PUBLIC ADMINISTRATION & REGIONAL STUDIES
10th Year, No. 2 (20) – 2017
Galati University Press, ISSN 2065 -1759

ABOUT CYBERCRIME IN EUROPEAN UNION

Mihaela AGHENITEI*

Abstract

Given that there is an important value in addressing the EU's fight against cybercrime in an area of justice, freedom and security, it should be stressed that the Council of Europe's Treaty on the fight against cybercrime is of considerable value. It is much more comprehensive than the EU Framework Decision and has the additional merit of being open to any country in the world interested in participation - a unique feature within the Council of Europe's instruments. Ratification includes Framework Decision no. 82 of the Annex to the Communication from the European Commission to the European Parliament and the European Council on the Implications of the European Court of Justice's judgment of 13 September 2005 in case C 176/03 COM (2005) 583 final The United States of the Treaty paves the way for a much wider, global, common to fight cybercrime.

Keywords: cybercrime; European Union; Cybercrime Treaty.

1. General approach

According to the official approach, 2017 marks "continued growth in a changing policy context" (European Commission, 2017). New trends in cybercrime are developing all the time, with estimated costs to the global operating economy billions of dollars. In the past, cybercrime was committed mainly by small groups or individuals. These days, we see extremely complex cybercrime networks, bringing together individuals from all over the world in real time to commit crimes on a tremendous scale.

The Convention on Cybercrime is the first international treaty on Internet crimes and other computer networks, dealing in particular with copyright infringements, fraud computer, infant pornography, and network security breaches. It also contains a number of skills and procedures, such as computer networks search and legal interception.

The Convention stipulates that its objective is to protect "society against cybercrime" by ensuring that such behaviour is incriminated and that sufficient powers are in place to effectively combat these crimes by facilitating detection, investigation and prosecution at national level, and internationally, and by ensuring swift and reliable international cooperation measures.

It is undoubtedly commonplace to assert that information and communication technologies (ICTs) are having a fundamental impact on our society. In this sense, the success of the 'information society' has been considered essential for Europe's growth, competitiveness and employment opportunities (http://eur-lex.europa.eu., 2001). I

In the field of cybercrime, there is a constant trend of development, the cost being estimated at the global economy, at the billions of dollars.

* Ph.D Lecturer, „Dunarea de Jos" University Galati, Faculty of Legal, Social and Political Sciences, e-mail: Aghenitei.Mihaela@ugal.ro

2. Point of view

Making that success a reality requires nevertheless, face the persistent threat of integrity-related computer crime. More strikingly, the threat needs to be dealt with in the framework of the global challenge posed to criminal justice by the development and widespread use of new technologies.

Already acknowledging this situation, the Council of Europe presented for adoption on November 2001 - Convention on Cybercrime, also recognized under the 'Cybercrime Treaty' (Council of Europe, 2001).

Open for ratification by the world at large and most notably recently ratified by the United States (xxx, 2006) the Treaty contains provisions regarding both criminal law and law of criminal procedure and criminal investigation, as well as regarding mutual assistance. Offences need to fulfil two general conditions in order to fall within its scope: firstly, to qualify as criminal offences and, secondly, to be committed deliberately and 'without right'. They are divided into four main categories: 1) offenses concerning the confidentiality, integrity and availability of systems and computer data, comprising illegal access, illegal interception, data interference, system interference and misuse of devices; 2) computer-related offences such as forgery and computer fraud; 3) content-related offences, in particular the production, dissemination and possession of child pornography (a protocol to the Convention covers the propagation of racist and xenophobic ideas); 4) offences related to infringement of copyright and related rights. Corporate liability for those offences is provided under certain conditions.

Notwithstanding the harmonization of substantive ICT criminal law, the aim of the Treaty is also to induce the ratifying countries to adapt their criminal procedural legislation to technology developments. In this sense, the Convention contains specific procedural rules on the rapid preservation of computer-stored data, production orders, the search, verification and confiscation of stored computer data, the real-time collection of such data as well as the applicable jurisdiction.

Moreover, the Treaty's provisions set out a series of general principles concerning international co-operation, extradition, mutual assistance, and spontaneous information. In order to stimulate international co-operation, a series of rules are provided on extradition of suspects under specific conditions, as well as on the Establishment of other forms of co-operation in the field of criminal investigation and prosecution, such as a network of contact points with a 24/7availability.

The Cybercrime Treaty was the first important international binding legal instrument to address the issue of cybercrime, but is no longer the only relevant transnational text for EU Member States.

The Council of the European Union (EU) adopted on 24 February 2005, Framework Decision 2005/222 / JHA on attacks against information systems (hereinafter referred to as the Framework Decision) with the objective of implementing judicial cooperation and other competent authorities, and other specialized law enforcement services by approximating national criminal law rules in the field of attacks against information systems (European Council, 2005).

The Framework Decision is structured around the definitions of 'illegal access', 'data interference', and 'system interference' as criminal offences.
As the Convention gives the participating countries considerable options to reserve and establish additional conditions for the described acts to constitute an offense, it is considered that the Framework Decision often contains stricter obligations for EU Member States to take useful measures to in line with its provisions, imposing the implementation on 16 March 2007 (European Council, 2005).

The urgency felt by the EU in adopting such a text is and must be related to the prior adoption of the EU Framework Decision adopted by the EU Council on 13 June 2002 on the European Arrest Warrant with teaching procedures between EU Member States, and that is the true (European Council, 2005; European Council, 2002). Article 2 (2) of this decision contains a generic list of 32 types of offenses for which the possibility of double criminality is abolished: those offenses are punishable in the issuing Member State by a custodial sentence or detention order for a maximum period of at least three years and are defined by the law of the issuing Member State, in accordance with the provisions of the Framework Decision for which double criminality is no longer necessary, lead to the surrender of the person concerned under a European arrest warrant.

The removal of the double criminality requirement can pose serious problems for the requested Member State or for another Member State where the act was 'committed' if the acts covered by the list are not in fact (criminal) offences there. Moreover, the list provides extremely vague descriptions, containing references such as 'sabotage' or 'racketeering', generally not correlating to well-defined types of crimes. This situation can easily lead to abuse, either by negligence or by intent, making it possible for judicial authorities to treat as 'listed' facts acts that can reasonably deemed not to fit the list, maybe hoping to obtain surrender with fewer data than otherwise required. The expression 'computer-related crime' is precisely one of those terms on the Article 2(2) list which is not defined. The open character of the cybercrime notion (Downing, R.W.,2005) explains in this sense the need felt for the adoption of an EU definition, considered necessary in order the make the European Arrest Warrant fully operational.

The emerging of two different but overlapping cybercrime instruments in Europe invites a comparison between the two. In this article, we analyse both instruments to determine the added value of the Framework Decision over the more comprehensive Cybercrime Treaty. This is not only interesting in the context of the fight against cybercrime, but also in view of the wider debate on the relationship – competition or complimentarily – of the 'two Europe'.

This paper does not, however, provide a systematic, comprehensive comparison of the Council of Europe Convention and the Framework Decision, which would be a rather tedious exercise. Rather, it focuses in section 2 on a series of concrete cybercrime problems: hacking, data and systems interference, spam, spyware, identity theft and phishing. This is a rather personal choice, driven by what we consider particularly topical problems in today's society. We place specific emphasis on the legal potential of both European legislative reactions to those threats, taking special care not to forget

that, in practical terms, most of those acts are strongly interlinked. As the Framework Decision is not the only legal instrument configuring the policy response at the EU level, a wider overview of legal instruments is hinted at. Following this approach, the problem of policing cybercrime and criminal law in the era of cybercrime is considered as well, giving special attention to the need not only for suitable substantive legislation, but also for appropriate measures concerning criminal procedure and criminal investigation. The topical subjects of multi-loci problems and data retention serve the purpose of illustrating the discussion in final of the paper. We end with a conclusion on the added value of the Framework Decision and on the merits of both European instruments at large in the fight against cybercrime.

The absence of a clear distribution of responsibilities to establish information security and to prevent cybercrime is perhaps one of the most important factors explaining the success of computer-related crime. The strategies more generally supported to ensure adequate information security and cybercrime prevention usually entail a mixture of legal, technological, and market-based solutions, as a strict law-enforcement agenda is in most cases believed to be unfeasible or inappropriate.

The problems related to investigation and prosecution of cybercrimes are numerous and can even concern the lack of balance between expenditure, which can be very important, and the multiplication of small-impact victimizations distributed across numerous jurisdictions (Grabosky, P., 2000). Although it has to be underlined that investigation and prosecution of computer-related crimes is especially challenging, it should be pointed out that ICT can also render investigation and prosecution of 'traditional' crimes particularly difficult (Wall, D.S., 2005).

This is all the more so, now changes in the organization of criminal activity and global social transformations are slowly leading to a situation where the implications of digital networks are every day less limited to strictly computer-related crime. Criminal justice has to adapt to these changes by transforming substantive criminal law in order to cover new and transnational crimes, but also by examining provisions related to procedural law and criminal investigations. We will now address some of the challenges in the information society to criminal justice in relation to two concrete issues, multi-loci problems and data retention.

There is probably no need to describe cyberspace as a new 'social topology' to acknowledge its structural and essential transnational dimension (Wall, D.S., 2005).

In any case, organized crime groups have not waited for explorations of the conceptual implications of widespread use of the Internet to see how they could take profit of the special nature of cyberspace. Very soon, they realized the potential of the absence of borders in the virtual world in contributing to the 'free flow' of crime and crime-related organizations, while the persistence of borders in the 'real world' still renders difficult, slow, expensive, or impossible the movements and cooperation of law-enforcement authorities. Always looking for the least risky way of obtaining maximum benefits, they quickly discovered the advantages of moving their home bases or at least part of their operations to 'weak states' that provide safe havens (Schneider, V. & Hyner, D., 2003).

Companies with servers located in those safe havens have on their side learnt the highly attractive force of positioning themselves as offering 'bullet-proof hosting', meaning that they guarantee their clients that their servers will not be closed down even if they receive requests of law-enforcement authorities.

3. Conclusion

New trends in cybercrime are developing all the time, with estimated costs to the global operating economy billions of dollars. In the past, cybercrime was committed mainly by small groups or individuals.
In these days, we see extremely complex cybercrime networks, bringing together individuals from all over the world in real time to commit crimes on a tremendous scale.

The Convention on Cybercrime is the first international treaty on Internet crimes and other computer networks, dealing in particular with copyright infringements, fraud computer, infant pornography, and network security breaches. It also contains a number of skills and procedures, such as computer networks search and legal interception.

The Convention stipulates that its objective is to protect "society against cybercrime" by ensuring that such behaviour is incriminated and that sufficient powers are in place to effectively combat these crimes by facilitating detection, investigation and prosecution at national level, and internationally, and by ensuring swift and reliable international cooperation measures.

References

Council of Europe (2001). ETS No. 185, *Convention on Cybercrime*, Budapest 23 November. In this article, it will be referred to as 'the Cybercrime Convention', 'the Convention', or 'the Treaty'.

Downing, R.W. (2005). Shoring up the Weakest Link: What Lawmakers around the World Need to Consider Developing Comprehensive Laws to Combat', *Columbia Journal of Transnational Law*, Vol. 43, no. 3, p. 711. Terms such as 'cyber-crime', 'computer crime', and 'network crime' have no universally accepted definitions. Part of the confusion arising from their use comes from the fact that criminals now use computers in the course of committing almost any crime. The computer's role in an offence, however, can be characterized in one of three ways: as a tool, as a storage device, or as a victim.

European Council (2002). *Council Framework Decision on the European arrest warrant and the surrender procedures between Member States of the European Union*, 13 June 2002 - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32002F0584

European Council (2005). http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32005F0222 , Council Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems, O.J., 16.03.2005, L 69/67, § 1.

Grabosky, P. (2000). *The Mushroom of Cyber Crime.* Prepared for Presentation at the Symposium on The Rule of Law in the Global Village, Palermo, 14th December, p. 3.

Schneider, V. & Hyner, D. (2003). The Global Governance of Cybercrime: *Issue Space and the Transnational Policy Network*, University of Konstanz, p. 4.
Wall, D.S. (2005). *The Internet as a Conduit for Criminal Activity*, in Pattavina, A., The Criminal Justice System and the Internet, Thousand Oaks, CA: Sage, pp. 77-98, 90.
xxx (2006). Revue Internationale de Droit Pénal. The United States became a party to the Convention on Cybercrime on September 29, Vol. 77.
http://eur-lex.europa.eu/legal content/EN/TXT/?uri=CELEX:52000DC000, COM(2000) 890, Brussels, 26th January 2001, p. 1.