ABSTRACT

Due to technological developments, cybercrime techniques evolve day by day. Nowadays, innocent users have been the target of cybercriminals who want to make money or extort sexual favor in the context of sextortion crime. This paper discusses the definition of sextortion with the techniques used by the criminals, legal framework of aforementioned crime in Turkey and discusses how to prevent and solve past crimes.

Keywords: cyber sextortion, cyber sexual extortion, online sexual exploitation, nonconsensual pornography, sexual blackmail

1. INTRODUCTION

The Internet’s under-regulated form drives a transformative level of global connectivity and communication by compressing time, place and distance (Llinares and Johnston, 2018). The Internet also has created a new social environment where individuals can engage in a range of virtual social relationships (CCRI, 2017). According to these evolution, the techniques used by the traffickers are constantly being updated with new methods of exploitation. The risk of online victimization by having negative sexual experience is known as one of the biggest problem against human rights. In this context, “sextortion”, which is a new form of online sexual violence, exists all over the world.

2. SEXTORTION

2.1. Definition of Sextortion

Sextortion is used as a method to threaten someone by exposing sexual images or sexually explicit images. Victims are threatened to share more sexual or nude images, perform sexual acts or paid money by doing so (Wolak and Finkelhor, 2016). In other words, sextortion
is a term which describes a term that the nonconsensual, malicious or criminally motivated distribution of sexual images via digital media. A sexual image constitutes of a picture or video (real or fake) that displays a person nude, partially clothed or in a sexual pose (Wolak et al., 2018).

In order to accept sextortion as a new cybercrime, being able to analyze this crime with all its dynamics is important.

Sextortion crime has two contexts in critics. Firstly, perpetrators acquire sexual images from victims whom they meet online by using fake profiles or hacked computers (Federal Bureau of Investigation: Sextortion, 2015). According to data, perpetrators acquire nude images of respondents without their consent in the 45% of cases (Wolak and Finkelhor, 2016). Another sextortion occurs with dating violence (Wolak and Finkelhor, 2016). Teen dating violence has been on the rise when analyzing crime trends. According to the survey conducted amongst 3,745 middle aged and high school students, 15% of girls and 7% of boys are pressured to send sexual photos by their partners. In the case of refusal, partner is threatened to share their sexual photos online as well as conducting unwanted communication (Zweig et al., 2013). Another important result is, especially girls are reported to feel coerced by their partners to send nude images and have more negative consequences such as exposure of images and harassment for sexting (Ringrose J. et al., 2012). There is a difference between sexting and sextortion. Sexting is an action with the consent of all parties involved while sextortion is not (Humelnicu I.V., 2016). According to the 2016 National Strategy survey, sextortion has been emphasized as the most significantly growing threat to children. In addition to that, in 2016 report by the U.S. Department of Justice, sextortion is the most significantly increasing type of online child exploitation that based on more than 1,000 law enforcement respondent of law enforcement investigators (National Strategy on Child Exploitation Prevention and Interdiction, 2016).

Victims may be adults as well as adolescents (National Intimate Partner and Sexual Violence Survey, 2011). In order to meet their victims for online grooming, criminals create fake accounts on social media depending on the context of target victim. After the criminals gain victims’ trust by building a relationship, they start sextortion.

2.2. Techniques used by the Criminals

Sextortion is also defined as social engineering which is the most common intrusion technique. Cybercriminals trick victims into granting access to their personal data. Criminals often use phishing which is requesting confidential information over the internet by deceiving users into accessing malware with a malicious email with an attachment. When this malware is installed on victims’ computers, it encrypts their crucial private data and offers to help fixing of the problem after payment of a recovery or decryption service fee has been made (R. Broadhursy, 2017). Criminals also persuade the victims to install a program which turns out to be a Trojan horse and by doing that Trojan horse installs a malware which gains access to victims’ web cameras so that it can record film/photos without them noticing (Humelnicu I.V., 2016). Especially some of the malicious software which provides access to all files and documents typed on keyboards, is specifically designed to be undetectable by-antivirus programs. Criminals tend to manipulate victims’ social media behavior by catfishing which is using a fake identity on a social network, is more effective in many of cases (Wittes, et al., 2016).

Techniques are changing by day. In a case, the hacker followed up his/her sextortion with different email accounts. According to the court records of criminal prosecution, it was elicited that the hacker used 30 different screen names to avoid detection, however, they were all from the same IP address. Many of victims keep detailed files and gathered information for more than
We may say the internet is the most common platform for this crime. Due to the high sexting rates, recording and sharing pornographic images of themselves and not using strong passwords or two-step verification, the easiest of cybersecurity targets is the average teenage or young-adult Internet user (Wittes, et al., 2016).

According to the predictive policing of many law enforcements to find new opportunities against crime, The Gendarmerie Nationale in France carried out through the concept of criminal intelligence with opening the use of artificial intelligence. In order to prevent this crime, or resolve past crimes, an application of anticipative policing is using mathematical techniques in order to identify potential targets. In the field of crime analysis, these applications will be used for to profiling criminals based on massive data, to model criminals’ behavior, criminal and investigator way of reasoning (Perrot, 2018). In order to prevent sextortion and resolve past sextortion cases, these artificial intelligence applications might be used by law enforcement when analyzing sextortion crime trends such as using some malwares that grants access to personal data by criminals. Nevertheless, it is crucial to state that these applications may cause a risk for privacy and have critics about them being biased.

2.3. Impact on Victims

Victims have described feeling like a slave during the sextortion and living with the anxiety of public exposure by the hackers. In addition to that, they do not feel any safer as long as having an Internet connection. Besides these, the victims can inflict self-harm and even commit suicide. The majority of victims cannot talk to anyone about the crime and seek help.

Child victims who are the easiest targets of crime are terrified by the potential social repercussions of sextortion. They are worried of losing friends and becoming the target of teenage bullying (Wittes, et al., 2016).

3. Sextortion Law and Legal Definition

3.1. Legal Definition of Sextortion

Sextortion is not legally defined as a crime in most countries. The prosecutions for sextortion often relies on other criminal statutes such as child pornography, harassment, extortion, as well as stalking, hacking and violating personal privacy. Upon examining recent cases, Brookings Institution indicates that new laws are needed in order to specifically target this crime (Wittes, et al., 2016).

The crime, which is at the core of the intersection of cybersecurity and sexual coercion is a form of extortion and/or blackmail crimes with different forms and statutes. Moreover, it is important not to confuse this crime with consensual sexting or online flirtations. In addition, sextortion cases are prosecuted under child pornography laws, as computer intrusions; as stalking or as extortions according to cause of sextortion do not exist in federal or state law (Wittes, et al., 2016). This means that, there is an international necessity to define sextortion as a crime in legislations.

Susan Brenner defines sextortion as a “cyber sexual extortion” and states that extortion statutes wherein the target’s property presumed to have value in financial sense may present difficulties for prosecutors. Brenner also suggests adopting new sextortion specific statutes or
revising existing extortion statutes for encompassing the harm of sextortion cases (Brenner, 2012).

3.2. Legal Framework of Countries

In France, however sextortion is not a specific legal concept in their legal system, the illicit extortion of sexual favors is punished by both civil and criminal laws. There are sexual assault, extortion, blackmail and corruption defined in their Criminal Code. France also has connected sextortion crime to gender-based violence protection, helping women with plans such as deploying online communication programs, and reducing gender-based violence with their 2016-dated interdepartmental plan (UIA-IROL, 2017).

In Hungary, sextortion is not regulated specifically either. According to the Hungarian Criminal Code, there is a sexual exploitation definition which is forcing someone to perform or tolerate sexual activities by threatening. The 2013 Amendments define sexual blackmailling and sexual extortion and include a punishment by longer imprisonment than simple exploitation. The gender-based violence, such as human trafficking and domestic violence are problems in Hungary but the country criminalizes trafficking in their criminal code with respect to EU regulations which are signed (UIA-IROL, 2017).

In addition, Italy has no regulations on sextortion in their Italian Penal Code and crime is usually associated with sexual assault, corruption and sexual harassment (UIA-IROL, 2017).

3.3. Legal Framework of Turkey

The Republic of Turkey has a unitary structure and the Turkey’s judicial system has a principle of independence of judiciary. The organization, duties and jurisdiction of the courts; trial procedures are regulated by the Article 142 of the Constitution of the Republic of Turkey (“Constituion”). The legal rights of Turkey are based on international rules of organizations which Turkey is being a member of, such as United Nations, International Labor Organization and Member of European Council. These organizations ratify most of the key conventions and declarations. Turkey also has accepted the right to individual petition to the European Court of Human Rights. However, Turkey put into force the Convention on Cyber Crimes Committed on Virtual Environment (“the Convention”), which objects to harmonize domestic laws on cybercrime and establish effective system of cooperation known as Budapest Convention on May 2014.

Although, there are number of existing laws with elements of sextortion, Turkish legal system does not provide a legal definition of sextortion.

These elements of sextortion are rooted in the protection of the rights guaranteed by the Constitution. According to the Constitution Article 17, everyone has the right to live, protect and develop her/his material and spiritual entity.

3.3.1. Offences against Sexual Integrity at Turkish Legislation

Discussed elements of sextortion that may constitute features of several sexual offenses defined in 5237 numbered Turkish Penal Code (“Penal Code”). Sexual crimes take place on the section of “Crimes against person” with the heading of “crimes against sexual immunities”. It is important to emphasize on sexual assault crimes and sexual abuse of children defined under “Offences against humanity” on Penal Code.

The first element of sextortion as sexual assault is defined in Article 102 at on Penal Code as violation of the physical integrity of another person, by means of sexual conduct, the perpetrator will be subjected from five to ten years imprisonment upon the complaint of the victim. In addition to that, the Article states that, if the said sexual behavior ceases at the level
of sexual importunity, the term of imprisonment shall be from two to five years. On the Second paragraph of the Article, it is stated that, if the act is committed by means of inserting an organ, or other object into the body the offender shall be punished with a term of imprisonment no less than twelve years. On the Third paragraph of the Article, it is mentioned that if the offence is committed against a person who is physically or mentally incapable of defending themselves or if the offence is committed by misusing the influence derived from a position in public office or private working relationship, the punishments imposed are increased by one half.

Although it is crucial to state that, using force, threatening or deceitful/fraudulent actions is not considered as component of the crime according to the aforementioned Article 102/3.

If the victim has physical or mental damage, in a state of coma or dies as a result of the sexual assault, the penalty for the offender would be aggravated according to the Article 102/5.

However, if a child is involved in such case, the applicable laws change. Child molestation is defined in Article 103 in Turkish Penal Code as; any person who abuses a child sexually sentenced to an imprisonment from eight years to fifteen years. If the said sexual abuse ceases at the level of sexual importunity, the term of imprisonment shall be from three years to eight years.

The “child” is defined as a person who is under the age of 18. On below points, Turkish Penal Code describes sexual molestation to children as acts of:

“a) All kinds of sexual attempt against children who are under the age of fifteen or against those attained the age of fifteen but lack the ability to understand the legal consequences of such act,

b) Sexual behaviours committed against other children by force, threat, fraud or another reason affecting the willpower.”

On the second paragraph of child molestation Article, it states that, if the sexual abuse is committed by means of inserting an organ, or other object into the body of the victim, the offender is sentenced to a term of imprisonment for no less than sixteen years. If the victim has not completed the age of twelve, the penalty shall not be less than ten years in case of abuse and less than five years in case of abuse. In cases where the perpetrator of the offense at the level of molestation is a child, the case of investigation and prosecution depends on the complaint of the victim, his / her parent or guardian. On the third paragraph of the Article, it is stated that if the offence committed against a person with whom he or she has third degree blood relation or kinship or by stepfather, stepmother, half-sibling or adopter or, if the offence is committed by her/his guardian, tutor, instructor, caregiver, custodial parents or by those who provide her/his with healthcare or are under an obligation to protect, look after or supervise her/him and by undue influence based on public office or employment relationship the punishments imposed are increased by one half.

As a result of the child molestation, if the victim suffers with serious consequences of intentional injury, the offender is additionally sentenced. If the injury is resulted with the death of the person, the offender is sentenced with aggravated life imprisonment.

Sexual harassment is also an element of sextortion. According to the Article 105 of Turkish Penal Code; “if a person is subject to sexual harassment by another person, the person performing such act is sentenced to a term of imprisonment from three months to two years or to a judicial fine; and if the act of sexual harassment is committed against a child, the offender is sentenced to imprisonment from six months to three years upon complaint of the victim.” On the Second paragraph of the Article, it is declared that if the act offence committed by undue influence based on employment relationship or by using the advantage of interfamilial
relationships or by using the advantage provided by mail or electronic communication instruments or by the act of exposing, the punishment to be imposed is increased by one half.

Sexual harassment crime in Turkish legislation introduces a general offense of harassment and covers the verbal or indecent assaulting. As an element of sextortion, the sexual harassment by mailing or with electronic communication is defined separately with increased punishment.

Even if these sections do not adequately address sextortion, other provisions of Turkish criminal law can be used to partially address sextortion as shown below.

3.3.2. Offences against Liberty

Under Turkish law, a case of sextortion could be penalized under the regulation of threat and blackmail.

According to the Article 106 as crime of “Threat” it is stated that if any person who threatens another individual by stating that he will attack the individual’s, or his relative’s, life or physical or sexual immunity shall be subject to a penalty of imprisonment for a term of six months to two years. This offense relies on the threat of right to live, physical integrity and sexual inviolability.

If the threat relates to causing extensive loss of economic assets or other related harms, there shall be a penalty of imprisonment for a term of up to six months or a judicial fine, upon the complaint of the victim.

If the crimes of intentional killing, intentional injury or damaging property are committed with the aim to threaten, the penalties for such offences shall be imposed additionally.

Blackmail is specifically addressed in Article 107 of the Penal Code. The first paragraph stated that any person who forces an individual to obtain an illegal interest or forces someone to act, or fail to act such not being within the scope of his duty, or to perform an act contrary to law; by stating that he will, or will not, do something which would be within his duty or rights, shall be sentenced to a penalty of imprisonment for a term of one to three years and a judicial fine of up to five thousand days.

The second paragraph of the Article is important for the sextortion cases. It provides; where a person threatens to disclose, or make an accusation as to, a matter that would damage a person’s honor or reputation for the purposes of obtaining a benefit for himself or others, he shall be sentenced according to the provisions of paragraph one.

It is crucial to state that victim might commit suicide because of the sextortion. Directing somebody to suicide is defined at Article 84 of the Turkish Penal Code as inciting or encouraging another person to commit suicide or strengthen an existing decision or assists a person in committing the act of suicide. The offence is sentenced from two to five years and if death occurs, offender shall be sentenced to a penalty of imprisonment for a term of four to ten years.

A result of committing suicide, it is important that victims’ cases are investigated. As we mentioned above, anticipative policing in criminal intelligence serves to resolve past crimes. In every suicidal case, countries should conduct a detailed investigation by examining the background of the crime where relation to sextortion may be found. Countries may use their databases similarly as Public Access to Court Electronic Records (PACER) service of United States.

Corruption might also be applied to the notion of sextortion. According to Article 252 of the Penal Code, an offense is committed when a person secures, directly or through other people,
an undue advantage to a public official to perform or not to perform a task with regard to his duty. This offense is punished with imprisonment from four years to twelve years.

The procedural provision in the Turkish criminal procedural law states in the 5271 numbered Turkish Criminal Procedure Code (“Procedure Code” with the Article 134, titled “Search in computers, computer programs and logs, copying and seizure”. In investigations of cybercrimes are often applied in the measures set out in articles 135-138 of the section titled “Surveillance of communications through telecommunication facilities”. According to the Article 135 of the Procedure Code permits only surveillance of communications between real people and limited only mentioned crimes in the Article, these measures do not cover the measures provided by the Convention and do not adequate procedural rules for the complex crimes such as sextortion.

3.3.3. Provisions in Turkish Labour Code

Turkish Labor Act (“Labor Act”) provides tools to fight sexual harassment at the workplace. According to the Article 24 of Labor Act, in the event of employee being sexually harassed by another employee/employer or third person in the workplace, where adequate measures are not taken, although the employer was informed of such conduct, employee then has the right to terminate the employment contract immediately. Also any termination of the employment contract by employee due to the sexual harassment, employer might pay compensation.

3.3.4. Gender-Based Violence Legislation

Sextortion may be connected to gender-based violence protection from different perspectives, not only from a legal point of view (UIA-IROL, 2017). The first step of access to the law for sextortion crime must be the change in discriminatory attitudes.

According to the Turkish Constitution Article 10, everyone is equal before the law without distinction as to language, .. or any such grounds. And also men and women have equal rights. The State has the obligation to ensure that this equality exists in practice. Besides, Article 50 of the Turkish Constitution states that minors, women, and physically and mentally disabled people are protected in terms of working conditions.

However, Turkey adopted number 6248 domestic violence law which is the Law to Protect Family and Prevent Violence against Women in cooperation with the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence. The purpose of this law is to protect women, children, and family members of victims of domestic violence and to provide services such as financial aid, psychological and legal guidance. According to the Law, there are various procedures adopted e.g. by issuing a restraining order to prevent the perpetrator of violence of by relocating the victim upon her request.

Despite of strong and comprehensive legislations, Turkey is already developing implementation systems to provide protection against victims of violence. For instance, the problem of the press is about writing the results of court cases where attackers are convicted, condemned and/or imprisoned is remain unlawfully in Turkey. This type of digital victimization appears as an unlawful violation of personal rights of women who have suffered from violence and abuse in their lives. In order to prevent this type of violence, firstly the press should be lawful within the frame of the right of the society to receive information and respect to data privacy of victims. Following that, the right to erase data might be applied to unlawful reports according to the right of being forgotten with developing effective criminal rules of procedures to gathering digital evidence and social awareness (Küpeli, 2016).
It is crucial to state that said legislations are not enough to create social awareness. In order to prevent the spread of cybercrimes like sextortion, it is important to educate the target victims by developing an educational system with regulations and by releasing videos explaining how sextortion occurs, what to do when being sextorted, as well as how parents can be ensure of the online safety of their children and how parents should talk to their children about it.

4. DEALING WITH SEXTORTION

In order to combat cybercrimes, states make regulations by enacting criminal and criminal procedural codes on their domestic laws. Identifying crime patterns and set off a definition of sextortion in comparative law will be served to coordinate an effective cooperation among states. In addition to the detailed legal regulations requirements in common, it is important to analyze crime dynamics in order to reach crime victims and prevent the spread of crime. Within this context, crime analysis can be done by using data mining techniques and machine learning algorithms.

Crime analysis is an investigation of the factors that constitute the crime along with the offense and the offender. This analysis also includes the prevention of the types of crime that have not yet been identified and taking necessary measures against crimes under the discipline of Criminology. In order to analyze, examine, demonstrates the correlation between crime trends and identify the concepts of crime with criminal, machine learning algorithms such as data mining can be used in.

Data mining is the process of finding anomalies and patterns of meaningful and future processes within large datasets to solve problems through data analysis (Han et al., 2012).

Machine learning is a general description of computer algorithms where model is introduced a problem. According to the data obtained from the problem, it is important to adjust to producing correct outputs for a large number of sample inputs. Machine learning methods are used to extract relationships in data mining (Nilsson, 1997).

Data mining and machine learning can be used for crime analysis. According to the data mining study in the field of criminal analysis by Bruin, Cocx and Kosters et al., the crime factors such as frequency, duration, seriousness and nature have been used to compare the similarity of criminals (Bruin et al., 2006). Nath et al. used a clustering model in data mining to identify crime patterns that are determined by using a machine learning algorithm. In the study, it was aimed to be able to support the security forces to solve the crimes faster (Nath, 2006).

The information that obtained by the combination of these techniques, can shed light on the solve of criminal provisions. According to accessing the data plays an important role for data mining of the crime, it is important for professionals to reach datasets which are derived with respect to privacy concerns.

In addition, it is difficult to predict crimes in advance. However, many kinds of crime such as occurred by using same methods can be avoided. According to the crime trends analysis, sextortion crime has complex structure with the combination of more than one crime as mentioned above. In order to monitor and potentially deter the future violations, determining the usage of phishing or cybersecurity vulnerability assessment malware tools and the relation between the defendant such as estranged/divorced spouses, dating partners, ex-boss in work life or authority on students are going to be an important stage of determining sextortion. However, sextortion crime may cause the death of the victim, the fact remains that, all the suicide cases also need to be examined with the possibility of blackmail or sextortion crime at the background.
5. CONCLUSION

Advances in technology have given rise to new types of cybercrimes with the new type of cyberattacks such as Internet of Things devices (camera, TV, modem etc.) and large-scale ransomware attacks including wide-range of cyber-bullying, online child sexual abuse, online scams, and identity theft. Cybercriminals mainly target innocent users to make money or extort sexual favor. Sextortion is “sexual extortion” which means to blackmail sexual information or images in order to extort sexual favors and/or money from victim. Criminals often use a phish with malware or email to deceive users on victim’s computers, however techniques of criminals are changing day by day. Despite of the Institutions and Associations are indicating that new laws are needed to target this crime; sextortion is still not legally defined as a crime in most of the countries. Although Turkey has a number of existing laws which deal with elements of sextortion, Turkish legal system still does not provide a legal definition of sextortion. Providing a legal framework of sextortion crime in comparative law with the effective cooperation among states on the transnational prosecutions, increasing victims’ access to the law, closing the implementation gap and using new machine learning technologies when analyzing cybercrime trends are going to support to fight against sextortion and all the cybercrimes in the legal area.
REFERENCES


