EUROPEAN ACADEMIC RESEARCH
Vol. IX, Issue 2/ May 2021

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

ISSN 2286-4822
www.euacademic.org

Cybercrime and Victimization in Computer Networks

ANDI PËRMETI
University of Tirana, Albania

Abstract

Cybercrime is today one of the biggest legal challenges and problems for the Republic of Albania as well as internationally. The Internet has become widespread in our country, being present everywhere. Cyberspace today is one of the biggest legal problems that Albania is facing and an international challenge for all waiting for an effective solution.

In the last two decades, cybercrime has emerged as a prominent "injury" area for criminologists and as a growing public safety concern. Although there are many terms that define cybercrime, this term generally refers to crimes committed by the use of computer and computer network, but also includes crimes that are not limited to the computer. Ongoing research has uncovered the nature and prevalence of cybercrime, in correlation with victimization insults and issues related to the investigation and punishment of this type of crime.

Online victimization is a new term, recently used by the science of Victimology because of technological development. The whole society should be educated for its prevention and educational, normative and punitive measures should be taken for the perpetrators who commit criminal offenses; but also victims or entities that may be subject to victimization in the future should be informed of the responsibility they have, especially during the actions they perform through electronic means and the Internet.

This paper aims to address a number of issues of online victimization as a new field of crime in Albania and beyond.

Keywords: Cybercrime, Crime, Online Victimization

1. CYBERCRIME IN THE REPUBLIC OF ALBANIA

Albania is one of the signatories of the Convention on Cybercrime. It has ratified this convention by Law no. 8888, dated 25.04.2002 "On the Ratification of the Convention on Cybercrime". Meanwhile, the implementation of the convention in the domestic legislation of the Republic of Albania dates back to January 2008. The main steps in the implementation of the Convention, in the domestic legislation have been made with the approval of the Law no 10023, dated 27.11.2008. Criminal justice lawmakers, given the special characteristics of cybercrime in relation to the aspect of jurisdiction, made the necessary changes to Article 7 of the Criminal Code. This law included a series of criminal offenses in the field of computer in the Criminal Code. These changes were followed by some changes in the Code of Criminal Procedure, providing some procedural moments such as the obligation to submit computer data, computer data seizure, accelerated storage and partial detection of computer data.[1]

Implement these legal changes [2] aims to prevent and investigate criminal activities in the field of information technology and, to achieve this goal, a development in special structures of the police force, courts and prosecutor's offices is required, in order to be able to respond with the appropriate expertise to all relevant issues.

I think it is very important that crime prevention and investigation bodies understand how any type of computer crime can be committed and also that they are equipped with the necessary technological tools to investigate and fight crime. This is because I think that the existence of comprehensive legislation that ensures a detailed breakdown of specific types of cybercrime is not the only adequate solution to this problem.

2. JURISDICTION AND SOVEREIGNTY IN CYBERSPACE

A global system of interconnected computer networks is called the Internet. The Internet can neither be defined by a beginning nor can it be concluded by an end, as the internet is like a super giant spider web made up of cables, optical fiber or various satellite waves. The Internet

[1] Cyber Crime in Albania "A statement of law, policy and practice" Bledar Abdurrahmani
[2] Bledar Abdurrahmani, Cyber Crime in Albania "A statement of law, policy and practice", Durrës, 2013

as a notion differs from legal concepts related to territorial space. Internet is an invisible and intangible virtual space, composed of electronic pulses, which mediate computers around the world interact among them. Internet is nobody's property and no one can control it, as anyone can access it without the need for any kind of document, thus crossing the traditional state borders.

Although all this infinite virtual space is not owned by anyone and no state controls it, it still happens that the laws of one state interact with the laws of another state, thus often violating each other's sovereignty. Jurisdiction in cyberspace is a very big problem both for the courts of different states and for the states themselves. The number of legislations that can be applied in the case of a civil or criminal violation in cyberspace is indefinable.

Jurisdiction in cyberspace is subject to all principles of international law. The starting point for state jurisdiction and international cooperation is sovereignty. The sovereign equality[3] of states is protected by rules of customary public international law. These include the obligation on states not to interfere in any form or for any reason whatsoever in the internal and external affairs of other States. Law enforcement and criminal justice matters fall within this exclusive domain of the sovereign state, with the result that, traditionally, criminal jurisdiction has been linked to geographical territory.[4]

States must therefore refrain from bringing pressure to bear on other states regarding the behaviour of specific national bodies, such as law enforcement agencies or the judiciary.[5] Persons may not be arrested, a summons may not be served, and police or tax investigations may not be mounted on the territory of another state, except under the terms of a treaty or other consent given. Of course, not all crimes occur 'neatly' within the territorial jurisdiction and, where this is the case,

[3] Comprehensive Study on Cybercrime (Draft-February 2013, of United Nations Office of Drugs and Crime).

[4] As such, states have a right to sovereignty and territorial integrity, and to freely determine their own political, economic, cultural and social system, including all matters, essentially within the foreign jurisdiction. See Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, annex to GA resolution A/RES/20/2131 (XX), 21 December 1965

[5] Cassese A, International Law, p. 53

international law has come to recognize a number of bases of extra-territorial jurisdiction in criminal matters.[6]

3. DEFINITION AND ACTIONS THAT CONSTITUTE ONLINE STALKING

Cyberstalking or known in Albanian as online stalking may be defined as the use of the Internet or other electronic means to stalk or harass an individual, which may be a natural or legal person. Cyberstalking may include false accusations, defamation, slander, libel, various monitoring such as identity and personal data theft, threats, vandalism, solicitation for sex, or gathering information that may be used to threaten or harass. These actions are often accompanied by real-time (physical) stalking, or otherwise known as "offline" stalking.

Both forms of stalking (whether online or offline) may be criminal offenses, motivated by a desire to control, intimidate, or exert pressure or influence on a subject. The person committing these acts (perpetrator) may be a person known or not to the victim. He may be anonymous and also require the involvement of other people via the internet, to take part in such illegal actions even when the latter may not know the target at all.

Technology ethics professor Lambèr Royakkers defines cyberstalking as perpetrated by someone without a current relationship with the victim. About the abusive effects of cyberstalking, he writes, "Stalking is a form of mental assault, in which the perpetrator repeatedly, unwantedly, and disruptively breaks into the life-world of the victim, with whom he has no relationship (or no longer has), with motives that are directly or indirectly traceable to the affective sphere. Moreover, the separated acts that make up the intrusion cannot by themselves cause the mental abuse, but do taken together (cumulative effect)." [7]

We talk about cyber-stalking as a criminal offense related to the commission of various actions or omissions committed on the network and by means of information technology, therefore, in order not to have a confusion in the well-defined term, it is important to

[6] Jeschek, H.H., Weigend, T.,1996 "Lehrbuch des Strafrechts.Allgemeiner Tei" l, Berlin: Duncker&Humbold, p. 167

[7] "THE DUTCH APPROACH TO STALKING LAWS", Lambèr Royakkers, CALIFORNIA CRIMINAL LAW REVIEW VOLUME 3: October, 2000, pg 1

distinguish between cyberstalking and other actions carried out over the internet, which may or may not constitute a criminal offense. Research has shown that actions that can be perceived to be harmless can be considered to be trolling [8], whereas if it is part of a persistent campaign then it can be considered stalking.

Cyberstalking author Alexis Moore separates cyberstalking from identity theft, which is financially motivated.[9] Taking into consideration the different definitions given to cyberstalking and also the practice followed by various authors, we can identify a non-exhaustive list of actions or omissions involving cyberstalking, where we can mention the following:

- False accusations: Cyberstalkers try to damage the reputation, dignity and personality of their victim(s) and turn other people against them.
- Attempts to gather information about the victim: Cyberstalkers may approach their victim's friends, family and work colleagues to obtain personal information. They may advertise for information on the Internet, or hire a private detective to obtain this information.
- Monitoring their target's online activities and attempting to trace their IP address in an effort to gather more information about their victims or their objectives.
- Encouraging others to harass the victim
- False victimization
- Attacks on data and equipment: Cyberstalkers may try to damage the victim's computer or the data contained in it or other electronic means, as in this way they achieve their goal of harming the victim(s).
- Ordering goods and services in the victim's name, making various subscriptions using the personal data of the victim, which can be fatal in certain cases.
- Arranging meetings, related to cases where cyberstalkers ask their victims to meet them, thus creating not only a risk of being a victim of online stalking, but also advancing to physical stalking or more.

[8] In Albanian it can be adapted to the term sending / receiving abusive messages that are transmitted through the electronic network and information technology tools)
[9] https://www.theepochtimes.com/back-off-surviving-and-combating-stalking-and-cyberstalking_2932790.html

- The posting of defamatory, offensive or derogatory statements and information.

Types of online stalking

Online stalking may start from mutual or one-way communication via computer or other electronic means by known or unknown persons. Online stalking occurs in various forms and some of these types can be divided into several groups, which should be noted that do not constitute an exhaustive list. Some of the types of online stalking are:

- Stalking by strangers
- Gender-based stalking
- Cyberstalking of intimate partners (of a current or former romantic partner)
- Cyberstalking of celebrities and public persons
- Cyberstalking By anonymous online mobs
- Corporate cyberstalking

Perpetrators' Profiles

Mental profiling of digital criminals has identified psychological and social factors that motivate stalkers as envy; pathological obsession (professional or sexual); unemployment or failure with own job or life; intention to intimidate and cause others to feel inferior. The stalker is delusional and believes he/she "knows" the target; the stalker wants to instill fear in a person to justify his/her status; belief they can get away with it (anonymity); intimidation for financial advantage or business competition; revenge over perceived or imagined rejection, etc. Cyberstalkers find their victims by using search engines, online forums, bulletin and discussion boards, chat rooms, social networking sites such as Myspace, Facebook, Bebo, Friendster, Twitter, Instagram and Indymedia, a media outlet known for self-publishing. They may engage in live chat harassment or flaming or they may send electronic viruses or instant messages and unsolicited e-mails (spams). Cyberstalkers may research individuals to feed their obsessions and curiosity. The acts of cyberstalkers may become more intense, such as repeatedly instant messaging their targets. More commonly, they will post defamatory or derogatory statements about their stalking target on web pages, message boards, and in guest books designed to get a reaction or response from their victim (respond to these messages) thereby initiating contact. In some cases, they have

been known to create fake addresses, sites, and blogs in the name of the victim containing defamatory or pornographic content.

Once they get a reaction from the victim, that is where their game begins, as they will typically attempt to track or follow the victim's internet activity and the victim's reaction allows such an opportunity. Classic cyberstalking behavior includes the tracing of the victim's IP address in an attempt to track their personal information, from their home address to blood type or bank accounts. Some cyberstalking situations do evolve into physical stalking, and a victim may experience abusive and excessive phone calls, vandalism, threatening or obscene mail, trespassing, and physical assault. Moreover, many physical stalkers will use cyberstalking (the internet and information technology tools) as a new method of harassing their victims.

Preliminary work by Leroy McFarlane and Paul Bocij has identified four types of cyberstalkers: the vindictive cyberstalkers, the composed cyberstalkers, the intimate cyberstalkers and collective cyberstalkers.[10]

a) Vindictive cyberstalker

The vindictive cyberstalkers noted for the ferocity of their attacks on the victim. They threatened their victims more than any other group and in the majority of cases, they actually stalked their target offline (physically). According to the study done by Bojic and Mcfarlane, a third of the perpetrators were known to have had a previous criminal record, and two-thirds were known to have victimised others before.

b) Composed cyberstalker

The composed cyberstalker is so named because it is theorized that their actions/omissions are aimed at causing constant annoyance and irritation to their victims.

c) Intimate cyberstalker

This group tried to win the feelings and gain the attention of their target. They also demonstrated detailed knowledge about victims. It was noted that the nature of their communication was much more intimate and smart than the other sub-groups, but when they were rebuffed, their messages were more threatening.

d) Collective cyberstalkers

This final group is characterised by two or more individuals pursuing victims via information technology tools. These types of perpetrators

[10] https://journals.uic.edu/ojs/index.php/fm/article/view/1076/996

were organized in online groups and had their own target group, which they would pursue and harass through the electronic network. Such perpetrators used much more sophisticated ways to persecute and threaten their victims. Another feature is that these perpetrators act in a coordinated manner with each other and plan their actions in persecution of the victim(s). According to Antonio Chacón Medina, author of "A new face of the Internet: stalking.

5. REGULATION OF ONLINE HARASSMENT/STALKING ACCORDING TO THE CRIMINAL LEGISLATION OF THE REPUBLIC OF ALBANIA

Albanian legislation in recent years has tried to regulate the issue of cyberstalking, by adopting several provisions, which condemn the various actions that constitute harassment, stalking and online molestation. There are some criminal offenses according to the Criminal Code of the Republic of Albania and if we analyze the structure of the criminal offense, we notice that in some specific parts, they aim to protect against cyber-stalking, since the Albanian legislation does not have specifically regulate this type of criminal offense, including in the provisions that we will analyze below. The Albanian Criminal Code has 4 provisions, which play an important role in regulating cyber-stalking. However, there are also other supporting provisions, which indirectly provide protection against cyber-stalking. These provisions will be analysed as follows:

A. Shameful acts

Paragraph IV of this provisions states that: "The proposal made by an adult person, by any means or form, to meet with a minor who has not reached the age of fourteen or a minor who is not sexually mature yet, with the aim of committing any of the criminal offences foreseen in this Section or in Section VIII, Chapter II of this Code, shall constitute a criminal offence and is punishable with one to five years of imprisonment."[11]

Some characteristics of this phenomenon are as follows: The object of this crime are the legal relations established to protect the normal sexual development and moral formation of minors, who have not reached the age of 14 or have not reached sexual maturity

[11] Article 108, Criminal Code of the Republic of Albania

Objectively, shameful acts are committed with active shameful physical or immoral acts against minors (provision in general). By shameful acts mean those ways of satisfying sexual lust, which do not contain the elements of any other sexual crime. In theory, shameful acts can be with physical actions, as well as with conversations, advice, pornographic images, etc., that push the minor to start premature sexual intercourse. The crime is deemed committed at the moment that the above action is committed. Another form of crime is involvement as a witness in acts of a sexual nature committed above. Another form of this criminal offense is, according to the fourth paragraph mentioned above, and the phrase "by any means or form" includes a wide range of proposals through various electronic means and the Internet. For example, the adult calls the minor on the phone, sends him/her messages or communicates on social networks, etc. to meet the latter in order to satisfy his sexual lust. The subject of this crime can be any person who has reached the age of 14 and is responsible. This crime can only be committed with direct intentions.

B. Sexual harassment

This offense in itself is comprehensive, even for online harassment, because if we analyze the nature of the latter, we come to this conclusion. "Commitment of actions of a sexual nature which infringe the dignity of a person, by any means or form, by creating a threatening, hostile, degrading, humiliating or offensive environment, shall constitute a criminal offence and is punishable with one to five years of imprisonment."[12]

Some characteristics of this crime are: The object of the crime are the legal relations established to ensure the inviolability of the morality and dignity of the person, female or male, specially protected by the criminal legislation from committing sexual behaviors, criminal acts. Objectively, the crime is committed by sexual behavior or by any means or form (phrase which includes the commission of this act by electronic means and through the Internet), creating an environment that is threatening, hostile, degrading, humiliating or offensive to the dignity of the person. This offense is committed by sexual harassment without the need for other consequences. The subject of this crime is any person who has reached the age of criminal responsibility and is

[12] Article 108/a , Criminal Code of the Republic of Albania

responsible. This act is committed intentionally and with the intention of fulfilling sexual lust.

C. Stalking

This is a provision, the content of which we note does not include stalking that occurs online, but that theoretically leaves room for this type of stalking as well. However, it is necessary to review According to this provision "Intimidation or harassment of a person through repetitive actions, with the intent to cause a state of constant and severe anxiety to or fear for personal safety, of a relative or person with whom that person has a spiritual connection, or to force him or her to change his or her way of living, shall be punished by imprisonment of six months to four years."[13]

Some characteristics of this criminal offense are as follows: Legal relations are the object of the criminal offense, they are important and are established to ensure the inviolability of a person (relatives, spouse, ex-spouse, ex-cohabitant, minor, pregnant woman or a person incapable of defending themselves), specifically protected by criminal legislation from criminal acts. Objectively, the offense is committed with repeated active actions that appear in ways of threatening or harassing the person. A necessary element of the criminal offense is that the actions are repeated and criminal consequences are required, such as causing a constant and severe state of anxiety or fear for personal safety or forcing that person to change his/her lifestyle, etc. Every person who has reached the age of criminal responsibility and is responsible is subject to the aforementioned consequences. This act is committed intentionally, based on weak motives and with the intention of causing insecurity, anxiety to the injured party.

D. Pornography[14]

According to this article, this criminal offense has as its object the legal relations established to protect the norms of social morality in relation to children, which are protected by criminal legislation, by criminal acts/omissions, which lead to the moral depravity of minors. Objectively, this criminal offense is committed in several forms according to the provision which are as follows: Production, distribution, advertisement, export, import, sale, and publication of

[13] Article 122/a Criminal Code of the Republic of Albania
[14] Article 117, Criminal Code of the Republic of Albania

pornographic materials, which are published on printings with typewriters, linotype, photography, drawings, etc. Also through production, import, offering, making available, distribution, broadcasting, use, or possession of pornography. The latter includes recruitment, exploitation, compulsion, or the persuasion of a child to participate in pornographic shows. Subject of the criminal offense may be any person who produces, advertises, imports, sells, registers, distributes or uses any means and form for the dissemination of pornographic materials involving children. What remains problematic is the question of who will be considered a child: A person under the age of 18 under the Convention on Cybercrime or a person up to the age of 14? This remains a matter of doctrine for discussion. Subject of the crime are also those persons who use the minors to commit this criminal offense. This act is committed intentionally.

Other provisions, which indirectly protect the subjects from cyber-stalking (according to the different definitions given to this term), sanctioned in the criminal code are:

- Threat due to racist and xenophobic motives through the computer system [15]
- Dissemination of racist or xenophobic materials through the computer system [16]
- Insulting due to racist or xenophobic motives through the computer system [17]
- Unauthorized computer interference [18]
- Unlawful wiring of computer data [19]
- Interference in computer data [20]
- Interference in computer systems [21]
- Misuse of equipment [22]

CONCLUSIONS

In the last two decades, cybercrime has emerged as a prominent "risky" area for criminologists and as a growing public safety concern.

[15] Article 84 / a, Criminal Code of the Republic of Albania
[16] Article 119 / a, Criminal Code of the Republic of Albania
[17] Article 119 / b, Criminal Code of the Republic of Albania
[18] Article 192 / b, Criminal Code of the Republic of Albania
[19] Article 293/a, Criminal Code of the Republic of Albania
[20] Article 293/b, Criminal Code of the Republic of Albania
[21] Article 293/c, Criminal Code of the Republic of Albania
[22] Article 293/ç, Criminal Code of the Republic of Albania

Although there are many terms that define cybercrime, this term generally refers to crimes committed by the use of computer and computer network, but also includes crimes that are not primarily computer-based. Ongoing research has uncovered the nature and prevalence of cybercrime, correlations of insults and victimization, and issues related to the investigation and punishment of this type of crime. Despite numerous studies and research on cybercrime, only a few studies have analyzed the theoretical causes and correlations of cybercrime victimization.

The conclusions that come from the studies, underline the importance of individual and situational factors in terms of online victimization. However, if both these factors, individual and situational, predict all types of cybercrime, online victimization remains equally incomprehensible. Assessing the role played by individual and situational factors in different forms of victimization by cybercrime will be related not only to the development of the theoretical structure of online victimization, but also to the advancement of the victimology scholarship by providing information on specific issues of public safety.

Victimization is the process of being victimized. Online victimization is a new term, recently used by the science of victimology as a result of technological development. Online victimization can be defined as the process by which a particular entity becomes victim to criminal offenses committed through computers and the Internet in cyberspace. Online victimization, in recent years has taken on a very large scale turning into a worrying problem, not only social but also legal.

Stalking/online harassment is one of the most prevalent criminal offenses since the beginning of the development of information technology. Also because the use of electronic devices and networks is not fully regulated in legal ways, criminals have been offered a new "legal" space to commit their crimes. Legislation against stalking/online harassment varies from country to country.

Albanian legislation in recent years has tried to regulate the issue of cyberstalking, by adopting several provisions, which condemn the various actions that constitute molestation, stalking and online harassment. There are some criminal offenses, according to the Criminal Code of the Republic of Albania, which if we analyze the nature of the criminal offense we notice that in some specific parts, they

aim to protect against cyber-stalking. However, since this type of criminal offense is not specifically regulated in the Albanian legislation, it is included in the provisions that we will analyze below. The Albanian Criminal Code has 4 provisions, which are more important in regulating cyber-stalking, but there are also other supporting provisions, which indirectly provide protection against cyber-stalking. These provisions are: Shameful acts, pornography, sexual harassment and stalking.

Therefore, in conclusion, we must say that in order to prevent online victimization, the whole society should be educated and educational, normative and punitive measures should be taken for perpetrators of criminal offenses. While victims or subjects that may be subject to victimization in the future should be informed of the responsibility they have, especially during the actions they perform through electronic means and the Internet. It is very important from the criminal-legal aspect, to know the resistance of the victim against the perpetrator of the criminal offense, because this also affects the classification of the offense and the imposition of the final sentence on the perpetrator.

REFERENCES

1. Constitution of the Republic of Albania
2. Criminal Code of the Republic of Albania, updated in 2017
3. Law no 8888, dated 25.04.2002 "On the Ratification of the Convention on Cybercrime".
4. Law No. 10023, dated 27.11.2008
5. Alexis Moore, What is cyberstalking, published on February 2017
6. Anne Wells Bransccons, Anonymity, autonomy and accountability: Challenges to the first amendment in cyberspaces, Yale.L.J., 2010
7. Antonio Chacon Medina, Una nueva cara de internet: El acoso, Universidad de Granada, 2003
8. Barnes, L.H., Teeters, K.H., New horizons in Criminology, New York, 1945
9. Faw.T. Ngo, Raymond Paternoster, Cybercrime victimization: An examination of individual and situational factors, Journal of Cyber Criminology, 2011
10. High-tech stalking, Law Enforcement Technology, 2005
11. Jai Shankur, The study of causation of crimes that occur in the cyberspace and its impact in the physical space, Chennai, 2007
12. John.E, Bash the stock bashers, Florida, 2010
13. M.Alexis Kennedy and Melanie.A. Taylor, Online harassment and victimization of college students, Las Vegas, 2010

14. Maria Koeppel, Molly Smith and Leana.A. Bouffard, Dating safety and victimization in traditional and online relationships, Sam Houston State University, 2016
15. Mathew Lafferman, Do facebook and Twitter make you a public person? How to apply the Gertz Public Figure Doctrine to Social Media? Santa Clara High Technology Law Journal, 2012
16. Prof. Dr. Vasilika Hysi, Introduction to Criminology, Tirana, 2010
17. R. Smathews, S. Aghill, D. Lindsky, A study of doxing its security implications and mitigation strategies for organizations, Canada, 2013
18. Ramljak A. Alija, Halilovic Haris, Viktimologija, Fakultet Kriminalistickh Naukau Sarajevu, 2004
19. Zvonimir Separovic, Vitimologija-studija zvtvama informatory, Fakultet Kriminalistickh Sarajevu, 2006
20. Nertil Bwrdufi, Cybercrime, strategy and national security, Dissertation, Tiranw, 2015
21. Online victimization of youth, Youth Internet Safety Survey 1-2, 2008-2014
22. Paul Bojic, An exploration of predatory behavior in cyberspace: Towards a typology of cyberstalkers, Aston University, 2003
23. Paul Bojic, Cyberstalking: Harassment in the internet age and how to protect your 1.