Analysis of Directive 2013/40/EU on attacks against information systems in the context of approximation of law at the European level

Lecturer Adrian Cristian MOISE, PhD.
Postdoctoral researcher, Titu Maiorescu University of Bucharest, Romania
adriancristian.moise@gmail.com.

Abstract:
In this article is carried out an analysis of one of the most important legal instruments at the level of the European Union in the field of fight against cybercrime: Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. This legal instrument in the fight against cybercrime has as subject matter to establish minimum rules concerning the definition of criminal offences and sanctions in the area of attacks against information systems. Also, Directive 2013/40/EU aims to develop a legal framework to prevent such offences and to improve cooperation between law enforcement bodies.
The article presents and analyzes the five categories of offences committed against information systems which are stipulated in Directive 2013/40/EU on attacks against information systems.
Keywords: *information system; computer data; attacks; cybercrime; Directive 2013/40/EU.*

This work was supported by the strategic grant POSDRU/159/1.5/S/141699, Project ID 141699, co-financed by the European Social Fund within the Sectorial Operational Program Human Resourses Development 2007-2013

1. Introduction

European Union has a limited ability to legislate in the area of criminal law, which has always been seen as a symbol of national sovereignty. Although European Union is, first of all, an organization of commercial policies, it has limited competencies in regulating criminal law. This situation is due to the fact that offence is an obstacle to trade between the Member States of the European Union, while for a stable economic and social development it is needed a more effective judicial cooperation in criminal matters.

The provisions of Article 83 paragraph 1 of the Treaty on the Functioning of the European Union [1] allow the Member States of the European Union to adopt directives that establish the „minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis". The offences of particularly seriousness, with a cross-border

dimension are the following: terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime and organised crime. The European Union Council unanimously decide, after the approval of the European Parliament, whether other offences may be added to the list of offences mentioned above, taking into account the evolution of crime.

Another possibility is stipulated in Article 83 paragraph 2 of the Treaty on the Functioning of the European Union concerning offences which are not particularly serious:

„If the approximation of criminal laws and regulations of the Member States proves essential to ensure the effective implementation of a Union policy in an area which has been subject to harmonisation measures, directives may establish minimum rules with regard to the definition of criminal offences and sanctions in the area concerned. Such directives shall be adopted by the same ordinary or special legislative procedure as was followed for the adoption of the harmonisation measures in question, without prejudice to Article 76".

The provisions of article 84 of the Treaty on the Functioning of the European Union allow promoting and supporting the actions of the Member States in the field of crime prevention, excluding any harmonisation of the laws and regulations of the Member States. Thus, Eurojust, the body of the European Union for the cooperation in criminal matters, created in the year 2002 through the Decision of the Council of the European Union 2002/187/JHA [2] of 28 February 2002, amended by the Decision of the Council of the European Union 2009/426/JAI [3] of 16 December 2008 has the role to stimulate and improve coordination of investigations and prosecutions among the competent judicial authorities in the Member States of the European Union when dealing with cross-border crime and serious organised crime [4].

In conformity with the provisions of Article 1 of Directive 2013/40/EU [5] of the European Parliament and of the Council of 12 August 2013 on attacks against information systems, the subject matter of this legal instrument is to establish minimum rules concerning the definition of criminal offences and sanctions in the area of attacks

against information systems. Also, this Directive aims to develop a legal framework to prevent such offences and to improve cooperation between law enforcement bodies.

In Article 2 of the Directive are presented several definitions, such as the notions of information system and computer data. Information system is defined as being a „device of inter-connected or related devices, one or more of which, pursuant to a programme, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of its or their operation, use, protection and maintenance". Also, computer data refers to „a representation of facts, information or concepts in a form suitable for processing in an information system, including a programme suitable for causing an information system to perform a function".

2. Analysis of offences stipulated by Directive 2013/40/EU on attacks against information systems

Directive 2013/40/EU on attacks against information systems comprises five categories of offences committed against information systems.

Thus, the first category of offence, stipulated by Article 3 of the Directive, refers to illegal access to information systems. This category of offence comprises a series of computer attacks, also known in the literature as hacking. The offence consists in committing intentionally the access without right to the whole or to any part of an information system, by infringing a security measure. The offence of illegal access to information systems must not be a minor case. In conformity with ground no.11 of the Directive, a case may be considered minor, „where the damage caused by the offence and/or the risk to public or private interests, such as to the integrity of a computer system or to computer data, or to the integrity, rights or other interests of a person, is insignificant or is of such a nature that the imposition o a criminal penalty within the legal threshold or the imposition of criminal liability is not necessary".

Offender in the area of IT illegally accesses information system by infringing a security measure. The most commonly encountered security measures used against illegal access to an information system are the following: passwords, access codes and encryption codes.

The second type of offence refers to illegal system interference. The offence of illegal system interference is stipulated by Article 4 of the Directive 2013/40/EU and consists in seriously hindering or interrupting the functioning of an information system by inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible. The offence of illegal system interference is committed intentionally and without right. Like in the previous article, the offence of illegal access to information system must not be a minor case.

The most known attack against an information system affecting the information system interference is Denial of Service-DOS- attack. In this form of attack, the offender tries to deny to authorized users the access to specific information, information systems and the network itself. DOS attack is in fact an attempt of the offender to make information resources unavailable for legitimate users. The purpose of such attack may be simply the prevention of access to target information system or the attack may be used with other actions in order to obtain unauthorized access to an information system or computer network.

Other attacks against an information system affecting the information system interference are the attacks based on malicious programs having as purpose to infect the information system, such as viruses. Usually, a virus installs a malicious code which may have different purposes, starting from the deterioration of user's information system and continuing with the extraction of valuable personal data, such as bank accounts, credit card accounts, etc.

The third type of offence refers to illegal data interference. Thus, the offence of illegal data interference stipulated by Article 5 of the Directive consists in deleting, damaging, deteriorating, altering or suppressing computer data on an information system, or rendering such data inaccessible. The offence of illegal data interference is committed intentionally and without right. Like in previous articles, the offence of illegal data interference must not be a minor case.

Between the offence referred to in Article 4 and the offence referred to in Article 5 of the Directive, I consider that there is a difference between these two offences, in relation to their purpose. Article 4 of the Directive comprises the offence of illegal system interference, by manipulation of computer data on the information system. On

the other hand, the provisions of article 5 refer to computer attack having as target only the computer data. Considering that most of the offences committed in cyberspace need illegal access to an information system and illegal system interference and illegal data interference, I think that the two offences referred to in Articles 4 and 5 are practically inseparable.

The fourth category of offence refers to illegal interception. Article 6 of the Directive contains the provisions relating to illegal interception, consisting in intercepting, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data. The offence of illegal interception is committed intentionally and without right. Like in previous offences of the Directive, the offence of illegal interception must not be a minor case. The activity of interception by technical means, requires listening, supervising of the content of communications, procurement of computer data either directly, by accessing and using the information system, or indirectly, by using some listening and/or recording electronic devices. The technical means are devices fixed on communication lines or devices designed to collect and record wireless communications [6].

The fifth category of offence, contained in Article 7 of the Directive refers to tools used for committing offences mentioned at articles 3 to 6. Thus, according to Article 7 of the Directive, the Member States are required to adopt the necessary measures to ensure that the intentional production, sale, procurement for use, import, distribution or otherwise making available, of one of the following tools, without right and with the intention that it be used to commit any of the offences referred to in Articles 3 to 6, is punishable as a criminal offence, at least for cases which are not minor:

" (a) a computer programme, designed or adapted primarily for the purpose of committing any of the offences referred to in Articles 3 to 6;

(b) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed".

In the Article 8 of the Directive are stipulated the provisions relating to incitement, aiding and abetting and attempt. Thus, in the Directive are criminalised incitement, aiding and abetting to commit any of the offences referred to in Articles 3 to 7 of the

Directive 2013/40/EU on attacks against information systems. Also, the attempt to commit an offence referred to in Articles 4 and 5 of the Directive is punishable as a criminal offence. We notice that the attempt is not criminalized in the Directive at Articles 3, 6 and 7, although that it is possible for these offences.

Member State are obligated, according to the provisions of Article 9 paragraph 1 of the Directive, to introduce to offences referred to in Articles 3 to 8 effective, proportionate and dissuasive criminal penalties. In particular, offences referred to in Articles 3 to 7 are punishable by a maximum term of imprisonment of at least two years, at least for cases which are not minor.

Offences referred to in Articles 4 and 5, when committed intentionally, are punishable by a maximum term of imprisonment of at least three years where a significant number of information systems have been affected through the use of a tool cu referred to in Article 7, designed and adapted primarily for that purpose. Also, in compliance with Article 9 paragraph 4 of the Directive, offences referred to in Articles 4 and 5 are punishable by a maximum term of imprisonment of at least five years where: they are committed within the framework of a criminal organization, as defined in the Framework Decision 2008/841/JHA on the fight against organised crime, irrespective of the penalty provided for therein; they cause serious damages; they are committed against a critical infrastructure information system.

According to Article 9 paragraph 5 of the Directive, the Member States shall take the necessary measures to ensure that when the offence of illegal system interference (Article 4) and the offence of illegal data interference (Article 5) are committed by misusing the personal data of another person, with the aim of gaining the trust of a third party, thereby causing prejudice to the rightful identity owner, this may, in accordance with national law, be regarded as aggravating circumstances, unless those circumstances are already covered by another offence, punishable under national law.
Taking into consideration the penalties applied for committing the offences referred to in Articles 3 to 7, I notice the existence of a national policy of the European Union, which sends a clear message about the seriousness of the way of approaching the phenomenon of cybercrime at the level of the European Union.

An important provision is the text of Article 10 paragraph 1 of the Directive, which ensures that legal persons can be held liable for offences referred to in Articles 3 to 8, committed for their benefit by any person, acting either individually or as a part of the legal person. In both situations, the person must have a leading position within that legal person, based on one of the following: a power of representation of the legal person, an authority to take decisions on behalf of the legal person and an authority to exercise control within the legal person.

Also, in Article 10 of the Directive, specifically in paragraph 2, the Member States are required to adopt the necessary measures to ensure that legal persons can be hold liable where the lack of supervision or control by a person referred to in paragraph 1, allowed the commission, by a person under its authority, of any of the offences referred to in Articles 3 to 8, for the benefit of that legal person. Finally, the liability of legal persons shall not exclude criminal proceedings against natural persons who are perpetrators or inciters of, or accessories to, any of the offences referred to in Articles 3 to 8 of the Directive.

In accordance with the provisions of article 11 of the Directive, sanctions against legal persons include criminal or non-criminal fines and other sanctions, such as: exclusion from entitlement to public benefits or aid; temporary or permanent disqualification from the practice of commercial activities; placing under judicial supervision; judicial winding-up; temporary or permanent closure of establishments which have been used for committing the offence.

Problems relating to establishing of criminal jurisdiction in case of committing the offences mentioned in the Directive 2013/40/EU on the attacks against information systems are referred to in Article 12. Establishment of jurisdiction with regard to the offences referred to in Articles 3 to 8 is carried out in case the offence has been committed: [7] ”a) in whole or in part within their territory; or b) by one of their nationals, at least in cases where the act is an offence where it was committed”.

In accordance with Article 12 paragraph 2 of the Directive, when establishing jurisdiction in accordance with point (a) of paragraph 1 of the Directive, a Member State shall ensure that it has jurisdiction where :

”(a) the offender commits the offence when physically present on its territory, whether or not the offence is against an information system on its territory; or

(b) the offence is against an information system on its territory, whether or not the offender commits the offence when physically present on its territory”.

Paragraph 3 of Article 12 stipulates the fact that the Member States may decide to establish jurisdiction over an offence referred to in Articles 3 to 8, committed outside its territory including where:

”(a) the offender has his or her habitual residence in its territory; or

(b) the offence is committed for the benefit of a legal person established in its territory”.

According to the provisions of Article 13 of the Directive, for the purpose of exchanging information relating to the offences referred to in Articles 3 to 8, Member States shall ensure that they have an operational national point of contact and that they make use of the existing network of operational points of contact available 24 hours a day and seven days a week. Member States shall also ensure that they have procedures in place so that for urgent requests for assistance, the competent authority can indicate, within eight hours of receipt, at least whether the request will be answered, and the form and estimated time of such an answer.

Also, paragraph 2 of Article 13 stipulates that the Member States shall inform the European Commission of their appointed point of contact. European Commission shall forward that information to the other Member States and competent specialised European Union agencies and bodies.

According to paragraph 3 of Article 13, Member States must take the necessary measures to ensure the appropriate reporting channels are made available in order to facilitate the reporting of the offences referred to in Articles 3 to 6 of the Directive to the competent national authorities without undue delay.

3. Conclusions

Having regard to the provisions of Directive 2013/40/EU on attacks against information systems and those of the Council of Europe Convention on cybercrime, which is the most important legal instrument at international and European level in the field of the fight against cybercrime, I have to make several comments. First of all, I notice the fact that the Directive 2013/40/EU on attacks against information systems

does not define one of the most important notions which is used still from its title: the notion of attack against an information system. I appreciate that the legislators of the Directive had to define the notion of attack on an information system, to better explain the steps to perform it and the offences committed as result of these steps. In the literature [8] there are some approaches in relation to the definition of the notion of attack against an information system and the stages through which the attack is performed.

Secondly, there are some differences between the two legal instruments in the field of fight against cybercrime. Thus, the provisions of Article 2 of the Council of Europe Convention on cybercrime criminalises the offence of illegal access to information system by infringing a security measure with the intention to get computer data and the offence of illegal access of a system connected to the network. I also notice that the provision relating to illegal access to information system connected to the network is not comprised in Directive 2013/40/EU on attacks against information systems. Having regard to the importance of computer networks in committing cybercrimes, we believe that the legislators of the Directive had to take into consideration this aspect too when they elaborated this regulatory act.

Third, following the carried out analysis, it was found that Directive 2013/40/EU on attacks against information systems, as well as the Convention, do not refer to the new types of offences, such as identity theft, spam, use of Internet in relation to terrorist activities.

Fourth, I noticed the fact that all offences in the Directive, as well as other definitions and procedural institutions are also contained in the Council of Europe Convention on cybercryme, as it follows: illegal access to information systems (Article 3 Directive) - illegal access (Article 2 Convention); illegal system interference (Article 4 Directive) – system interference (Article 5 Convention); illegal data interference (Article 5 Directive) – data interference (Article 4 Convention); illegal interception (Article 6 Directive) – illegal interception (Article 3 Convention); tools used for committing offences (Article 7 Directive) – misuse of devices (Article 6 Convention); the definition of the terms information system and information data (Article 2 Directive) - the definition of the terms information system and information data (Article 1 Convention); exchange of

information (Article 13 Directive) - 24/7 Network (Article 35 Convention) and mutual assistance regarding accessing of stored computer data (Article 31 Convention); jurisdiction (Article 12 Directive) – jurisdiction (Article 22 Convention).

Also, I noticed the fact that in the Directive are absent some very important procedural law instruments, such as computer search and conservation of computer data.

On the matter of the offence of illegal system interference referred to in Article 4 of the Directive, I noticed the fact that the legislators of the Directive did not make, in the text of this article, a clear delimitation between serious offences determining a serious illegal system interference, such as DOS attacks prepared through organised crime for the purpose of extortion and attacks prepared by different natural persons for political purposes.

References

[1]Treaty on the Functioning of the European Union, Official Journal of the European Union, 26.10.2012, C326/47, Retrieved 29 April 2015 from: http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:12012E/TXT&from=en.
[2]Council Decision 2002/187/JHA of 28 February 2002 setting up Eurojust with a view to reinforcing the fight against serious crime, Official Journal of the European Communities, L 63, 06.03.2002, Retrieved 29 April 2015 from: http://www.eurojust.europa.eu/official_documents/eju_dec.htm.
[3]Council Decision 2009/426/JAI of 16 December 2008 on the strengthening of Eurojust and amending, Official Journal of the European Union, L 138, 04.06.2009, Retrieved 29 December 2014 from: http://www.eurojust.europa.eu/official_documents/eju_dec.htm.
[4]Eurojust, Retrieved 29 April 2015 from: https://e-justice.europa.eu/contentPresentation.do?&lang=ro&idTaxonomy=23&id Country=EU&vmac=0jSB5FQ85OXgZ4joc4nryj7FXgk7uXy84e3S3gLW2VdEhkj8SVxzp0bo7eyPIiZgrrejrJiZ_thT4a2PvmdN_AAAAV4AAADo.
[5]Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA, 14.08.2013, L218/8, Retrieved 21 April 2015 from: http://eur-lex.europa.eu/legal-content/RO/TXT/PDF/?uri=CELEX:32013L0040&from=RO.
[6]Moise, A.C. (2011). Metodologia investigării criminalistice a infracţiunilor informatice. Bucharest: Universul Juridic Publishing House, pp.75.
[7]Article 12 paragraph 1 of the Directive 2013/40/EU on attacks against information systems.
[8]Moise, A.C. (2011). Metodologia investigării criminalistice a infracţiunilor informatice. Bucharest: Universul Juridic Publishing House, pp.141-142, where the following notions are used: ”Attack is an action brought against a target, by using a tool, exploiting vulnerability, for the purpose of getting an unauthorised result. An attack against an information system is performed according to the following steps: 1. Research of information system for the purpose of getting information; 2. Entering the information system; 3. Modification of the information system settings; 4. Communication with other systems; 5. Networks and devices interference”.