EUROPEAN ACADEMIC RESEARCH
Vol. III, Issue 4/ July 2015

Impact Factor: 3.4546 (UIF)
DRJI Value: 5.9 (B+)

ISSN 2286-4822
www.euacademic.org

Legal Response against Cybercrime in Albania

NERTIL BËRDUFI
Ph.D. Candidate, Lecturer
Law Department, "Hëna e Plotë" (Bedër) University
Albania

Abstract:

As we have entered a new era of computer-based lifestyle, lawmakers have been trying to make essential and considerable changes in the law to make it as compatible as possible with crimes committed by in cyberspace and/or through computer systems. The increasing incidence of criminal activity and the potential emergence of new types of crimes pose great challenges for legal systems and law enforcement. Crimes committed in the online environment exceed national boundaries by becoming more difficult to investigate. As a result, the national and international security threats increase. This article presents a critical analysis of the Albanian jurisdiction to address whether existing laws are sufficient to fight cybercrime and if there are areas for revision.

Key words: Cybercrime, cyberspace, law, jurisdiction.

Introduction

What is Cybercrime? The history of the definitions developed in such a way that computer and cybercrimes can have their own definitions. In the OECD recommendations of 1986 computer-related crime is considered an illegal behavior, unethical or unauthorized with respect to automatic processing and data

transmission.[1] In 1987 Council of Europe recommendations computer-related crimes are described simply as listed and defined deeds in the proposed guidelines or recommendations for national legislators.[2]

In the recommendations of the Council of Europe in 1995 the term "offenses related to Information Technology" is used. In this recommendation, the IT crimes are described as: involving an offense from an investigation which the investigating authorities should obtain information possessed or transmitted in computer systems, or electronic data processing systems.[3] In 2001 the Commission of the European Union 2001 introduced a single definition in which "computer-related crimes are treated in a broad sense as any crime that in some way or another involve the use of information technology"[4]. In the same year Council of Europe Convention on Cybercrime entered into force. This convention separates cybercrime in four different categories: (1) offenses against the confidentiality, integrity and availability of computer data and systems, (2) computer-related offenses, (3) content- related acts; (4) offenses in connection with violations of copyright and related rights.[5]

This list is not limited and allows for expansion in domestic law. Content-related offenses such as breach of copyright, racism, xenophobia, and child pornography, cannot

[1] Computer Related Criminality: Analysis of Legal Politics in the OECD Area, 1986

[2] Recommendations No.R (89) 9, approved by the European Committee of Ministers of the Council of Europe on September 13, 1989 and Report by the European Committee on Crime Problems: Computer-related crime. See http://cm.coe.int/ta/rec/1989/89r9.htm (accessed on 10 May 2015)

[3] Recommendations No.R (95) 13, approved by the European Committee on Crime Problems (CDPC), May29-June 2, 1995: Concerning problems of criminal procedural law connected with information technology: See http://www.cm.coe.int/ (accessed on 10 May 2015)

[4] The European Parliament, the Economic and Social Committee and the Committee of the Regions, January 26, 2001.http://www.europa.eu.int (accessed on 10 May 2015)

[5] Council of Europe Convention on Cybercrime 2001 http://www. conventions.coe.int.Treaty. (accessed on 10 May 2015)

be understood normally as cybercrimes by many observers. Violations of copyright are based on agreements and civil contract and traditionally do not constitute criminal offenses in many countries. Violations of copyright will often apply civil remedies because of numeral complicated issues. Child pornography has always been a criminal offense.

Cybercrimes are crimes that have gone beyond conventionalism and now have threatened the national security of all countries, even in technologically developed countries. Different types of cybercrimes are emerging in the world today, hacking, bombing, diddling, viruses, spoofing and salami attacks are all capable of security breaches in information systems of vital installations. For this reason, legal regulation of these crimes is essential. One of the most important goals of the legislation is to prevent criminal offenses. A potential perpetrator should be given a clear warning that certain criminal acts cannot be tolerated, and when offenses occur, the perpetrators must be punished for the crime committed explicitly and efficiently. These basic principles are also valid for cybercrime. These remedies include an number of anti-cybercrime laws well established for use in the prosecution of cyber criminals and procedural rules governing the collection of facts and evidence in the investigation. Cybercrime is a crime without bourders, offenders can take advantage of gaps in existing legislation to avoid prosecution and punishment. It is therefore important that any legal system should take action to ensure that its laws are sufficient to meet the challenges presented by cybercrime.

The phenomenon of cybercrime

Cybercrime is one of the biggest legal challenges, since from 2000-2014 the Internet has expanded at an average rate of 741.0 % globally and currently about 3 billion people are

online[6]. Cybercrime is a criminal activity involving information technology infrastructure, illegal access, illegal interception (by technical means of non-public transmission of computer data, from or within a computer system), data interference, forgery and electronic fraud.[7] The only difference between conventional crime and cybercrime is the virtual medium. Business, economic and white collars crimes have rapidly been transformed and computers have been used to spread these types of crimes in activities and environments in which they are located. Cyberspace today is one of the biggest legal challenges which has stimulated a different form of crime, creating an environment for new methods of crime. Almost all crimes that can be committed by a person now can be performed by the use of computers.

The reasons of computer weaknesses can be summarized in: a relatively small space for storing data, the easy access, the high possibility of making mistakes due to its complex system, the negligence of humans while giving sensitive information on computers without protecting it, and the difficulty in finding evidence of the crimes in cyberspace.[8]

Some time ago in May 2000, a computer virus known as the "love bug" emerged and spread rapidly around the globe. According to a report, the virus has infected at least 270,000 computers in the first hours after its release.[9] The virus has destroyed files blocking e-mail traffic to more than twenty countries, and some have estimated that the virus caused 10 billion dollars in damages.[10] Security experts have discovered that the virus originated from the Philippines.[11] The

[6]World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (accessed 28 March 2015).
[7] Ibid.
[8]The Unites States Department of Justice www.justice.gov/criminal/cybercrime (accessed on 06 June 2015)
[9]*The Gardian*, Love bug virus creates worldwide chaos, http://www.theguardian.com/world/2000/may/05/jamesmeek, (last accessed 28 April 2015)
[10] Ibid.
[11] Ibid.

investigations of this crime were troubled by the lack of computer crime laws in the Philippines: investigators had found deficiencies trying to get warrants, local prosecutors had to look the statutes and laws of their country more thoroughly in order to find relevant articles to get a warrant.

Even when the suspect Onel de Guzman was arrested, there have been deficiencies in the law because there were no laws to convict him for what he had done.[12] These charges were eventually dropped after the Department of Justice concluded that "there are no laws that apply to what he did in connection with the computer and that investigators have enough evidence to support a conviction for theft."[13] This incident urged Philippines to adopt state law on cybercrime and measures of imprisonment for those who hack the computer systems and/or distribute viruses or other harmful programs,[14] although the since laws cannot be applied Onel de Guzman was not punished. This happening identified the problem of lack of criminal laws for cyberspace and the fact that this is a problem that exceeds national boundaries so an international cooperation was needed for the fight of such crimes. It became clear the importance that states should take measures to implement new laws for criminalizing cybercrimes and that these laws need to be similar through all the states. But most countries still do not have legislation in place to deal with computer related crimes.

The essence of this article provides a critical overview of the provisions that have adopted in Albania for prosecuting and punishing cybercrime offenders and whether such laws are adequate enough to target this kind of crimes.

[12] Ibid.

[13] The New York Times, *Philippines to Drop Charges on E-Mail Virus*, http://www.nytimes.com/2000/08/22/business/technology-philippines-to-drop-charges-on-e-mail-virus.html?ref=topics, (last accessed 28 April 2015)

The case of Albania

After a long period of authoritarian rule and its slow development after emerging from a difficult transition to democracy, Albanian legal framework appears to be in compliance with the Convention on Cybercrime to which it is a state party. Even though there is no specific law on cybercrime in Albania, the legislator has incorporated international norms in the national legislation by amending existing laws and adopting new laws which have developed domestic legislation on the better protection of the citizens and the country from cyber threats. Albania has ratified the Council of Europe's Convention on Cybercrime in 2002. With the growing use of internet by the Albanian society, including its use for criminal purposes such as for pornographic intent, and in order to undertake the obligations required by the Budapest Convention, in 2013 Albanian parliament amended the Criminal Code to include the criminalization of new trends of committing old crimes. For example, currently the amended provision about child pornography criminalizes the production, distribution, advertising, import, sale and publication of pornographic materials in environments where there are children *by any means or form*, and the production, importation, offering, making available, distribution, transmission, use or possession of child pornography, as well as consciously creating access to, by any means or form.[15] The added words "by any means or form" are of crucial importance for the criminalization of new ways of the traditional child pornographic crime. Prosecutors, lawyers and judges can use this provision to criminalize online child pornography and to punish its perpetrators.

However, this amendment cannot be considered as the ideal solution of such an increasing threat as online child

[14] Ibid.

[15] Law no. 144/2013 "For some changes to law no. 7895, date 27.1.1995 "Criminal Code of the Republic of Albania", amended" . 2013. Article 29

pornography. Just the phrase "by any means or form" is not enough considering the rapid spread of online child pornography and the increased threat to children of such a crime. An explicit criminalization of child pornography via the internet is required. Explicitly criminalizing online child pornography would also give this crime the real importance that it has and raise the awareness of such a dangerous threat both to the jurists and to the broad civil society, in the eyes of which this crime often goes neglected.

Criminal Procedural Code describes in a range of articles the methods of collecting the evidence during crime investigation and prosecution.[16] However these methods are general ways of collecting evidence. There is no Article describing how to collect online evidence. Such vague articles leave investigators and prosecutors in a blind alley, when dealing with online crimes. This gap is covered by the international legislation that Albania has ratified and which in such cases can be directly referred to and applied. However this does not justify the vague articles of the national laws and does not imply that there is no necessity of improving them.

The law on Electronic Communication ensures that Internet Service Providers (ISP) and any other communications service provider shall preserve for 2 years subscriber's data for investigation purposes.[17] The procedures of taking these computer data from the investigation authorities are specified in the Criminal Procedural Code. The data can be taken only if they are connected with a specific criminal investigation. Albania has ratified all the three European Conventions "On Extradition", "On Mutual Assistance in Criminal Matters" and "European Convention for the Transfer of Proceedings in Criminal Matters". However, there is a big problem with the Albanian extradition law which impedes the full realization of

[16] Criminal Procedural Code of Republic of Albania 1991, articles 149-226, edition of 2008

[17] Law no. 9918, date 19/05/2008 "On Electronic Communications in the Republic of Albania" s.d. Article 101(1)

international legal standards on extraterritorial legislation. It is the existence of the provision for double criminality, prescribed under Article 6 of the Criminal Code which states that the Albanian Criminal Code applies fully to Albanians who commit crimes within Albania but Albanian nationals who commit crimes abroad can be punished only if the alleged offence is recognized by the jurisdiction of both states, the only exception to double criminality being if the foreign court has given the final sentence.[18] Albanian Criminal Code provides that the extradition of Albanian nationals is possible only if the offence is recognized by both states involved and there is a bilateral agreement for extradition.[19] This provision hinders the punishment of many individuals who commit crimes which are not mutually recognised. For the better protection from cybercrime, Albanian government needs to eradicate the principle of dual criminality when dealing with the extradition of this type of offences since the Albanian criminal law does not cover all the wide range of cybercrime offences.

Recently there has been a significant increase in the internet usage in Albania. The International Telecommunication Union indicates that by the end of 2010 more than 45 percent of Albanian youth had access to the internet. This percentage has increased to 60 at the end of 2013. Despite this, there are no safe internet usage measures in place yet. According to the Electronic and Postal Communication Authority, there is no mechanism to monitor internet content or access to websites from private individuals through registered ISPs in the country, making it harder to identify cybercriminals.

[18] Criminal Code of the Republic of Albania ,1995, Article 6

[19] Government of Albania. Annex to the First, Second, Third and Fourth Periodic Report According to General Guidelines Regarding the Form and Content of Periodic Reports to be submitted by State Parties under Article 44, Paragraph 1/B of The Convention on Human Rights. s.d. available at: http://www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/Albania-Annex-future.doc, (accessed 11 August 2014)

Till in the beginning of 2014 Albania did not have a specialized cybercrime unit in the prosecution office. It had just a Joint Investigation Unit that deals with economic crimes, money laundering, corruption and cybercrime. These units are found in seven main prosecution offices around the country. However there was one Cybercrime Investigation Unit in the Police sector of Tirana. In the Albanian criminal justice system the prosecutor leads and controls the investigations conducted by the state police or other police structures with the authority to investigate, thus also this unit is in close cooperation with the prosecution office of Tirana, by somehow filling the gap of the lack a cybercrime unit inside the prosecution office.

The Cybercrime Investigation Unit is a separate structure inside the Department of Organized Crime and Serious Crimes at the General Police Directorate. It is composed of eight specialists (seven police officers and one IT specialist) and its main function is the investigation of cybercrimes all over the country. Crimes covered by this unit include the provisions of the Criminal Code about unauthorized access to computers, interference in computer data, computer fraud etc., but the Unit also serves for supporting other investigative structures that during investigations are faced with facts and circumstances in the cyber field. This structure's priorities are: 1) the identification and putting before criminal responsibility the individuals or groups who commit criminal activity in this field; 2) Preliminary inspection of computer data stored in computer systems seized in the quality of evidential material and 3) supporting the structures that perform investigations for cases where during investigations are faced with facts and circumstances related to the cyber field.[20] The Sector against Cybercrime now serves as a 24/7 point of contact in line with Budapest Convention.

[20] The sector of Cybercrime Invetigation Unit is created in 8 districts 2014 available at Gazeta Panorama: http://www.panorama.com.al/2014/06/11/krijohet-sektori-i-hetimit-te-krimit-kibernetik-ne-8-qarqe/ (accessed 09 August 2014)

The rapid increase of internet usage in Albania in the recent years started bringing on the surface new risks for Albanian citizens and the government. There have been many crimes committed by cybercriminals, such as unauthorized access to bank accounts, frauds with credit cards, access to governmental websites, etc. which have caused the loss of huge amounts of money. This raised the concern of the new government, and in June 2014 the General Prosecutor of Albania, under the order "For the functioning of the Cybercrime Investigation Unit", announced that The Cybercrime Investigation Unit will now have special structures at eight district prosecution offices, in Tirana, Durres, Korca, Elbasan, Vlora, Shkoder, and Fier, which will deal with the investigation and prosecution of cybercrimes.

For the start of functioning of the special structure at 8 district prosecution offices, a training seminar was organized in Tirana with the help of Police Assistance Mission of the European Community to Albania (PAMECA) mission with Albanian and Italian experts.[21] The concept of cybercrime elaborated by the Albanian Prosecution is based on the Budapest Convention, according to which these crimes include not only acts with computers but also those related to unauthorized access to data, including personal data in social networks and also in the wide technological networks, bank networks etc. This unit will investigate 18 offences.[22] . It is just the beginning and the Unit may not have all the required equipment and experience in the investigation of this crime but it is a new beginning for Albania. Finally more importance will be given to the online activities of individuals, by thus raising the awareness of dangers from the internet to the society and

[21] Ibid.

[22] Crimes that will be investigated by Cybercrime Investigation Unit include: insult, racism, fraud, counterfeiting or unauthorized access, committed through computer or electronic ways, illegal interception of computer data, fraud related to art works, copyrights infringement, pornography, etc. See: http://www.panorama.com.al/2014/06/11/krijohet-sektori-i-hetimit-te-krimit-kibernetik-ne-8-qarqe/(accessed 10 August 2014)

raising the consciousness of the government about cyber threats, bringing these crimes in focus. There has been developed also a manual of guidance for police officers, "Investigation of Electronic Crime and Computer Evidence", which compliance is mandatory because it has the status of a police general order.[23] There exists also a Forensic Laboratory which has sufficient equipment and software to examine computer systems. However, more specialist software is needed for monitoring internet activities, and also more training and specialized staff. Within CyberCrime@IPA, investigators and prosecutors from Albania have participated in several international trainings, and in activities about international cooperation for the investigation and prosecution of cybercrimes. The Head of Sector against Cybercrimes, General Directorate of State Police was funded by the CyberCrime@IPA project to participate in the Master of Sciences (MSc) programme in Forensic Computing and Cybercrime Investigation offered by UCD. [24] Now all police recruits, prosecutors and judges in Albania are given basic training on electronic evidence and advanced training is given to specialist officers of cybercrime.

Conclusions and recommendations

Despite the advantages the rapid development of technology entails, it has also shown to have a dark side. Increased opportunities for criminal behavior through internet may lead to increased national threats. Crimes committed in the online environment exceed national boundaries, becoming more difficult to investigate. As a result, the national and international security threats increase.

[23] "CyberCrime@IPA Assessment Report Criminal justice capacities on cybercrime and electronic evidence in South-eastern Europe." Strasbourg, 2013. pg 19

[24] "CyberCrime@IPA Assessment Report Criminal justice capacities on cybercrime and electronic evidence in South-eastern Europe." Strasbourg, 2013. pg 19-21

The results of this analysis showed that the legislation of Albania is in compliance with European standards and international conventions. Albania has signed and ratified all the international conventions which cover the protection from cybercrimes. But, despite this fact, the Albanian legislation still needs to be amended to be fully compliant with the ratified conventions and to provide the necessary flexibility for the prohibition and prosecution of such dynamic crimes. The government should increase collaboration with ISPs and should increase the number of awareness raising campaigns about the dangers of internet and online safety.

Albania has always been more preoccupied with urging matters such as poverty, political instability, and traditional crimes such as rape, murder and theft, and the fight against cybercrime has been lagging behind. But, recently there has been a turning point and Albanian government has started paying more attention to the criminal activity in the cyberspace by implementing new provisions and taking new measures of protection.

Despite this, the majority of the law enforcement personnel are not equipped with the necessary technological knowledge, while cyber criminals are experts in computer technology. In combating these crimes there is a need for educating and developing human resources, which is one of the most reliable strategies. In addition to this, universities, schools of higher education and academic institutions should set up special courses designed to allow the next generation of judges and lawyers to become skilled in what is a difficult area, but very profitable.

BIBLIOGRAPHY

Criminal Procedural Code of Republic of Albania (1995) edition of 2008.

Computer Related Criminality: Analysis of Legal Politics in the OECD Area (1986).

Convention on Cybercrime 2001

"CyberCrime@IPA Assessment Report Criminal justice capacities on cybercrime and electronic evidence in South-eastern Europe." Strasbourg, 2013

Internet Library of law and Court Decisions, http://www.internetlibrary.com/alldecisions.cfm.case33.

Government of Albania. Annex to the First, Second, Third and Fourth Periodic Report According to General Guidelines Regarding the Form and Content of Periodic Reports to be submitted by State Parties under Article 44, Paragraph 1/B of The Convention on Human Rights. s.d. available at: http://www2.ohchr.org/english/bodies/crc/docs/AdvanceVersions/Albania-Annex-future.doc, (accessed 11 August 2014)

H.L.A Hart, The concept of law, Claredon Law Series, 1961

Lacey, Nicola: (2007) H.L.A. Hart's Rule of Law; The Limits of Philosophy in historical Perspective. 36. pp 1203-1224.

Law no. 144/2013 "For some changes to law no. 7895, date 27.1.1995 "Criminal Code of the Republic of Albania", amended". 2013

Law no. 9918, date 19/05/2008 "On Electronic Communications in the Republic of Albania"

Recommendation No. R (95) 13 [1995] of Council of Europe, Concerning Problems of Criminal Procedural Law connected with Information Technology, adopted by the Committee of Ministers on September 11.

Recommendation Nr (89) 9, of the Council of Europe on September 13 1989 and Report by the European Committee on Crime Problems: Computer-related crime. See http:// cm.coe.int/ta/rec/1989/89r9.htm.

Recommendation Nr (95) 13, adopted by the European Committee on Crime Problems (CDPC) at its 44th plenary session May29-June 2, 1995

The European Parliament, the Economic and Social Committee and the Committee of the Regions. http://www.europa.eu.int. (accessed 1 April 2014)

Vanguard Paper, Crime Alert, 2010.

Web Sites

Council of Europe Treaty Office <http://www.conventions.coe.int> (accessed 30 March 2015).

Cybercrime Law, International Think Tank On Justice, Peace And Security In Cyberspace <www.cybercrimelaw.net> (accessed 25 March 2014).

Electronic Privacy Information Center, Revised U.S. Encryption Export Control Regulations, January 2000, available at: https://epic.org/crypto/export_controls/regs_1_00.html (accessed 28April 2015)

The Gardian , Love bug virus creates worldwide chaos, http://www.theguardian.com/world/2000/may/05/jamesmeek, (last accessed 28 April 2015)

Philippines to Drop Charges on E-Mail Virus, The New York Times: http://www.nytimes.com/2000/08/22/business/technology-philippines-to-drop-charges-on-e-mail-virus.html?ref=topics, (last accessed 28 April 2015)

Privacy International Organization <www.privacyinternational.org> (accessed 30 March 2014).

The FBI Federal Bureau of Investigation <www.fbi.gov> (accessed 25 March 2014).

The sector of Cybercrime Invetigation Unit is created in 8 districts 2014 available at Gazeta Panorama: http://www.panorama.com.al/2014/06/11/krijohet-sektori-i-hetimit-te-krimit-kibernetik-ne-8-qarqe/ (accessed 09 August 2014)

The Unites States Department of Justice www.justice.gov/criminal/cybercrime (accessed 28 March 2014)

World Internet Usage and Population Statistics, http://www.internetworldstats.com/stats.htm (accessed 28 March 2015).

World Socialist Website <www.wsws.org> (accessed 28 March 2014).