**ANALELE ȘTIINȚIFICE ALE UNIVERSITAȚII „AL. I. CUZA" IAȘI**
**TOMUL LXIII, ȘTIINȚE JURIDICE, 2017, NR. II**

# UNELE CONSIDERAȚII PRIVIND INFRACȚIUNEA DE PERTURBARE A FUNCȚIONĂRII SISTEMELOR INFORMATICE

# SOME CONSIDERATIONS REGARDING THE OFFENCE OF DISRUPTING THE FUNCTIONING OF COMPUTER SYSTEMS

**ADRIAN CRISTIAN MOISE**[1]

**Rezumat:** Pornind de la prevederile art. 5 din Convenția Consiliului Europei privind criminalitatea informatică și de la prevederile art. 4 din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice, ambele referindu-se la afectarea integrității sistemului informatic, în prezentul articol se realizează o analiză a infracțiunii de perturbare a funcționării sistemelor informatice, prevăzută de art. 363 din Codul penal, urmărindu-se dacă legiuitorul român a transpus prevederile celor două instrumente juridice de la nivel internațional și european. Reglementarea legală urmărește să protejeze datele informatice stocate în cadrul sistemelor informatice, accentul fiind pus pe efectul pe care îl au pentru sistemele informatice afectate acțiunile asupra datelor informatice. Totodată, în articol se analizează atât cel mai cunoscut atac împotriva unui sistem informatic care afectează integritatea sistemului informatic, acesta fiind atacul DOS – Denial of Service –, cât și alte atacuri împotriva unui sistem informatic care afectează integritatea sistemului informatic, cum sunt atacurile bazate pe programele malițioase care au ca scop infectarea sistemului informatic.
**Cuvinte cheie:** perturbare, sistem informatic, date informatice, atac, programe malițioase.

**Abstract:** Starting from the provisions of Article 5 of the Council of Europe Convention on Cybercrime and the provisions of Article 4 of the Directive 2013/40/EU on attacks against information systems, both relating to illegal system interference, this Article performs an analysis of the offence of disrupting the functioning of the computer systems sanctioned by Article 363 of the Romanian Criminal Code, in order to ensure that the Romanian legislator transposed the provisions of the two legal instruments from international and European level. The

[1] Lector univ. dr, Universitatea Spiru Haret din București, Facultatea de Științe Juridice, Economice și Administrative, Craiova, România; avocat, Baroul Dolj; E-mail: adriancristian.moise@gmail.com.

legal regulation aims to protect the computer data stored in computer systems, focusing on the effect they have on computer systems affected by the actions on computer data. At the same time, the article analyzes both the most common attack against a computer system that affects the integrity of the computer system, such as the DOS (Denial of Service) attack, as well as other attacks against a computer system that affects the integrity of the computer system, such as the attacks based on malicious programmes aimed at infecting the computer system.
**Keywords:** disrupting, computer system, computer data, attack, malicious programmes.

## 1. Introducere

Infracțiunea de perturbare a funcționării sistemelor infoarmatice este prevăzută în art. 363 din Capitolul VI *Infracțiuni contra siguranței și integrității sistemelor și datelor informatice* din Codul penal. Textul de lege prevede că: *„Fapta de a perturba grav, fără drept, funcționarea unui sistem informatic, prin introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la date informatice, se pedepsește cu închisoarea de la 2 la 7 ani”*.

Reglementarea legală urmărește să protejeze datele informatice stocate în cadrul sistemelor informatice împotriva atacurilor de piraterie informatică sau altor activități malițioase care au ca scop aducerea în stare de nefuncționare a sistemelor informatice. Spre deosebire de infracțiunea reglementată în art. 362 din Codul penal ce se referă la alterarea a integrității datelor informatice, în cazul infracțiunii de perturbare a funcționării sistemelor informatice, accentul este pus pe efectul pe care îl au pentru sistemele informatice afectate, acțiunile asupra datelor informatice (introducerea, transmiterea, modificarea, ștergerea, deteriorarea sau restricționarea accesului la datele informatice)[2].

## 2. Incriminarea faptei de afectare a integrității sistemului informatic în cadrul Convenției Consiliului Europei privind criminalitatea informatică

Pentru a proteja accesul operatorilor și utilizatorilor la tehnologia informațiilor și comunicațiilor, Convenția Consiliului Europei privind

[2] Romanian Information Technology Initiative și Guvernul României, *Ghid introductiv pentru aplicarea dispozițiilor legale referitoare la criminalitatea informatică*, București, 2004, p. 61, [Online] la: http://www.riti-internews.ro/ro/ghid.htm, accesat la 22.10.2017.

criminalitatea informatică[3] a prevăzut în art. 5 incriminarea afectării funcționării normale a unui sistem informatic. Art. 5 din Convenție se referă la infracțiunea de afectare a integrității sistemului informatic care implică afectarea gravă, intenționată și fără drept a funcționării unui sistem informatic prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea sau suprimarea datelor informatice[4].

Pentru ca dispozițiile art. 5 să fie aplicate este necesar ca funcționarea sistemului informatic să fie afectată[5]. Termenul de afectare are semnificația oricărui act care interferează cu funcționarea corespunzătoare a sistemului informatic[6]. În plus, textul art. 5 din Convenția Consiliului Europei privind criminalitatea informatică prevede faptul că afectarea sistemului informatic să fie gravă. Este responsabilitatea statelor membre de a stabili criteriile care trebuie îndeplinite pentru ca afectarea sistemului informatic să fie considerată gravă[7].

Am remarcat faptul că acțiunile de introducere și transmitere a datelor informatice nu sunt definite de Convenția Consiliului Europei privind criminalitatea informatică, nici de Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică. Putem considera faptul că acțiunea de introducere a datelor informatice într-un sistem informatic poate fi definită ca orice act în legătură cu interfețele de intrare fizică pentru a transfera informațiile la un sistem informatic, în timp ce

---

[3] Convenția Consiliului Europei privind criminalitatea informatică a fost adoptată la Budapesta la data de 23.11.2001, disponibilă [Online] la: http://www.conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, accesat la 22.10.2017.

[4] În Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică pct. 61 sunt definiți următorii termeni: termenii de „periclitare” și „deteriorare” se referă la alterarea integrității datelor și programelor informatice; termenul de „ștergere” a datelor informatice semnifică acțiunea de îndepărtare a datelor informatice din dispozitivele de stocare; termenul de „suprimare” a datelor informatice reprezintă acțiunea care afectează disponibilitatea datelor informatice; termenul de „modificare” a datelor informatice se referă la acțiunea de alterare a datelor informatice existente în special prin instalarea unor programe distrugătoare.

[5] A. Savin, *EU Internet Law*. Edward Elgar Publishing Limited, Cheltenham, Glos, 2013, p. 238.

[6] Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică pct. 66, disponibil [Online] la: http://conventions.coe.int/treaty/en/reports/html/185.htm, accesat la 22.10.2017.

[7] Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică pct. 67, disponibil [Online] la: http://conventions.coe.int/treaty/en/reports/html/185.htm, accesat la 22.10.2017. M. Gercke, International Telecommunication Union. *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, Geneva, 2012, p. 33, [Online] la: www.itu.int/ITU D/cyb/cybersecurity/legislation.html, accesat la 22.10.2017.

acțiunea de transmitere a datelor informatice se referă la acte care necesită intrarea de la distanță a datelor în sistemul informatic[8].

În literatura de specialitate s-a abordat problema dacă spam-ul sau mesajul nesolicitat ar putea fi incriminat de prevederile art. 5 din Convenție, întrucât spam-ul poate suprasolicita funcționarea sistemului informatic. La ora actuală, Convenția Consiliului Europei privind criminalitatea informatică nu incriminează în mod explicit spam-ul. Legiuitorii Convenției au considerat că acest comportament nu poate conduce la grave afectări a sistemului informatic, iar acest comportament trebuie să fie incriminat numai în situația în care comunicația este afectată în mod intenționat și grav[9].

## 3. Incriminarea faptei de afectare ilegală a integrității sistemului informatic în cadrul Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice

Infracțiunea de afectare ilegală a integrității sistemului informatic este prevăzută în art. 4 din Directiva 2013/40/UE[10] privind atacurile împotriva sistemelor informatice și constă în perturbarea gravă sau întreruperea funcționării unui sistem informatic prin introducerea, transmiterea, periclitarea, ștergerea, deteriorarea, modificarea, suprimarea datelor informatice sau prin a le face inaccesibile. Infracțiunea de afectare ilegală a integrității sistemului informatic se săvârșește cu intenție și fără drept și trebuie să nu reprezinte un caz minor.

## 4. Analiza infracțiunii de perturbare a funcționării sistemelor informatice prevăzută de art. 363 din Codul penal

### 4.1. Condiții preexistente

#### 4.1.1. Obiectul infracțiunii

Obiectul juridic special îl constituie relațiile sociale care protejează integritatea datelor informatice conținute pe suporturile specifice sistemelor informatice.

---

[8] A.C. Moise, *Dimensiunea criminologică a criminalității din cyberspațiu*, Editura C.H. Beck, București, 2015, p. 102.

[9] Raportul Explicativ al Convenției Consiliului Europei privind criminalitatea informatică pct. 69, disponibil [Online] la: http://conventions.coe.int/treaty/en/reports/html/185.htm, accesat la 22.10.2017.

[10] Directiva 2013/40/UE a Parlamentului European și a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice și de înlocuire a Decizei-Cadru 2005/222/JAI a Consiliului, JO UE, 14.08.2013, L218/8.

Obiectul material este reprezentat de sistemul informatic a cărui activitate este grav perturbată de infractor. Astfel, constituie obiect material următoarele[11]: componentele sistemului informatic, adică unele dintre părțile care formează un sistem informatic (exemple de sisteme informatice: computer, telefon mobil, dispozitiv ATM – Automatted Teller Machine –, agendă computerizată, aparat de fotografiat digital, imprimantă, tabletă electronică) sau o rețea; computerele în sine, care reprezintă dispozitive care constau în una sau mai multe componente asociate, incluzând unități de procesare și periferice și care sunt controlate de programe stocate intern; rețeaua care reprezintă un grup interconectat de computere, echipamente de comutare și ramuri de interconectare; rețeaua Internet, care reprezintă o rețea de rețele.

Perturbarea gravă poate avea ca obiect fie întregul sistem informatic, fie părți ale acestuia sau servicii sau programe deservite sau rulate de acesta.

### 4.1.2. Subiecții infracțiunii

Subiectul activ al infracțiunii de perturbare a funcționării sistemelor informatice poate fi orice persoană care îndeplinește condițiile generale prevăzute de lege pentru a răspunde penal.

Participația penală este posibilă în toate formele sale: coautorat, instigare și complicitate.

Subiectul pasiv al infracțiunii de perturbare a funcționării sistemelor informatice este persoana fizică sau juridică care deține sau utilizează legitim sistemul informatic a cărui funcționare este perturbată.

## 4.2. Conținutul constitutiv

### 4.2.1. Latura obiectivă

Elementul material al infracțiunii de perturbare a funcționării sistemelor informatice se realizează prin acțiunea de a perturba grav funcționarea unui sistem informatic. În legătură cu această activitate, legiuitorul român prevede următoarele condiții esențiale pentru existența infracțiunii în această formă[12]: perturbarea să fie gravă; perturbarea să fie realizată fără drept; ingerința cu consecințe grave asupra funcționării sistemului informatic să aibă loc prin introducerea, transmiterea,

[11] S. Corlățeanu, C. Căşuneanu, *Delicte contra datelor şi sistemelor informatice*, în Dreptul nr.11/2004, p. 208.

[12] I. Vasiu, L. Vasiu, *Informatică juridică şi drept informatic*, Editura Albastră, Cluj-Napoca, 2007, p. 139.

modificarea, ștergerea sau deteriorarea datelor informatice sau prin restricționarea accesului la datele informatice.

Autorii Convenției Consiliului Europei privind criminalitatea informatică au lăsat la latitudinea fiecărui stat-parte să își însușească și să interpreteze noțiunea de perturbare gravă[13]. Totuși, legiuitorul român nu oferă niciun criteriu pentru a putea aprecia dacă perturbarea a fost sau nu gravă. Astfel, în aceste circumstanțe, considerăm că sarcina aprecierii faptului dacă perturbarea este gravă sau nu va fi lăsată pe umerii instanțelor de judecată.

Perturbarea gravă trebuie să fie realizată fără drept, astfel încât ea nu va exista în situația în care ingerința într-un sistem informatic este permisă sau autorizată (cum ar fi, de exemplu, testarea securității sistemului informatic).

Textul legal precizează următoarele tipuri de ingerințe care pot da naștere la perturbări grave: introducerea de date informatice, care are în vedere atât introducerea de date exacte într-o manieră corectă, cât și introducerea de date incorecte; transmiterea de date informatice, care presupune efectuarea unor comunicări de date informatice, conducând la supraîncărcarea sistemelor informatice; modificarea datelor informatice, care se referă la alterarea datelor informatice, astfel încât acestea pot să fie utilizate, dar procesarea acestora va produce rezultate incorecte; ștergerea datelor informatice, care se referă la eliminarea datelor informatice de pe suportul fizic pe care sunt stocate; deteriorarea datelor informatice, care se referă la alterarea datelor, în așa fel încât acestea nu mai pot fi utilizabile; restricționarea accesului la datele informatice se referă la restricționarea totală sau parțială sau la întârzierea semnificativă a accesului la datele informatice, atunci când utilizatorul are nevoie de acestea.

Urmarea imediată constă în producerea unui rezultat, o consecință a ingerinței fără drept, rezultând o perturbare gravă a funcționării unui sistem informatic.

Între activitatea cybercriminalului și urmarea imediată produsă trebuie să existe o legătură de cauzalitate, aceasta rezultând din materialitatea faptei. Expertiza informatică poate să determine existența legăturii de cauzalitate, aceasta putând răspunde și la întrebarea care vizează

[13] I. Vasiu, L. Vasiu, *op.cit.*, p. 159; S. Schjolberg, S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime*. ed. a II-a, AIT, Oslo, 2011, pp. 41-42.

gravitatea perturbării și dacă acest rezultat reprezintă urmarea acțiunii făptuitorului.

**4.2.2. Latura subiectivă**

Pentru existența infracțiunii de perturbare a funcționării sistemelor informatice este necesar ca fapta să fie săvârșită cu vinovăție. În această situație, forma de vinovăție necesară este intenția, atât directă, cât și indirectă.

**4.3. Formele infracțiunii**

Actele pregătitoare sunt posibile, dar nu sunt incriminate și, ca atare, nu se pedepsesc.

Tentativa este posibilă și se pedepsește conform art. 366 C. pen.

Consumarea infracțiunii de perturbare a funcționării sistemelor informatice se realizează în momentul producerii urmării imediate, adică a perturbării grave a funcționării sistemului informatic. În situația în care această urmare nu se realizează, se poate vorbi doar de acte pregătitoare efectuate de infractor sau de săvârșirea altor infracțiuni (de exemplu, alterarea integrității datelor informatice sau accesul ilegal la un sistem informatic).

Epuizarea infracțiunii are loc în momentul săvârșirii ultimului act incriminat de lege comis de făptuitor.

Infracțiunea de perturbare a funcționării sistemelor informatice poate fi săvârșită în formă continuă sau continuată.

**4.4. Modalități**

Infracțiunea de perturbare a funcționării sistemelor informatice prezintă șase modalități normative în varianta tip: introducerea, transmiterea, modificarea, ștergerea sau deteriorarea datelor informatice ori restricționarea accesului la datele informatice. Acestor modalități normative pot să le corespundă mai multe modalități de fapt.

**4.5. Sancțiuni**

Pedeapsa prevăzută pentru infracțiunea de perturbare a funcționării sistemelor informatice este închisoarea de la 2 la 7 ani.

Acțiunea penală se pune în mișcare din oficiu.

**5. Atacuri frecvent întâlnite în criminalitatea informatică care afectează integritatea sistemului informatic**

**5.1. Atacurile Denial of Service**

Cel mai cunoscut atac împotriva unui sistem informatic care afectează integritatea sistemului informatic este atacul Denial of Service – DOS – (Refuzul serviciului).

În această formă de atac, atacatorul încearcă să interzică utilizatorilor autorizați accesul la informații specifice, la sistemele informatice și la rețeaua însăși. Scopul unui astfel de atac poate fi prevenirea accesului la sistemul informatic țintă sau atacul poate fi utilizat împreună cu alte acțiuni în scopul de a obține accesul neautorizat la un sistem informatic sau la o rețea.

Atacul DOS reprezintă, de fapt, o încercare a infractorului de a face resursele informatice nedisponibile pentru utilizatorii legitimi. De exemplu, atacul SYN flooding poate fi utilizat pentru a împiedica temporar funcționarea sistemului informatic. Atacul SYN flooding reprezintă un exemplu de atac DOS care profită de modul în care rețelele de comunicații care utilizează protocolul de comunicații TCP/IP au fost proiectate să funcționeze, acest exemplu putând fi utilizat pentru a ilustra principiile de bază ale unui atac DOS. Datorită faptului că protocolul de comunicații TCP/IP reprezintă o conexiune orientată, o sesiune sau o legătură directă de comunicații trebuie să fie creată înainte de trimiterea datelor informatice. Sistemul informatic client inițiază comunicarea cu server-ul (computerul ale cărui resurse clientul dorește să le acceseze). Așadar, se vor parcurge următorii pași:[14]

1. Computerul client trimite o cerere de sincronizare (SYN).
2. Server-ul trimite un mesaj de confirmare (ACK) și un semnal de sincronizare SYN, care aprobă cererea computerului client care a fost făcută în Pasul 1. Computerul client și server-ul trebuie să se sincronizeze reciproc cu numere de secvențe.
3. Computerul client trimite un mesaj de confirmare (ACK) înapoi la server, confirmând cererea de sincronizare a server-ului.

Atacul SYN flooding utilizează acest proces prezentat mai înainte, pentru a inunda sistemul țintă, victimă a atacului, cu multiple pachete SYN care au o adresă IP care nu există. Acest fapt determină server-ul să răspundă prin mesaje SYN/ACK.

[14] D.L. Shinder, E. Tittel, *Scene of the cybercrime. Computer Forensics Handbook*, Syngress Publishing Inc., Rockland, Massachusetts, 2002, pp. 318-319.

Deoarece adresele IP sursă pentru pachetele SYN, trimise de atacator nu sunt bune, semnalele de confirmare (ACK) pe care server-ul le așteaptă nu vor veni niciodată. Prin urmare, serviciul este refuzat către clienții legitimi care așteaptă să stabilească comunicații cu server-ul.

Atacurile DOS sunt dirijate pentru un singur sistem informatic de atac. Un atac DOS care folosește multiple sisteme de atac, este cunoscut sub numele de Refuzul serviciului distribuit (Distributed Denial of Service – DDOS).

Scopul atacului DDOS este același: refuzul de a utiliza un serviciu sau sistem. Într-un atac DDOS, metoda folosită pentru refuzul serviciului este distrugerea țintei cu ajutorul comunicațiilor de la mai multe sisteme informatice diferite. O rețea cu agenți de atac (uneori numiți zombie) este creată de atacator, iar la primirea comenzii de atac de la atacatori, agenții de atac încep să trimită comunicații specifice împotriva țintei. Agenții de atac sunt sisteme informatice care au fost compromise și la care sofware-ul de atac DDOS a fost instalat. Crearea unei rețele de atac poate fi un proces în mai mulți pași, în care atacatorul mai întâi compromite câteva sisteme informatice, care sunt apoi utilizate ca intermediare sau conducătoare și care vor compromite alte sisteme informatice.

### 5.2. Atacurile bazate pe programele malițioase care au ca scop infectarea sistemului informatic

Există trei tipuri de programe malițioase care au ca obiectiv infectarea unui sistem informatic: virușii, viermii și caii troieni[15].

Un virus este un program care infectează fișiere executabile sau fișiere obiect[16]. Orice program care se multiplică fără acordul utilizatorului este un virus[17]. Mai întâi, virusul se va multiplica, răspândindu-se către alte sisteme informatice[18], după care acesta își va activa funcția sa malițioasă.

Un vierme reprezintă un program destinat pentru a obține avantajul față de o vulnerabilitate într-o aplicație sau într-un sistem de operare în

---

[15] L. Klander, *Anti Hacker –Ghidul securităţii reţelelor de calculatoare*, Editura All Educational, Bucureşti, 1999, p. 385.

[16] M. Dobrinoiu, *Infracţiunea de alterare a integrităţii datelor informatice*, în Revista Română de Dreptul Proprietăţii Intelectuale nr.3/2006, p. 62.

[17] C. Féral-Schuhl, *Cyberdroit. Le droit à l' épreuve de l' Internet*, ed. a VI-a, Dalloz, Paris, 2010, pp. 918-923.

[18] J. Traxler, J. Forristal, *Hach Proofing Your Web Applications*, Syngress Publishing Inc., Rockland, Massachusetts, 2001, p. 16; C. Easttom, J. Taylor, *Computer Crime, Investigation, and the Law*, Course Technology, Cengage Learning, Boston, Massachusetts, 2010, p. 57.

scopul de a penetra un sistem informatic. Odată ce viermele a exploatat vulnerabilitatea unui sistem informatic, acesta imediat cercetează alte sisteme informatice care au aceeași vulnerabilitate.

Spre deosebire de virus, viermele reprezintă un program de sine stătător care există independent de alte programe, iar pentru a rula nu are nevoie de alte programe[19]. Acțiunile pe care viermii le realizează includ ștergerea fișierelor unui sistem informatic, sau controlul de la distanță al sistemului informatic de către atacator.

Viermele se multiplică pe un sistem informatic și încearcă să infecteze și alte sisteme informatice, care ar putea fi atașate la aceeași rețea.

Calul Troian reprezintă un program, care în mod aparent efectuează o acțiune utilă, dar în fapt el efectuează acțiuni de distrugere care nu sunt cunoscute de utilizator[20].

Calul Troian este un program care apare pentru a executa funcții valide, dar conține ascunse în cadrul său instrucțiuni ce pot provoca daune sistemelor informatice pe care se instalează. Acest program reprezintă o metodă de inserare a unor instrucțiuni într-un program, astfel încât programul va executa o funcție neautorizată, în timp ce aparent execută una obișnuită.

Calul Troian efectuează următoarele acțiuni:[21] ștergerea sau modificarea fișierelor; transmiterea fișierelor prin rețea la cyber-atacator; instalarea în sistemul informatic a altor programe malițioase și viruși.

**Concluzii**

Dispozițiile din cuprinsul art. 363 C. pen. sunt inspirate din prevederile art. 5 din Convenția Consiliului Europei privind criminalitatea informatică și din prevederile art. 4 din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice. Astfel, spre deosebire de textele Convenției Consiliului Europei privind criminalitatea informatică și Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice, observăm faptul că legea română nu reține ca modalități alternative *periclitarea* sau *suprimarea* datelor informatice și introduce o modalitate nouă, cea de *restricționare* a accesului la aceste date informatice. Considerăm că acțiunea

[19] T. Amza, C.P. Amza, *Criminalitatea informatică*, Editura Lumina Lex, Bucureşti, 2003, p. 115.

[20] D.L. Shinder, E. Tittel, *Scene of the cybercrime. Computer Forensics Handbook*, Syngress Publishing Inc., Rockland, Massachusetts, 2002, p. 336.

[21] Ibidem.

de *suprimare* a datelor informatice, care reprezintă echivalentul unei distrugeri a datelor informatice, ar fi trebuit să fi fost reținută ca modalitate alternativă de săvârșire a infracțiunii, alături de *periclitare*.

Prin urmare, legiuitorul român a transpus în cadrul art. 363 C. pen. atât prevederile art. 4 (afectarea ilegală a integrității sistemului) din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice, cât și prevederile art. 5 (afectarea integrității sistemului) din Convenția Consiliului Europei privind criminalitatea informatică.

Cu toate că cele mai importante instrumente juridice de combatere a criminalității informatice la nivel european nu incriminează în prezent unele comportamente care perturbă grav funcționarea sistemelor informatice, cum este de exemplu, spam-ul (mesajul nesolicitat), suntem de părere că legiuitorii celor două acte normative trebuie să le actualizeze, prin incriminarea și acestor comportamente ilegale care afectează grav sistemele informatice. Datorită efectelor pe care mesajele nesolicitate le pot produce într-un sistem informatic sau rețea, considerăm că spam-ul ar putea fi incriminat de prevederile art. 5 din Convenția Consiliului Europei privind criminalitatea informatică și de prevederile art. 4 din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice, ambele prevederi referindu-se la afectarea integrității sistemelor informatice.