminate de trecători ori de intemperii, suspect putând fi oricine.

În cazul infracțiunilor informatice însă, chiar dacă sistemul informatic este închis în cameră și are un proprietar unic, atât timp cât este conectat la internet și este și infectat cu programe malițioase, prezumtivul "domiciliu informatic privat" al suspectului, devine aproape automat echivalentul unei "piețe publice", fiind mai indicată aplicarea prezumțiilor privitoare la comiterea faptei într-un spațiu public, urmând a se restrânge perimetrul investigat pe măsura administrării de probe suplimentare percheziției informatice.

Astfel, în cazul în care urmărirea penală a neglijat scanarea de viruși a sistemului, ori a omis să adreseze satisfăcător ipotezele alternative de comitere a faptei, apărarea va avea totdeauna un punct de start în a induce dubiul cu privire la făptuitor solicitând prin procedura expertizei tehnice scanarea de viruși a mediilor de stocare și documentarea de către expert a capabilității de a oferi control de la distanță a virușilor identificați, situație în care, dubiul cu privire la făptuitor nu poate fi neglijat în lumina statisticilor care arată frecvența alarmantă a astfel de situații în societate.

Instanța va ține cont de noua situație, examinând și coroborând celelalte probe administrate ori dispunând administrarea de noi probe acolo unde este posibil, fie pe latura tehnică, fie cu privire la celelalte aspecte precum persoana făptuitorului, acțiuni și activități conexe comiterii faptei și care nu puteau fi comise de către un program informatic (ex. corespondență în legătură cu fapta, operațiuni financiare legate de faptă, inscripționarea pe mijloace de stocare a datelor informatice externe de tip CD/DVD a materialelor ilegale, etc).

În lipsa probelor sigure, certe care să elimine satisfăcător ipoteza controlului de la distanță ori comiterea automată a faptei de către un program malițios, nesiguranța indusă cu privire la autorul real impune aplicarea regulii potrivit căreia „orice îndoială este în favoarea inculpatului".

Regula in dubio pro reo constituie un complement al prezumţiei de nevinovăţie, un principiu instituţional care reflectă modul în care marele principiu al aflării adevărului se regăsește în materia probaţiunii. Ea se explică prin aceea că, în măsura în care dovezile administrate pentru susţinerea vinovăţiei celui acuzat conţin o informaţie îndoielnică tocmai cu privire la vinovăţia făptuitorului, în legătură cu fapta imputată, autorităţile judecătorești penale nu-și pot forma o convingere care să se constituie într-o certitudine și, de aceea, ele trebuie să concluzioneze în sensul nevinovăţiei acuzatului și să-l achite. Înainte de a fi o problemă

de drept, regula in dubio pro reo este o problemă de fapt. Înfăptuirea justiţiei penale cere ca judecătorii să nu se întemeieze, în hotărârile pe care le pronunţă, pe probabilitate, ci pe certitudinea dobândită pe bază de probe decisive, complete, sigure, în măsură să reflecte realitatea obiectivă (fapta supusă judecăţii). Numai așa se formează convingerea, izvorâtă din dovezile administrate în cauză, că realitatea obiectivă (fapta supusă judecăţii) este, fără echivoc, cea pe care o înfăţișează realitatea reconstituită ideologic cu ajutorul probelor.[14]

Astfel, în cazul respingerii ipotezei comiterii automatizate ori de la distanță de către un alt făptuitor a infracțiunii, instanța în motivarea sa este ținută să detalieze modalitatea și elementele de fapt care au dus la eliminarea îndoielii, atât în baza cerințelor legale dar mai cu seamă în lumina realităților sociale de necontestat privind frecvența acestor situații.

Dacă la infracțiunile clasice, comise în spațiul fizic, șansele de a identifica terțul care a comis fapta sunt ceva mai mari, în mediul digital însă, ținând cont atât de realitățile tehnice și de statistici, cât și de costurile investigațiilor suplimentare percheziției informatice, șansele identificării făptuitorului real și de cele mai multe ori chiar comiterea faptei de către o altă persoana decât suspectul sau inculpatul, reprezintă provocarea majoră pentru practicieni și instanțe în stabilirea adevărului în cauzele de criminalitate informatică.

VI. CONCLUZII

Adaptarea sistemului judiciar și a practicii la exigențele societății digitale implică un drum anevoios dar necesar de desprindere de ideile preconcepute referitoare la modalitățile de săvârșire a faptelor penale din spațiul fizic și verificarea minuțioasă a detaliilor fiecărei cauze sub toate aspectele, mai cu seamă a acelor aspecte care în cazul infracțiunilor clasice sunt de regulă, în baza cunoașterii empirice sau a legităților științelor ce le guvernează, indiscutabile ca și concluzii.

Justiția nu se poate făptui desprins de realitățile sociale, în speță, dreptul la un proces echitabil și prezumția de nevinovăție neputând fi apărate și aplicate în cazul ignorării realităților distincte ale societății digitale precum frecvența cu care se întâlnește în societatea actuală situația controlului de la distanță, fără știrea utilizatorului, a sistemelor informatice.

References/Bibliografie

Centrul National de Raspuns la Incidente de Securitate CERT-RO, *Report on Cybersecurity Alerts Processed by CERT-RO în 2015*, în "IJISC – International Journal of Information Security and Cybercrime", Volume 5, Issue 1, 2016

Brenner, S. W., Carrier, B., Henninger, J., *The Trojan Horse Defense in Cybercrime Cases*, 21 în „Santa Clara High Technology Law Journal", nr. 1, 2004

Bowles, S., Hernandez-Castro, J., *The first 10 years of the Trojan Horsedefence*, în "Computer Fraud & Security", Elsevier, 2015.

Driga, C., Purici, S., *Fighting the classical crime-scene assumptions. Critical aspects în establishing the crime-scene perimeter în computer-based evidence cases*, în "CKS-Challenges of the Knowledge Society", "Nicolae Titulescu" University Publishing House. 2016

Haagman, D., Ghavalas, B., *Trojan defense: A forensic view*, Digital Investigation, nr. 2, 2005

Zlati, G., *Percheziția sistemelor informatice și a mijloacelor de stocare a datelor informatice (II)*, în "Caiete de drept penal", nr. 4/2014

[14] ÎCCJ, dec. pen. nr. 343/A din 28 octombrie 2014, disponibilă pe http://www.iccj.ro/cautare.php?id=114819. Ultima consultare 2 octombrie 2016.