EUROPEAN COOPERATION IN FIGHTING CYBERCRIME

Liana Iulia PAUL*

Abstract

In the last years cybercrime has increased significantly in Europe and across the world. Thus we may notice a wide range of efforts in order to combat this phenomenon.

National and international institutions were created for this purpose with the aim to protect social, political and economic development.

The paper also underlines the most common cybercrime aspects and the importance of international cooperation in this area.

Key words: *European cooperation, cybercrime, institutions, rights*

JEL Classification: [K14]

1. Preliminary Considerations

In the last years cybercrime has increased significantly in Europe and across the world.

Sophisticated computer hacking lead to the growth of cybercrimes.

Statistic reports show the prevalence of these infringements and underline the importance of the comparisons regarding the structure and trends of cybercrime.

Fundamental human rights ought to be protected in these circumstances.

The article focuses on the European cooperation, but in order to combat cyber intruders located around the globe, a good international cooperation is needed.

2. European Institutions

The affiliation of our country, Romania, to the European Union's community represents a guarantee of its stability, economic development and prosperity. [1]

According to another opinion, in order to face all types of challenges, regarding global interactions, a continuous international management development is needed. [2]

Every country has its own legal system which can be more or less elaborated.

The foundation of the EU legal framework became more and more developed due to the European ideas which arose for the protection of the same purpose – the European citizens' safety.

The European Union is the political, social and economic entity in Europe and it is composed of 28 countries since 2013. Among the most important European institutions are:

* M.A. ''Dimitrie Cantemir'' Christian University

[1] G. Fabian, *Drept instituţional comunitar,* Editura Sfera Juridică, Cluj-Napoca, 2008, p.47.

[2] V. Puşcaş, *România spre Uniunea Europeană*, Editura Institutul European, Iaşi, 2007, p.22.

a) The European Parliament;
b) The Council of European Union;
c) The European Commission;
d) The Court of Justice of the European Communities;
e) The European Court of Auditor.

The juridical norms regulating the activity of the EU's institutions, the actions and common policies are included in the so named acquis communautaire.

The acquis communautaire is a very important concept in the European Union which covers all treaties, EU legislation, international agreements, standards, court verdicts, fundamental rights provisions and horizontal principles in the treaties such as equality and non-discrimination. In short: EU-law. [3]

In order to help Member States' law enforcement agencies fight crime and terrorism the EU has built a set of tools.

Nowadays, the three of the most pressing challenges are as it follows:

- preventing terrorism and countering radicalisation;
- fighting organised crime**;**
- fighting cybercrime[4].

There are also a few key actions which are proposed:

- Countering radicalization - the Commission will set up a Centre of Excellence to collect and disseminate expertise on anti-radicalisation;
- Updating the Framework Decision on Terrorism - to provide a more coherent legal framework to deal with the foreign fighter phenomenon;
- Cutting the financing of criminals - cooperation between competent authorities in Europe will be strengthened;
- Enhancing dialogues with the IT industry - from 2015, the Commission launched an EU Forum with major IT companies to counter terrorist propaganda on the internet and in social media and to explore ways to address the concerns of law enforcement authorities on new encryption technologies;
- Strengthening the legal framework on firearms to address the illegal trafficking and reactivation of weapons, to establish common standards, share more information and boost cooperation with third countries;
- Reinforcing our tools to fight cybercrime - the priority is to identify ways to overcome obstacles to criminal investigations online, notably on issues of competent jurisdiction and rules on access to Internet-based evidence and information;

[3] See *Acquis Communautaire* available at http://en.euabc.com/word/12
[4] See *Commission take steps to strengthen EU cooperation in the fight against terrorism, organized crime and cybercrime* from http://europa.eu/rapid/press-release_IP-15-4865_en.htm

- Enhancing the capacities of Europol**,** including through the creation of a European Counter Terrorist Centre which will help the EU Agency to step up support for national law enforcement authorities' actions. [5]

We may say that a good international cooperation in the field of cybercrimes is likely to confer a more effectively protection, detection and enforcement.

3. Cybercrime Aspects

Among the three priorities of EU institutions, preventing terrorism and countering radicalization, fighting organised crime and fighting cybercrime**,** the last one is of interest in our paper.

In doctrine we may observe different opinions regarding cybercrime's definition. Terms like cybercrime, computer crime, computer-related crime or high-tech(nology) crime are being used alternatively without a precise definition.[6]

We may notice a few categories of cybercrimes:

- cybercrimes in which the computer is a target ;
- cybercrimes in which the computer is a weapon or tool of the offense;
- cybercrimes in which the computer is incidental in committing some offenses. [7]

The virtual space in which this kind of offenses can occur is suggestively called cyberspace.

Cyberspace is defined as "the global domain within the information environment consisting of the interdependent network of information systems infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers"[8]

Furthermore we must underline the computer systems and data's matchless definition. According to an opinion there are two perspectives in defining the "information system's" term.

From a traditional point of view the information system can be taken into account starting with its function or structure.

The functional perspective of the informatic's system represents a technological implemented environment with the aim to register, store and transmit information.

From the structure's perspective it consists of a human, processes, data and technologies collection which forms a structure for different functions or objectives. [9]

---

[5] *Idem.*

[6] I. Vasiu si L. Vasiu, *Criminalitatea în cyberspaţiu*, Editura Universul Juridic, Bucureşti, 2011 p. 119.

[7] *Idem,,* p. 120.

[8] See *Managing Information Security Risk* available at http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf

[9] I.Vasiu and L.Vasiu, *Dreptul tehnologiei informaţiilor şi comunicaţiilor,* Editura Albastră, Cluj-Napoca, 2014, p. 7.

For a better understanding and protection against the most encountered cybercrimes, a suggestive classification has been made: [10]

a) against individual:
- drug trafficking;
- offensive content and harassment.

b) against individual property:
- electronic funds transfer fraud;
- dissemination of offensive materials.

c) against society:
- cyber-bullying and cyber-stalking;
- cyber bullying *vs.* cyber stalking.

d) against private organizations:
- theft of telecommunications services;
- telecommunications piracy.

e) against government:
- electronic vandalism and extortion;
- cyber warfare and terrorism.

We should say that all the aspects presented above must receive appropriate attention to stop "cyber thieves from overseas"[11] achieve their objectives.

4. Efforts to Combat the Cybercrime Phenomenon

National and international institutions were created with the aim to protect social, political and economic development.

The European legal framework provides a three-path solution in order to face the cybercrime's phenomenon:

- the reduction of frictions among national legislations;
- the introduction of new investigative powers;
- the facilitation of international cooperation. [12]

[10] See *Main Types of Cybercrime* available at https://sites.google.com/site/callingoffcybercrime/types-of-cyber-crime

[11] See *Cyber Crime And Trade Secret Protection* from https://www.wilmerhale.com/uploadedFiles/Shared_Content/Editorial/Publications/Documents/Reprint-New-York-Law-Journal-CyberCrime-And-Trade-Secret-Protection-Cedarbaum-Love-2014.PDF

[12] See *The European Legal Framework on Cybercrime: striving for an effective implementation* available at http://www.ssoar.info/ssoar/bitstream/handle/document/27731/ssoar-clsc-2010-5-calderoni-the_european_legal_framework_on.pdf?sequence=1

Combating today's digital security challenges requires a collective approach in which law enforcement and private industry are compelled to work closely together. In this complex environment, such partnerships are becoming increasingly important, especially due to the rapid rate at which technology continues to evolve."[13]

We truly consider that in order to overcome obstacles we must work together to resist these threats, in full respect of human's fundamental rights.

5. Conclusions

In the last years cybercrime has increased significantly in Europe and across the world harming democratic values.

Sophisticated computer hacking lead to the growth of cybercrimes.

Fundamental human rights ought to be protected in these circumstances in order to guarantee the society's prosperity and security.

National authorities must cooperate more effectively with the EU institutions to overcome obstacles and protect the principles of the political, social and economic environment.

Every country has its own legal system which can be more or less elaborated.

The article focuses on the European cooperation, but in order to combat cyber intruders located around the globe, a good international cooperation is needed.

Bibliography

1. G. Fabian, *Drept instituţional comunitar,* Editura Sfera Juridică, Cluj-Napoca, 2008.
2. V. Puşcaş, *România spre Uniunea Europeană,* Editura Institutul European, Iaşi, 2007.
3. I. Vasiu si L. Vasiu, *Criminalitatea în cyberspaţiu,* Editura Universul Juridic, Bucureşti, 2011.
4. I. Vasiu and L. Vasiu, *Dreptul tehnologiei informaţiilor şi comunicaţiilor,* Editura Albastră, Cluj-Napoca, 2014.
5. *Acquis Communautaire* available at http://en.euabc.com/word/12
6. *Commission take steps to strengthen EU cooperation in the fight against terrorism, organized crime and cybercrime* from http://europa.eu/ rapid/press-release_IP-15-4865_en.htm
7. *Managing Information Security Risk* available at http://csrc.nist.gov/ publications

[13] *See Europol and Chainalysis Reinforce their Cooperation in the Fight Against Cybercrime* from https://www.europol.europa.eu/latest_news/europol-and-chainalysis-reinforce-their-cooperation-fight-against-cybercrime - Cooperation between Europol's EC3 and Chainalysis is already leading to successful remedial activities, in particular in the field of crypto currencies. In addition, further cooperation in this area and others have been identified with the potential to expand the sharing of cyber threat intelligence and in tackling other cyber related issues.

/nistpubs/800-39/SP800-39-final.pdf
8. *Main Types of Cybercrime* available at https://sites.google.com/site/callingoff cybercrime/types-of-cyber-crime
9. *Cyber Crime And Trade Secret Protection* from https://www.wilmerhale .com/uploadedFiles/Shared_Content/Editorial/Publications/Documents/Reprint-New-York-Law-Journal-CyberCrime-And-Trade-Secret-Protection-Cedarbaum -Love-2014.PDF
10. *The European Legal Framework on Cybercrime: striving for an effective implementation* available at http://www.ssoar.info/ssoar/ bitstream/handle/document /27731/ssoarclsc-20105calderonithe_european_legal_framework_on.pdf?sequence=1
11. *Europol and Chainalysis Reinforce their Cooperation in the Fight Against Cybercrime* from https://www.europol.europa.eu/latest_news/europol-and-chainalysis-reinforce-their-cooperation-fight-against-cybercrime-Cooperation between Europol's EC3 and Chainalysis is already leading to successful remedial activities, in particular in the field of crypto currencies. In addition, further cooperation in this area and others have been identified with the potential to expand the sharing of cyber threat intelligence and in tackling other cyber related issues.