Revista Universul Juridic ● nr. 10, octombrie 2017, pp. 58-65

CÂTEVA ASPECTE REFERITOARE LA INFRACȚIUNEA DE ALTERARE A INTEGRITĂȚII DATELOR INFORMATICE

Lector univ. dr. Adrian Cristian MOISE
Universitatea Spiru Haret din Bucureşti

Abstract

Starting from the provisions of Article 4 of the Council of Europe Convention on Cybercrime and the provisions of Article 5 of the Directive 2013/40/EU on attacks against information systems, both relating to illegal data interference, in this Article is performed an analysis of the offence of altering the functioning of the computer systems provided by the Article 362 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 Romanian legal regulation aims to protect the computer data stored in the information systems in order to prevent the alteration, deletion or deterioration of the computer data or restricting access to such data.

The article also presents and analyzes an attack frequently encountered in cybercrime, which aims to alter the integrity of computer data.

Keywords*: alteration; computer data; computer system; interference; malicious programmes; attack.*

§1. Introducere

Infracțiunea de alterare a integrității datelor informatice este prevăzută în art. 362 din Capitolul VI *Infracțiuni contra siguranței şi integrității sistemelor şi datelor informatice* din Codul penal. Textul de lege prevede:

„Fapta de a modifica, şterge sau deteriora date informatice ori de a restricționa accesul la aceste date, fără drept, se pedepseşte cu închisoarea de la unu la 5 ani".

Reglementarea legală din cuprinsul art. 362 din Codul penal are ca scop protejarea datelor informatice stocate în cadrul sistemelor informatice, urmărind să împiedice modificarea, ştergerea sau deteriorarea datelor informatice, ori restricționarea accesului la aceste date.

§2. Incriminarea faptei de afectare a integrității datelor informatice în cadrul Convenției Consiliului Europei privind criminalitatea informatică

Art. 4 din Convenția Consiliului Europei privind criminalitatea informatică[1] reglementează protecția integrității datelor informatice împotriva interferențelor neautorizate. Afectarea integrității datelor se realizează prin următoarele acțiuni în mod intenționat şi fără drept: *distrugerea*, *ştergerea*, *deteriorarea*, *modificarea* şi *eliminarea* datelor existente într-un sistem informatic.

Art. 4 din Convenția Consiliului Europei privind criminalitatea informatică oferă statelor membre opțiunea de a restricționa incriminarea comportamentelor descrise mai sus de producerea unor daune grave. Infracțiunea de afectare a integrității datelor informatice implică atacuri de tip hacking, scopul nefiind obținerea accesului la un sistem informatic sau interceptarea datelor informatice, ci modificarea acestor date informatice.

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

Infracțiunea de afectare ilegală a integrității datelor informatice prevăzută de art. 5 din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice[2] constă în ştergerea, distrugerea, deteriorarea, modificarea, eliminarea datelor informatice dintr-un sistem informatic sau în a le face inaccesibile. Totodată, infracțiunea de afectare ilegală a integrității datelor informatice se săvârşeşte cu intenție şi fără drept. La fel ca şi în articolele precedente, infracțiunea de afectare ilegală a integrității datelor informatice trebuie să nu reprezinte un caz minor.

Între infracțiunea prevăzută de art. 4 (afectarea ilegală a integrității sistemului informatic) şi infracțiunea prevăzută de art. 5 (afectarea ilegală a integrității datelor informatice) din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice considerăm că există o diferență între aceste două infracțiuni, în legătură cu scopul acestora. Art. 4 din Directiva 2013/40/UE cuprinde infracțiunea de afectare ilegală a sistemului informatic, prin manipularea datelor informatice din sistemul informatic. Pe de altă parte, dispozițiile art. 5 din Directiva 2013/40/UE se referă la atacurile informatice care au ca țintă numai datele informatice. Având în vedere, că majoritatea infracțiunilor care se săvârşesc în spațiul virtual necesită accesul ilegal la un sistem informatic şi afectarea ilegală a

[1] Convenția Consiliului Europei privind criminalitatea informatică a fost adoptată la Budapesta la data de 23.11.2001 şi este disponibilă pe site-ul: http://www.conventions.coe.int/Treaty/EN/Treaties/Html/185.htm, consultat la 22.10.2017.

[2] Directiva 2013/40/UE a Parlamentului European şi a Consiliului din 12 august 2013 privind atacurile împotriva sistemelor informatice şi de înlocuire a Decizei-Cadru 2005/222/JAI a Consiliului, Jurnalul Oficial al Uniunii Europene, 14.08.2013, L218/8.

sistemului informatic şi a datelor din acel sistem informatic, considerăm că cele doua infracțiuni cuprinse în articolele 4 şi 5 sunt practic inseparabile[3].

§4. Analiza infracțiunii de alterare a integrității datelor informatice prevăzute de art. 362 din Codul penal

4.1. Condiții preexistente

4.1.1. Obiectul infracțiunii

Obiectul juridic special îl constituie relațiile speciale ce vizează integritatea, funcționarea şi folosirea în condiții optime a datelor sau programelor informatice[4].

Obiectul material al infracțiunii constă în suportul material (hard-disc sau alt suport de stocare a datelor informatice) pe care se află datele modificate, şterse, deteriorate sau la care a fost restricționat accesul[5].

4.1.2. Subiecții infracțiunii

Subiectul activ al infracțiunii de alterare a integrității datelor informatice poate fi orice persoană care îndeplineşte condițiile generale prevăzute de lege pentru a răspunde penal.

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

Subiectul pasiv al infracțiunii de alterare a integrității datelor informatice este persoana fizică sau juridică care are drepturi (de proprietate, de utilizare) asupra datelor sau programelor informatice.

4.2. Conținutul constitutiv

4.2.1. Latura obiectivă

Elementul material al infracțiunii de alterare a integrității datelor informatice se realizează prin mai multe acțiuni alternative de a modifica, şterge sau deteriora date informatice ori de a restricționa accesul la aceste date informatice[6].

Actele prin care se realizează elementul material al infracțiunii de alterare a integrității datelor informatice produc efecte negative asupra datelor informatice, mai ales cu privire la a funcționarea acestora în maniera prevăzută de persoana care utilizează sistemele informatice ce conțin aceste date[7].

---

[3] A se vedea Adrian Cristian Moise, *Dimensiunea criminologică a criminalității din cyberspațiu*, Ed. C.H. Beck, Bucureşti, 2015, p. 144.

[4] Ioana Vasiu, Lucian Vasiu, *Informatică juridică şi drept informatic*, Ed. Albastră, Cluj-Napoca, 2007, p.135.

[5] Ministerul Administrației şi Internelor. Secretariatul General. Serviciul Informare-Documentare, *Criminalitatea Informatică. Sinteză Documentară*, Tipografia Ministerului Administrației şi Internelor, Anul VII, nr.2 (25), Bucureşti, 2006, p. 28.

[6] Maxim Dobrinoiu, *Infracțiunea de alterare a integrității datelor informatice*, în Revista Română de Dreptul Proprietății Intelectuale nr.3/2006, p. 59.

[7] Maxim Dobrinoiu, *Infracțiuni în domeniul informatic*, Ed. C.H. Beck, Bucureşti, 2006, pp. 180-183.

Modificarea datelor informatice se referă la introducerea de noi date sau ştergerea anumitor secțiuni care au ca rezultat formarea unor noi date informatice, diferite de cele inițiale şi neconforme cu ceea ce reprezentau aceste date[8]. Prin urmare, suntem de părere că modificarea datelor informatice se referă la acțiunea de alterare a datelor existente în special prin instalarea unor programe malițioase.

Ştergerea datelor informatice reprezintă acțiunea de îndepărtare a datelor din dispozitivele de stocare a datelor informatice. De asemenea, ştergerea poate însemna şi distrugerea suportului de date, rescrierea pe discuri optice rescriptibile (CD-RW, DVD-RW), memorii flash[9]. Ştergerea datelor informatice nu constituie totdeauna şi eliminarea acestora definitivă. Există situații, în care datele informatice şterse pot fi recuperate cu ajutorul unor software de investigare criminalistică a infracțiunilor informatice, cum sunt de exemplu, software-le care utilizează aplicațiile interfeței grafice cu utilizatorul: **ProDiscover**, **X-Ways**, **EnCase** şi **FTK**. De asemenea, datele informatice şterse pot fi recuperate şi cu ajutorul unor instrumente software care utilizează aplicațiile liniei de comandă, cum este de exemplu, software-ul **SafeBack**.

Deteriorarea datelor informatice constă în alterarea integrității datelor şi programelor informatice ca urmare a exercitării unor acțiuni fizice sau logice împotriva acestora[10].

Totodată, acțiunea de deteriorare a datelor informatice se referă şi la distrugerea parțială sau alterarea integrității sau conținutului de informații al acestor date.

Deteriorarea datelor informatice se poate realiza, fie direct prin intervenția manuală a cybercriminalului, sau indirect prin utilizarea unor programe malițioase care au ca scop infectarea sistemului informatic (de exemplu, viruşii, viermii, caii troieni sau bombele logice).

Restricționarea accesului la datele informatice reprezintă totalitatea actelor prin care datele informatice nu mai sunt accesibile, într-un anumit interval de timp, persoanelor sau softwarelor autorizate a le accesa.

Restricționarea accesului la datele informatice constituie rezultatul acțiunilor exercitate de către cybercriminal asupra sistemelor informatice sau suporturilor de stocare a datelor informatice. Datele informatice vor continua să existe, ele nefiind şterse, în schimb, acestea nu mai pot fi accesate, întrucât nu mai sunt disponibile[11].

---

[8] Ionuț Ciprian Spiridon, *Reflecții cu privire la legislația română în domeniul criminalității informatice*, în Revista Dreptul nr. 6/2008, p. 240.

[9] Adrian Cristian Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Ed. Universul Juridic, Bucureşti, 2011, p. 80.

[10] Ioana Vasiu, Lucian Vasiu, *op.cit.*, p. 136.

[11] Mihai Adrian Hotca, Maxim Dobrinoiu, *Infracțiuni prevăzute în legi speciale*, Ed. C.H. Beck, Bucureşti, 2008, p. 592.

Urmarea imediată constă în atingerea adusă integrității datelor informatice printr-una din activitățile incriminate de legiuitor în art. 362 din Codul penal.

Între activitatea cybercriminalului şi urmarea imediată produsă trebuie să existe o legătură de cauzalitate, aceasta rezultând din materialitatea faptei.

4.2.2. Latura subiectivă

Pentru existența infracțiunii de alterare a integrității datelor informatice este necesar ca fapta să fie săvârşită cu vinovăție. În acest caz, forma de vinovăție necesară este intenția atât directă, cât şi indirectă.

4.3. Formele infracțiunii

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

Tentativa este posibilă şi se pedepseşte conform art. 366 C. pen..

Consumarea infracțiunii de alterare a integrității datelor informatice se realizează în momentul în care se produc oricare dintre acțiunile cuprinse în elementul material al infracțiunii. Aşadar, infracțiunea de alterare a integrității datelor informatice se consideră consumată atunci când infractorul a modificat, şters sau deteriorat în vreun fel datele dintr-un sistem informatic sau a restricționat accesul la aceste date deținătorului legitim al sistemului informatic.

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

Infracțiunea de alterare a integrității datelor informatice poate fi săvârşită în formă continuă sau continuată.

4.4. Modalități

Infracțiunea de alterare a integrității datelor informatice prezintă patru modalități normative: modificarea, ştergerea, deteriorarea sau restricționarea accesului la datele informatice.

4.5. Sancțiuni

Pedeapsa prevăzută pentru infracțiunea de alterare a integrității datelor informatice este închisoarea de la unu la 5 ani.

Acțiunea penală se pune în mişcare din oficiu.

§5. Atacuri întâlnite în criminalitatea informatică care afectează integritatea datelor informatice

Unele dintre cele mai des întâlnite atacuri împotriva sistemelor informatice, care afectează integritatea datelor informatice cuprinse în acestea sunt atacurile cu viruşi.

Viruşii reprezintă programe malițioase care au ca obiectiv infectarea sistemelor şi datelor informatice.

Un virus este un program care infectează fişiere executabile sau fişiere obiect[12]. Orice program care se multiplică fără acordul utilizatorului este un virus. De obicei, un virus se ataşează la un fişier astfel încât virusul rulează în memorie sau în sistemul de operare de fiecare dată când sistemul execută fişierul infectat.

Odată ce virusul a infectat un sistem informatic, acesta efectuează două sarcini separate. Astfel, prima sarcină este de a se multiplica el însuşi prin răspândirea către alte sisteme informatice[13]. După ce virusul s-a multiplicat prin răspândirea pe alte sisteme informatice, acesta efectuează a doua sarcină prin care se activează funcția sa malițioasă.

În literatura de specialitate a fost realizată o clasificare a viruşilor[14]:

a. Viruşi care infectează fişiere de programe executabile (fişiere cu extensia **.EXE**; **.COM**).

b. Virusul rezident

Acesta este un virus care se încarcă în memoria RAM, de fiecare dată când sistemul informatic este deschis, acesta rămânând acolo. Un virus rezident poate întrerupe aproape orice funcție executată de sistemul de operare, acesta fiind alterat.

c. Virusul boot infectează Master Boot Record (MBR) al hard-discului, acesta conținând programe necesare pentru pornirea sistemului informatic şi o descriere a modului cum unitatea de disc este organizată (tabela de partiție).

d. Virusul companion

Acesta este un virus care se ataşează la un fişier executabil prin crearea unui nou fişier cu o altă extensie.

e. Macro Virusul

Acest virus este un program scris într-un script, denumit *macro*. Un *macro* reprezintă o serie de comenzi şi instrucțiuni care pot fi grupate împreună într-o singură comandă. Aceste comenzi şi instrucțiuni sunt utilizate pentru a automatiza o serie de sarcini complexe sau de a repeta aceste serii de sarcini.

Când documentul utilizatorului este deschis, instrucțiunile virusului *macro* sunt executate şi infectează sistemul informatic[15].

---

[12] Maxim Dobrinoiu, *Infracțiunea de alterare a integrității datelor informatice*, în Revista Română de Dreptul Proprietății Intelectuale nr.3/2006, p. 62.

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

[14] A se vedea Mark Ciampa, *Security. Guide To Network Security Fundamentals*, ed. a III-a, Ed. Course Technology. Cengage Learning, Boston, Massachusetts, 2009, pp. 42-43; Adrian Cristian Moise, *Metodologia investigării criminalistice a infracțiunilor informatice, op. cit*., pp. 143-144.

[15] National Institute of Standards and Technology. U.S. Department of Commerce, *Computer Security.Incident Handling Guide*, Gaithersburg, Maryland, 2008, pp. 5-2, disponibil pe site-ul: http://csrc.nist.gov/publications/ PubsSPs.html, consultat la 22.10.2017.

f. Virusul polimorfic

Acest virus se modifică ori de câte ori apare şi îşi criptează conținutul, fiind foarte dificil de detectat.

§6. Concluzii

Având în vedere cele prezentate mai înainte, observăm faptul că legea penală română nu enumeră ca modalități alternative *distrugerea* sau *eliminarea* datelor informatice ca în textele Convenției Consiliului Europei privind criminalitatea informatică şi Directivei 2013/40/UE privind atacurile împotriva sistemelor informatice, ci introduce o modalitate nouă de săvârşire a infracțiunii, şi anume *restricționarea accesului* la datele informatice dintr-un sistem informatic sau dintr-un mijloc de stocare a datelor informatice.

Totodată, infracțiunea de alterare a integrității datelor informatice, deşi aparent este o infracțiune de pericol, considerăm că de fapt este o infracțiune de rezultat deoarece presupune producerea unui prejudiciu proprietarilor de sisteme (în caz de modificare, ştergere, deteriorare a datelor informatice) sau utilizatorilor legitimi ai sistemelor informatice (prin restricționarea accesului la datele informatice).

Astfel, având în vedere analiza efectuată, remarcăm că România a transpus aproape în totalitate prevederile art. 4 (afectarea integrității datelor) din Convenția Consiliului Europei privind criminalitatea informatică cât şi prevederile art. 5 (afectarea ilegală a integrității datelor) din Directiva 2013/40/UE privind atacurile împotriva sistemelor informatice în textul art. 362 C. pen.

Bibliografie

1. Mark Ciampa, *Security. Guide To Network Security Fundamentals*, ed. a III-a, Ed. Course Technology. Cengage Learning, Boston, Massachusetts, 2009.

2. Maxim Dobrinoiu, *Infracțiunea de alterare a integrității datelor informatice*, în Revista Română de Dreptul Proprietății Intelectuale nr.3/2006.

3. Maxim Dobrinoiu, *Infracțiuni în domeniul informatic*, Ed. C.H. Beck, Bucureşti, 2006.

4. Chuck Easttom, Jeff Taylor, *Computer Crime, Investigation, and the Law*, Ed. Course Technology, Cengage Learning, Boston, Massachusetts, 2010.

5. Mihai Adrian Hotca, Maxim Dobrinoiu, *Infracțiuni prevăzute în legi speciale*, Ed. C.H. Beck, Bucureşti, 2008.

6. Ministerul Administrației şi Internelor. Secretariatul General. Serviciul Informare-Documentare, *Criminalitatea Informatică. Sinteză Documentară*, Tipografia Ministerului Administrației şi Internelor, Anul VII, nr. 2 (25), Bucureşti, 2006.

7. Adrian Cristian Moise, *Dimensiunea criminologică a criminalității din cyberspațiu*, Ed. C.H. Beck, Bucureşti, 2015.

8. Adrian Cristian Moise, *Metodologia investigării criminalistice a infracțiunilor informatice*, Ed. Universul Juridic, Bucureşti, 2011.

9. National Institute of Standards and Technology. U.S. Department of Commerce, *Computer Security.Incident Handling Guide*, Gaithersburg, Maryland, 2008.

10. Julie Traxler, Jeff Forristal, *Hach Proofing Your Web Applications*, Ed. Syngress Publishing Inc., Rockland, Massachusetts, 2001.

11. Ionuț Ciprian Spiridon, *Reflecții cu privire la legislația română în domeniul criminalității informatice*, în Revista Dreptul nr. 6/2008.

12. Ioana Vasiu, Lucian Vasiu, *Informatică juridică şi drept informatic*, Ed. Albastră, Cluj-Napoca, 2007.