

Cyberbullying, Stalking and Online Harassment in North Macedonia and in Serbia

Ana Stevanovic

PhD in Arts and Media, Faculty of Dramatic Arts, University of Arts, Belgrade Serbia)

Oliver Risteski

MA in Criminology and Criminalistics, Center for Security Research, Skopje, North Macedonia)

Gentjan Skara

PhD in EU Law, Department of Law, Beder University College, Albania

Abstract

Information technology and the internet are deeply embedded in every segment of the human life. On the one hand the massive usage of computer systems, social media, information and communication devices and the internet facilitate the functioning of the human being, but on the other hand they increase the risks to the cyber security. The rapid development of information technology and the massive usage of information communication platforms lead to new possibilities of improving new forms of computer crime.

This paper studies the emergent forms, legal framework, law enforcement gaps, digital aspects, and psychological aspects of cyberbullying, stalking and online harassment in North Macedonia and Serbia. Two study cases for the Telegram groups in both countries. The paper contains EU law comparison, recommendation and prevention mechanism for mitigating this criminal phenomenon.

The aim of this paper is to achieve an adequate security strategy for recognizing the cyber threats against personal data, raising awareness, and build more resilient digital society. In particular, the research is going to have some contribution to improve cybersecurity through a multi-stakeholder approach including state institutions, academia, CSOs, and private companies involved in the field of cyber security.

Key words: Cybersecurity, computer crime, cyberbullying, stalking, online harassment, information technology.

1. Introduction

Cybercriminal phenomena bring huge numbers of security threats in cyberspace, cyber criminals are a step forward ahead of the official stakeholders. It seems law enforcement have been caught unprepared for the new security challenges in the digital world. With the quick development of information technology and social networks, information becomes more accessible, communication is facilitated, and people share many photos and videos, which may be misused in the future. Using the internet network according to the data of the State Statistical Office in North Macedonia, in the first quarter of 2020, 79.9% of the households had access to the Internet at home. The participation of households with broadband connections in the total number of households was 87.8% in 2020. In the first quarter of 2020, 81.4% of the total population aged 15-74 used the

Internet, and 70.9% used the Internet every day or almost every day¹. North Macedonia with 84% usage of the Internet for social networks to create user profiles, messages and other contributions on Facebook, Twitter, and other social platforms is the fifth country in Europe after Malta, Iceland, Norway and Hungary². According to the latest data available of the State Statistical Office, 100 percent of young people aged from 15 to 24 in our country use the Internet, 96% percent of them use it every day or almost every day, 90 percent are part of social networks, 94% exchange messages, and 95% send content they create themselves³. This is a much faster pace of internet use than other age groups. These high numbers of internet users speak for themselves that we have a huge number of internet users who can be potential victims of the digital threats. But, do we have an adequate education system that promotes safe use of the Internet, especially in the area of creating personal content, using social media and media literacy when the users are young people? Social media is a global network through which a lot of personal information is shared to interact with its members. This, on the one hand, facilitates human social life, where information is freely accessible, and there is greater communication exchange, but on the other hand there is a huge space in which this electronic data is exchanged - cyberspace, and where this electronic data can be misused. Social media has imposed new trends in human behavior, increased dynamics of sharing personal information (photos, videos, locations, etc.), thus increasing the risks and threats of the users of these social networks. Cyberbullying is bullying committed in cyberspace but consequences are in reality. It takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through social platforms, text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.⁴

Information technology and the internet are deeply embedded in every segment of the human life. On the one hand the massive usage of computer systems, social media, information and communication devices and the internet facilitate the functioning of the human being, but on the other hand they increase the risks to the cyber security. The rapid development of information technology and the massive usage of information communication platforms lead to new possibilities of improving new forms of computer crime.

The aim of this paper is to achieve an adequate security strategy for recognizing the cyber threats against personal data, raising awareness, and build more resilient digital society. In particular, the research is going to have some contribution to improve cybersecurity through a multi-stakeholder approach including state institutions, academia, CSOs, and private companies involved in the field of cyber security. This paper studies the emergent forms, legal framework, law enforcement gaps, digital aspects, and psychological aspects of cyberbullying, stalking and online harassment in North Macedonia and Serbia. Two study cases for the Telegram groups in both countries. The paper draws on desk research methodology and contains EU law comparison, recommendation and prevention mechanism for mitigating this criminal phenomenon.

¹ See Report of the State Statistical Office, available at: https://www.stat.gov.mk/pdf/2020/8.1.20.31_mk.pdf

² See more for usage of internet for social media on Association for e-commerce at: <https://ecommerce.mk>

³ See more for “Javna soba” on Novatv at: <https://novatv.mk/telegram-ja-zatvori-grupata-javna-soba-na-barane-na-mvr/>

⁴ See more for cyberbullying at: <https://www.stopbullying.gov/>

The research is structured by this introduction and 5 sections. The second and third sections analyse from the legal, psychological and social perspective of the issue of cyberbullying in North Macedonia and Serbia. The fourth section discuss the cases of Telegram group in Serbia and in other Western Balkan countries, followed by an analyse of the cybersecurity challenges in the digital era. The last section provides recommendations.

2. CASE NORTH MACEDONIA

2.1. It seems that cybersecurity was caught off guard by the cybercriminal phenomena

Telegram is a very popular mobile and desktop messaging platform that has 550 million users according to their latest report⁵. Recently, in North Macedonia and the region we are increasingly witnessing the emergence of a variety of Telegram's groups, where explicit photos and videos are shared among its members. The first well known group that appeared in Macedonia was called "Public Room". In these groups sometimes explicit content is exchanged of girls and women, even underaged, their personal information, phone numbers, residential addresses, Facebook and Instagram profiles, etc. Although it is forbidden to post illegal pornographic content in accordance with the terms of use of Telegram⁶. This phenomenon has been increasingly trendy in the region. Common to all these groups is that the Telegram platform is most commonly used, in most of the cases, because of anonymity⁷ on this platform. The first group "Public Room" of Telegram had over 7000 members and about 10,000 photos and videos were shared⁸.

The Ministry of Interior was investigating the case, trying to find out who were the persons behind the group, and called on the citizens to report abuses in future cases. The Ministry of Interior officially confirmed that "Telegram" did not want to cooperate to provide electronic evidence of their members. Telegram's first "Public Room" was unveiled in January 2020, but was closed shortly after negative public reactions. The investigation of this case in the Ministry of Interior was led by the Sector for Computer Crime and Digital Forensics in coordination with the Public Prosecutor's Office (PPO), and the investigation identified the creator and administrator of the group and confiscated electronic devices with the objective to provide electronic evidence. The group numbered over seven thousand members, but after the investigation, the number dropped dramatically. According to Interior Minister Mr. Nake Chulev, about 800 photos and videos, mostly from Facebook, Instagram, and the Internet, were shared, but there were also private photos and videos⁹. This whole case itself caused an avalanche of public disagreement because there was a huge number of victims of gender-based violence, whose personal data became publicly available on the social network Telegram, and there was double victimization of the victims, instead of condemning those who committed the violence, the victim's conduct was condemned,

⁵ See more for most popular messaging apps on Statista, available at:

<https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>

⁶ See Terms of use of Telegram, available at: [Terms of Service \(telegram.org\)](https://www.telegram.org/terms)

⁷ More for anonymity on Telegram at: <https://www.techmesto.com/manage-remain-anonymous-mode-telegram-group/>

⁸ See more for "Public Room" now is called "Just for adult" <https://republika.mk/vesti/crna-hronika/javna-soba-sega-se-vika-grupa-samo-za-vozasni-i-vekje-ima-rechisi-7000-chlenovi/>

⁹ Statement of the Minister of MoI, see more "Chulev: The administrators of the group "Public Room" are not known yet", Slobodna Evropa, at: <https://www.slobodnaevropa.mk/a/30402017.html>

even though her personal information was shared publicly without her consent. Some of the explicit materials that were shared among the members were private photos and videos that the girls once sent to their partners or ex-husbands, a case when it came to the so-called retaliatory pornography, which is the sharing in the public of other people's private materials (photos or videos) with sexual content without the consent of the person to whom the materials belong, to embarrass and disparage the public.

According to the official report of MoI, Sector for Internal Affairs - Skopje had filed six reports to the PPO's Skopje for the first case "Public Room". Registered criminal offenses related to sharing personal information through social networks for the Sector for Internal Affairs (SiA) in Skopje are 67 criminal offenses under Article 149 "Abuse of personal data" of the Criminal Code, three of which relate to sharing photos of persons on social networks whereby one criminal charge was filed for one criminal act against one perpetrator and charges were taken on the record for two criminal acts committed by an unknown perpetrator. The first registered crime committed by sharing photos of people on social networks was recorded in 2014. Twenty four registered criminal offenses under Article 193 "Showing pornographic material to a child" of the Criminal Code, of which 15 criminal charges were filed for 15 criminal offenses against 17 perpetrators and charges were taken for nine criminal offenses committed by an unknown perpetrator. The first crime, "Displaying child pornography", was recorded in 1997. Nine registered criminal offenses under Article 193a "Production and distribution of child pornography" of the Criminal Code, of which six criminal charges were filed for six criminal offenses against seven perpetrators and three criminal charges were taken on a criminal record with an unknown perpetrator. The first crime, "Production and distribution of child pornography", was recorded in 2003.¹⁰

2.2. Law enforcement and the gaps in law

According to the existing legislation on this matter, the question of criminal or civil liability was raised and a separate question was raised to whom should this liability be directed, towards those who shared photos and videos, to the creator, administrators, or to all members of the group? The case has become even more sensitive as there have been underage girls among those whose photos have been shared, and such activities are linked to child pornography. According to the investigation conducted by the Ministry of Interior and the Public Prosecutor's Office, an Indictment was filed against two persons aged 32 and 21, who are charged with a criminal offense "Production and distribution of child pornography", provided in Article 193-a paragraph 3 regarding with paragraph 1 of the Criminal Code and they were remanded in custody. The crime they are charged with was committed in the period from 19 December 2019 to 28 January 2020, and the two defendants, the first as the founder, the second as the administrator of the group "Public Room" on the social network Telegram, were obliged to take care of the content of the textual and audio-visual contents that are shared by the members of the group. However, they deliberately allowed the group to make available video content showing obvious sexual acts with a child. Following the outbreak of this scandal, the social network "Telegram" extinguished this group¹¹, but the damage to the victims had already been done.

¹⁰ Official report of the Ministry of Interior for free access to public information, register of MoI no.16.1.2-1330 from 02.11.2021

¹¹ Link to the first Public room, now closed <https://t.me/javnasobamk>

The impression in the public was that the first case of a public room in Macedonia had a very slow and ineffective court resolution almost a year after its appearance in public, because measures were taken against only two perpetrators (creator and administrator of the group) for the crime "Production and distribution of child pornography" provided in Art. 193-a of the Criminal Code. Many of the perpetrators who shared explicit content were not identified, and the victims, fearing double victimization and stigmatization in society, did not even report this type of violence. All this encouraged the perpetrators to create new groups with increased dynamics in Macedonia and the region. The case Public Room 2 also appeared on the Telegram. The manner of execution was identical to the previous case, the Public Prosecutor's Office in Skopje in cooperation with the Ministry of Interior immediately contacted Telegram to obtain real data on user profiles of creators, administrators, and members of the group, but from Telegram no response has been received to such a request. This data is necessary to provide electronic evidence and to establish the identity of those who shared explicit content. The Public Prosecutor's Office then used the international legal aid mechanisms, under the positive domestic and international regulations, to request the data from the United Kingdom. So far, the authorities have not received a response to this request. It was also too difficult to determine criminal responsibility in the group Public Room 2 because there were victims from several cities, and more Public Prosecution Offices needed to intervene (Prilep PPO, Kavadarci PPO, Bitola PPO). As the conduct of the investigation is secret, from the information available to the public so far it can be determined that an order has been issued to establish a case for - "Production and distribution of child pornography - Article 193-a of the Criminal Code in the Public Prosecutor's Office Veles, namely digital expertise of a video of child pornography was found on the suspect's mobile phone.

From the current case law, we can summarize that except for the criminal offense "Production and distribution of child pornography - Article 193-a of the Criminal Code, which is prosecuted *ex officio*, for other forms, sharing personal information with explicit content without consent of the victims, no procedure has been initiated, no electronic evidence has been provided for the perpetrators who shared this content, nor have the perpetrators of this type of violence been identified at all. For all individual cases when the victim is an adult, the injured parties were directed by the Police to initiate a procedure for criminal offense "Abuse of personal data" - article 149, and "Endangering safety" - Article 144 of the Criminal Code of the Republic of Macedonia. According to the criminal act "Abuse of personal data" it covers someone who, contrary to the conditions established by law without the consent of the citizen collects, processes or uses his personal data, will have fines or imprisonment of up to one year.

Due to perception of the laziness and unwillingness of the Macedonian institutions to face this security risk, fearing double victimization, many of the victims did not report to the Police at all. Following the actualization of public room cases in Macedonia, many civil society organizations organized protests aimed at amending the Criminal Code and implementing the provisions of the Istanbul Convention - Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, which Macedonia has been signed and ratified by the Assembly. The Ministry of Labor and Social Policy in cooperation with the Ministry of Justice formed a working group that worked on the introduction of a new crime "Stalking". Stalking under

the Istanbul Convention is defined as repeated / continuous engagement in threatening behavior directed at another person, causing him/her to fear for his or her safety¹².

The proposed changes by the Ministry of Justice were approved by the Government on July 28th, 2021 and it remains for them to be voted by the Assembly and to implement these legal changes in the Criminal Code. The amendments provide for fines of up to three years in prison for those who follow, persecute or interfere with another person for a long time, abusing the victims' data, telecommunications, or other communication systems. Punishment will also be given to those stalkers who psychologically abuse, harass or intimidate their victims and thus cause them to feel insecure, anxious, or afraid for their safety or the safety of their loved ones¹³. The purpose of the envisaged changes is to ensure the protection of women from sexual and any other harassment through communication channels, social networks, including the latest cases such as "Public Room".

In order to effectively process these legal changes, it is necessary to involve all stakeholders and train the institutions in charge of this matter, the Ministry of Interior, Public Prosecutor's Office, Courts, Ministry of Labor and Social Policy, and civil society organizations.

2.3. Psychological aspects

Victims of this type of violence are going through a difficult psychological period. Especially if we take into account the fact that the victims come from a small settlement where everyone knows each other. The victims are stigmatized by society and the dysfunction of the legal system contributes to them feeling helpless and without legal protection from this violence that happens to them. According to psychologist Ana Blazeva, shame is the key emotion, that usually keeps victims completely alone in their pain and agony. The experience of violence is traumatic. Each of the victims bears individually, the abuse and violence that have been emotionally killed girls and women have been exposed to torture on their bodies. Exposure to a specific look, speech, and other gestures that aim to humiliate, is felt directly as an attack on the body and the person of the victim. To have experience of such brutal objectification and vulgarity is experienced as a direct attack on oneself, one's self-image, and one's self-worth. The attack shakes security, self-confidence, information security in others, security in both physical and cyber space. Insecurity means constant fear, fear overwhelms and deprives much of freedom. It affects not only the deprivation of freedom of expression, movement, contact but also other spheres of functioning - sleep, diet, work responsibilities, etc. In that sense, cyber-violence is no less painful or less real or harmful than direct violence¹⁴.

¹² See more for stalking under Convention on Preventing and Combating Violence against Women and Domestic Violence, Council of Europe - Istanbul Convention, available at: <https://rm.coe.int/stalking-istanbul-convention-web-a5/1680925867>

¹³ Statement of the Minister of Justice Bojan Maricic from 27.07.2021, available at: <https://sdk.mk/index.php/makedonija/demnene-na-internet-stanuva-krivichno-delo-izmenite-na-krivichniot-zakonik-pominaa-na-vlada/>

¹⁴ See more for the psychological aspects with psychologist Ana Blazeva, available at: <https://libertas.mk/ana-blazheva-psiholog-za-slucha-ot-avna-soba-sramot-e-kluchnata-emoci-a-shto-na-chesto-gi-drzhi-zhrtvite-celosno-osameni-vo-svo-ata-bolka/>

Such is the case with two young girls from Gevgelija who have been living in agony and they are afraid to leave home, after their ex-boyfriend with whom they were in a long relationship, shared their personal photos through the group "GevgelijaHub" on social networks and in private messages. He was reported by them for misuse of personal data and the production and distribution of child pornography.

One of the victims said:

"When I first heard about the 'Public Room' case, I thought it was scary what was happening to the girls and women here and I wondered if anyone would help them. It seemed to be a problem that is not mine, that happens far away from me and does not touch me in any way. Before long, such a group with the title 'GevgelijaHub' appeared in my area. I was born and live in Gevgelija. I am calm by nature and I am not considered a person who harms others. I thought that was enough to protect myself from injuries. Immediately after the group 'GevgelijaHub' appeared, I received a screenshot that my photo had been shared. At that moment, the world collapsed on my head. This is the photo that was taken in my previous relationship. I had a long relationship with my ex-partner and the photo was taken while we were together. I do not know what was the motive of that man to hurt me like that, but believe me, it would have been a severe blow to any woman, especially from a smaller environment where everyone knows everyone."

This young woman from Gevgelija, although in shock, gathered the strength to report the case to the authorities. She goes on to say:

"I recovered after a few days. Shock, sadness, and panic turned into anger and a desire for justice. I have not wronged anyone. He wanted to ruin my life and I would not let him. I decided to go and report him to the police. Nobody in the police understood that this was a big injury, that I could not sleep, eat, or go out because of what he did to me. All of Gevgelija was looking at my photo, photos of other girls, and nobody cared about that."

The victim contacted an NGO and they offered her legal assistance. Considering that the police did not complete the investigation and did not take any action regarding the case, the NGO lawyer filed the criminal charges to the Public Prosecutor's Office in Gevgelija, where she submitted all the collected evidence, screenshots, saved conversations with the man, etc. The report was filed with the help of the lawyer Natasha Boskova from the non-governmental Coalition Margini.¹⁵

¹⁵ Interview with the victim for "Sakam da kazam", available at: <https://sdk.mk/index.php/neraskazhani-prikazni/sedum-mesetsi-mojot-zhivot-i-mojata-trauma-lezhat-vo-fioka-vo-obvinitelstvo-a-zlostornikot-mi-se-smee-svedochi-gevgelichanka-chij-poraneshen-dechko-spodeluva-nejzini-fotografii/?fbclid=IwAR1XReQUgA1BECVcbLiJp-Ba7CHfo-cFk5WXdPcXkTXEhUi0CwBEsQVAjfs#.YB5WGW-f1QA.facebook>

The report submitted to the Prosecutor's Office by the complainants states that during the summer of 2013, when one of the victims was in an intimate relationship with the defendant and when she was only 16 years old, at the request of the defendant, a video with pornographic content was recorded on his mobile phone. The second injured applicant states that two years ago, at the request of the same defendant, she sent him a photo with intimate content from her mobile phone to his mobile phone. At the time of the photoshoot, the second victim was an adult. While they were in an intimate relationship with the reported person, they state that he threatened them that if they did not treat him well, he would publish the video clip and the photo. The report also states that the clip with pornographic content recorded in 2013 with one victim and the photo of the other victim from 2017, in the period from 05.07.2020 to 09.07.2020, was shared between 23 people through the Facebook messenger application due to which one of the girls reported the case to the police station in Gevgelija. Police in Gevgelija acted on the instructions of the Prosecutor's Office, whereupon the defendant was called to state the allegations in those cases. Also, as evidence in the application were submitted the Facebook addresses of 12 people who shared these contents among themselves, among which was not the address of the reported person.

The official state of Prosecutor's Office for criminal act "Production and distribution of child pornography" under Article 193-a of the Criminal Code, was because the event occurred more than 7 years ago, and from the evidence submitted by the complainants at the time of the crime can not be determined with certainty whether the complainant, she was a minor or not, which is an important element for the existence of this crime, according to the Prosecution.

Usually in such proceedings, with a warrant search for a computer system, the Police requires the Prosecutor, next that request is going to the court, the computer and mobile phone of the reported person should be confiscated in order to extract the data needed to determine whether there are elements of a crime. In this case, the investigation doesn't identify the original sender of the video and photos, because he is not among the 12 Facebook profiles for which the applicant submitted evidence that they shared.¹⁶

One of the victims in the Public Room on Telegram, decided publicly to talk about this scandal. She made a video in which she addressed, and explained everything she went through. She explained that she had posted a photo on her Facebook profile. That photo had been stolen and customized with indecent comments. After that it was shared in the Public Room. She started to receive many calls and messages with humiliating offers.¹⁷

2.4. Digital rights and Telegram privacy policy and other regulation review

We are living in the digital world, every digital interaction among the users in cyberspace should be secure, digital law needs to protect and safeguard fundamental human rights. Digital rights are human rights and legal rights closely linked to freedom of expression and privacy, are those that allow people to access, use, create and publish digital media, as well as access and use computers,

¹⁶ See more in: "Sakam da kazam", Gevgelija Prosecutor's Office can not determine whether the victim is a minor on an intimate recording that is shared, and there is no search warrant for the phone and computer of the reported person, aailable at: <https://sdk.mk/index.php/neraskazhani-prikazni/gevgeliskoto-obvinitelstvo-ne-mozhe-da-utvrddali-zhrtvata-e-maloletna-na-intimnata-snimka-shto-se-spodeluva-a-nema-nalog-za-pretres-na-telefonot-i-kompjuterot-na-prijaveniot/>

¹⁷ Video message of the victim, available at: <https://www.instagram.com/tv/CKi6fl8jzJA/?hl=en>

other electronic devices and communications networks. Digital rights are human rights in the digital age. Digital revolution nowadays brings almost everything to happen in cyberspace. Social media made drastic changes in human online behavior, cyberspace at the same time is a huge opportunity but also a source of insecurity for their users. The purpose of digital rights is to protect the user of violence in cyberspace and to feel safe. Digital rights are merely an extension of the human rights set out in the Universal Declaration of Human Rights by the United Nations as applied to the online world. We can group following key digital rights:

i) Universal and equal access to the Internet

People should be able to access the Internet regardless of their income, their geographical location or their disabilities. The UN Human Rights Council recognises in a report that the right of access is essential to freedom of opinion.

ii) Freedom of expression, information and communication

These basic human rights are threatened on the Internet when governments block websites or social networks, which is a violation of the right to communication and free association, or censor content, which is contrary to freedom of expression and information.

iii) Privacy and data protection

Citizens must have control over who stores their personal data and be able to delete them at any time. The right to privacy is threatened on the Internet by the theft of credentials, the appropriation of personal data and their use for financial gain, etc. (sharing private personal data, storing them in so called “Public room” channel on Telegram without consent of the victim).

iv) Right to anonymity

The right to anonymity and encryption of communications is particularly threatened in those countries that prohibit the sending of encrypted messages and communications, which is necessary for reliable and secure transactions on the Internet.

v) Right to be forgotten

This is the right to have a person's private information removed from Internet searches, databases and directories. It is currently recognised by the EU in the GDPR as a 'right to delete' and it has already been invoked in other countries such as Argentina, the US, South Korea and India.

vi) Providing electronic evidences

Internet service providers, providers of access to online content and services, or other companies or public authorities should provide you with easily accessible information about your rights and possible remedies. National authorities have an obligation to protect you from criminal activity committed on or using the Internet

vii) Protection of minors

Governments must not only ensure the protection of children on the Internet, as in the case of child pornography, but also ensure that companies provide the means to guarantee safe access without infringing the rights of children. If you are a child or a young person, you are entitled to special protection and guidance while using the Internet. (In so called "Public room" channel on Telegram some of the personal data were from minors)

viii) Intellectual property

Authors must be guaranteed recognition of their artistic or literary work and the right to be remunerated for its use, while guaranteeing free access to works that are already in the public domain¹⁸.

3. CASE SERBIA

3.1. It seems that cyber security is still not the main topic when it comes to the Republic of Serbia

Despite the fact that Chapter 24 has been open in the process of negotiations on joining the European Union, there are almost no changes (except for moving deadlines), at least when it comes to security in cyberspace. This chapter is called "Justice, Freedom and Security" and deals with all possible aspects of security such as organized crime, migration, asylum, drug and human trafficking, euro counterfeiting, borders, as well as police and customs cooperation. Among all these aspects, cyber security has strayed somewhere, which is treated practically exclusively from the angle of cybercrime. This fact follows the paradigm established at the beginning of the century within the European Union, that cyber security, which at that time was much more related to cybercrime, be addressed in a package with all these other, not so "cyber" issues.

The European Commission's Chapter 24 screening report was published in May 2014 and points to the fact that the fight against high-tech crime in Serbia is still in its infancy. It was stated that Serbia has formed a special VTK unit within the Ministry of Internal Affairs, as well as the Special Prosecutor's Office for High-Tech Crime. Serbia has signed the Council of Europe Convention on Cybercrime and has largely aligned its legislation with Directive 2013/40 / EU on attacks against information systems. It was also concluded that the amendments to the law, especially in the part related to sanctions, must be fully harmonized with EU regulations.

In the 2016 Progress Report on Serbia, the European Commission pointed out that Serbia does not have a strategy on high-tech crime and that it is necessary to adopt it. The Action Plan for Chapter 24 of the Government of Serbia provided measures to harmonize its laws with Directive 2013/40 / EU and European Union standards for combating high-tech crime through the analysis of the existing legal framework "in order to determine the degree of compliance with Community law

¹⁸ Digital rights essential in the internet age, available at: <https://www.iberdrola.com/innovation/what-are-digital-rights>

and EU standards (deadline first quarter 2016)”, and drafting laws and regulations based on the analysis (deadline last quarter 2016).

In the recommendations of the screening report related to the status of the police in the fight against organized crime, the Commission noted the need for provisions related to specialized training as well as increasing the capacity of the Department for Combating High-Tech Crime at the Ministry of the Interior. an increasing number of criminal activities to be investigated, as well as the introduction of special techniques that would enable the Department to comply with modern operational international standards.

Among the last in Europe, Serbia passed the Law on Information Security at the beginning of 2016, and by the end of the same year, it adopted bylaws. The implementation of this law, despite the fact that it should be completed, is still in the initial phase. The reason for this is the somewhat recklessness of the legislator who classified all authorities (11,000 of them) in the list of ICT systems of special importance and set them serious standards, which most of them do not have and will not have the capacity to meet, and there is essentially no real need for it. measures with many who found themselves on that list.

In accordance with this law, the National CERT within RATEL was formed and the registration of special CERTs was established.

3.2. Information security development strategy: behind closed doors

The key moment in this area in 2017 is certainly the development and adoption of the Strategy for the Development of Information Security in Serbia (2017-2020). In August 2021. The Minister of Trade, Tourism and Telecommunications in the Government of the Republic of Serbia, Tatjana Matic, announced that the Government adopted the Strategy for the Development of the Information Society and the Information Year of Security Measures and the Information Year of Security and Social Activity on December 2, 2010 and Social Activity on December 2, 2006.

On that occasion, Matic pointed out that Serbia recognizes significant digitalization and information security, which the enviable results in this area show.

The strategy covers two important areas - information society and information security, whose further development is a prerequisite for full digitalization of society, the development of society. The adoption and implementation of the strategic document in the field of information society development and information security is important in order to continue with further improvement of digital knowledge and business skills of all communities and the basics of business and business establishment and economic development. improving digital infrastructure in educational institutions.

In addition, it is necessary to continue and intensify activities on digitalization of services and business in the public and private sector, and with all that, it is important to improve the information-independent state-private position, mutual cooperation and privacy by promoting regional and international cooperation. The Strategy for the Development of the Information

Society and Information Security for the Period from 2021 to 2026, with the Action Plan detailing activities until 2023.

The strategy is in line with the EU strategy on cyber security, and sets 7 principles for the development of information security in Serbia, including timely risk recognition, preventive measures and effective response to incidents, as well as continuous development of information security protection systems in legal, organizational and technical level, with adaptability to new circumstances and challenges. It is important to point out that special parts of the strategy relate to the safety of children on the Internet and information security in the education system.

For unknown reasons, the Ministry of Trade, Tourism and Telecommunications, which has had the best history of public hearings so far, did not publish a public hearing before the adoption of this strategy, and it was left without comments from the professional public, industry and civil society. It remains to be seen whether this practice will continue during the adoption of the action plan for the strategy.

Challenges

The reports on the implementation of the action plan for Chapter 24, in the period July-December 2016 and January-June 2017, within the recommendation 9, which refers to high-tech crime, clearly indicate that things have not moved much in this area compared to the screening report.

What is most visible as a challenge is the personnel policy, i.e. the blocked systematization of jobs in the Police Directorate, and the general two-year ban on employment in the public sector. Institutions are trying to reach the necessary standards for staffing of sectors relevant to cybercrime, such as the sector for Technological Crime in the Ministry of the Interior and the Special Prosecutor's Office for the Fight against Technological Crime, through reorganization and internal personnel maneuvers.

On the ground, the situation brings to the surface other challenges, again of a personnel nature. The non-competitiveness of the state when it comes to working conditions, especially financial, for the profiles needed in the sectors dealing with cybercrime, is a problem that is difficult to overcome. The risk that someone will move to the private sector after a few years spent in these institutions is more than real, and the state must find some modality to motivate experts to work for the state. A potential solution in this area is the concept of public-private partnerships, which could be a serious starting point for overcoming these challenges.

The future

The Prime Minister of Serbia, Ana Brnabić, has repeatedly stated that cyber security and the fight against cybercrime are high on the Government's priority list. We will see if her words will reflect on the factual situation in Serbia, but what is certain is that Serbia as a state has just scratched the field of cyber security and that we have a long way to go to reach some of the lands in the region and Europe. The lucky circumstance in this process is that there are partners in the country and abroad who are willing to help and who with their experience and expertise can contribute to making the adoption and implementation of the latest standards easier and more efficient.

The state's openness, i.e. its readiness to encourage the development of public-private partnerships and cooperation with all stakeholders, including academia, industry and civil society organizations, determines how quickly and well it will be able to achieve the desired results, and finally close Chapter 24., at least when it comes to cyber security.

3.4. Legal framework of fighting cyberbullying in Serbia

Serbia does not have a specific legislation targeting cyberbullying. However, certain offenses contained in the Criminal Code are applicable even in the case of cyberbullying. The following section identifies legal provisions in each criminal code and provides a general overview of each offense that could be applied in the case of cyberbullying.

The Criminal Code in Serbia has only three articles (Arts 144, 145, 146) applicable in the case of cyberbullying. The first offense relates to the ‘Unauthorized photographing’. Pursuant to Article 144 (1) of the Criminal Code, whoever makes, without authorization, a photographic, film, video or other recording that significantly violates his personal life or who delivers such recording to a third party shall be punished with a fine or imprisonment up to one year. In the case that this offense is committed by an official in discharge of duty, such person shall be punished with imprisonment up to three years.¹⁹

The second offense deals with ‘Unauthorized Publication and Presentation of another’s Texts, Portraits and Recordings’. According to Article 145 (1), publishing or displaying “a file, portrait, photograph, film or phonogram of a personal character without the consent of the person who composed the file or to whom the file refers, or without the consent of the person shown in the portrait, photograph or film or whose voice was recorded on a phonogram or without the consent of another person whose consent is required by law and thus significantly interfere with the personal life of that person, shall be punished by a fine or imprisonment for a term not exceeding two years.” In the case that this offense is committed by an official during the performance of his / her duties, shall be punished by imprisonment for a term not exceeding three years.²⁰

The third offense relates to the “Unauthorized collection of personal data”. Article 146 of Serbia Civil Code prohibits obtaining, communicating, disclosing, using, collecting of personal data without the authorization. Whoever commits such offense shall be punished by a fine or imprisonment for a term not exceeding one year.²¹ In the case that such offense is committed by an official person in the performance of service, he/she shall be punished by imprisonment for a term not exceeding three years in Serbia.²²

3.5. Impact of the EU Law on candidate countries

The Treaty of Lisbon, adopted in 2007 and entered into force in 2009, pays a particular importance to fundamental human rights. One of the founding values of the Union is the respect for human

¹⁹ Criminal Code in Serbia, Art 144 (2).

²⁰ Criminal Code in Serbia, Art 145 (2).

²¹ Criminal Code in Serbia, Art 146 (1 and 2)

²² Criminal Code in Serbia, Art 146 (3).

rights.²³ Furthermore, the Treaty of Lisbon introduced a specific objective, *inter alia*, to ‘combat social exclusion and discrimination, and shall promote social justice and protection, equality between women and men, solidarity between generations and protection of the rights of the child’ Also, in its relations with the wider world, the EU upholds and promotes its values and contributes to the protection of human rights, in particular the rights of the child. In line with the Lisbon Treaty, the EU Charter of Fundamental Rights guarantees the protection of human’s rights by EU institutions and EU Member states when implementing EU Law.

While the EU recognizes the human’s rights, neither Treaty of Lisbon or EU Charter have a single provision that would completely and directly define and regulate cyberbullying issues. Furthermore, neither Treaty of Lisbon or EU Charter confer a competence on the EU as a general policy area. Under the principle of conferral, the EU acts only within the limits of the competences assigned by the Member States to attain the objectives set out therein. Competences not conferred upon the Union in the Treaties remain with the Member States.²⁴ Article 2 TFEU recognizes: i) exclusive competence- only the Union may legislate and adopt legally binding acts, whereas the Member States being able to do so themselves only if so empowered by the Union or for the implementation of Union acts;²⁵ ii) shared competences - the Union and the Member States may legislate and adopt legally binding acts in that area but the Member States shall exercise their competence to the extent that the Union has not exercised its competence;²⁶ and supplementary competences – the EU supplements the actions of EU MS actions without thereby superseding their competence in these areas.²⁷ In the case of cyberbullying, the EU has only supplementary competences. In other words, the EU only supports, coordinates or supplement the initiatives adopted by Member States at domestic level.

In addition to the EU Member States to bring their domestic legislation in compliance with the EU Law, even candidate countries have an obligation to approximate their existing and future legislation in compliance with EU Law. Serbia and North Macedonia as candidate countries are in

²³ Treaty on European Union (TEU) [2016] OJ C 202/1, Art 2.

²⁴ Arts 4 (1) and 5 (2) TEU

²⁵ Treaty on the Functioning of the European Union (TFEU) [2016] OJ C 202/1, Arts 2 (1) and 3 TFEU. The Union shall have exclusive competence in the following areas: (a) customs union; (b) the establishing of the competition rules necessary for the functioning of the internal market; (c) monetary policy for the Member States whose currency is the euro; (d) the conservation of marine biological resources under the common fisheries policy; (e) common commercial policy and (f) for the conclusion of an international agreement under certain conditions laid down in second paragraph of Art 2 TFEU.

²⁶ Arts 2 (2) and 4 TFEU. Shared competence applies in the following principal areas: (a) internal market; (b) social policy, for the aspects defined in this Treaty; (c) economic, social and territorial cohesion; (d) agriculture and fisheries, excluding the conservation of marine biological resources; (e) environment; (f) consumer protection;(g) transport; (h) trans-European networks; (i) energy; (j) area of freedom, security and justice; (k) common safety concerns in public health matters, for the aspects defined in this Treaty.

²⁷ Arts 2 (5) and 6 TFEU. The EU shall have coordinative or supportive competencies in the following areas: (a) protection and improvement of human health; (b) industry; (c) culture; (d) tourism; (e) education, vocational training, youth and sport.

different stages of integration. Serbia has opened 18 out of 35 EU chapters and closed only 2 EU Chapters²⁸ whereas North Macedonia is waiting to open EU negotiation.

Both states have signed the SAA which represent the legal base between the candidate countries and the EU and the Member States in *ex parte*. The SAA aims to bring each country closer to the standards which apply in the EU. Approximation of domestic legislation with the EU *acquis* is one of the conditions for the accession of candidate states to the EU, confirmed by the European Council at the Copenhagen Summit in 1993. In this summit, the European Council decided that any European country wishing to join the EU had to meet the “acceptance of the Community *acquis*: ability to take on the obligations of membership, including adherence to the aims of political, economic and monetary union”²⁹

The SAA with Serbia and North Macedonia contain an identical approximation clause which lay down the obligation to approximate their domestic legislation. The approximation clause stipulates that both parties “recognise the importance of the approximation of [Serbia and North Macedonia’s] existing legislation to that of the Community and of its effective implementation” and Serbia and North Macedonia shall “endeavour to ensure that its existing laws and future legislation shall be gradually made compatible with the Community *acquis*”.³⁰ Therefore, approximation of laws has a particular importance for the candidate countries wishing to join the EU because they have to approximate domestic legislation with that of the EU.

3.6. How does the law in Serbia treat revenge pornography and the abuse of other people's intimate photos and recordings?

The Special Prosecutor's Office for High-Tech Crime has formed several cases over the past two years related to the sharing of explicit content in different groups on various social networks and applications, the Prosecutor's Office said.

In 2019, the highest number of reports, 43, were for persecution, followed by 24 reports for showing, obtaining and possessing pornographic material and exploiting a minor for pornography, 13 reports for sexual harassment, two reports for blackmail - and only three reports for a single crime. which is not prosecuted *ex officio* - unauthorized publication of other people's pictures and recordings.

²⁸ Commission, Serbia’ < https://ec.europa.eu/neighbourhood-enlargement/enlargement-policy/negotiations-status/serbia_en > accessed 24 January 2022.

²⁹ European Council, ‘Conclusion of the Presidency’ (SN 180 / 1 / 93 Rev 1, 21-22 June 1993) <http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressData/en/ec/72921.pdf> part 7A (iii), accessed 23 January 2022.

³⁰ Stabilisation and Association Agreement between the European Communities and their Member States of the one part, and the Republic of Serbia, of the other part (SAA with Serbia) [2013] OJ L 278/16, Art 72; Stabilisation and Association Agreement between the European Communities and their Member States, of the one part, and the former Yugoslav Republic of Macedonia, of the other part (SAA with North Macedonia) [2004] OJ L 84/13, Art 68.

During the year of the pandemic, the numbers increased, so there were 60 reports of persecution, as many as 40 reports of child pornography cases, 16 reports of sexual harassment, one report of blackmail and five reports of unauthorized publication of other people's photos and footage.

The numbers show that the number of reports for the only act of vengeful pornography prosecuted on the victim's private lawsuit, sharing other people's pictures and recordings without permission, recorded an extremely small number of reports during both years. Lawyer Diana Malbaša believes that revenge pornography should be recognized as a serious social problem and a serious violation of women's human rights.

Therefore, such behavior should be treated in such a way in criminal proceedings and such acts should be prosecuted *ex officio*. There is a possibility of changing this law, but after a serious analysis, Djordje Krivokapic agrees. Revenge pornography is often linked to other forms of violence, so we do not have data on how often reports end in a conviction.

What can victims of revenge pornography in Serbia do?

Anyone can file a report of revenge pornography and misuse of private images and recordings directly with the Special Prosecutor's Office for High-Tech Crime at vtk@beograd.vtk.jt.rs, or by mail to Savska 17a in Belgrade.

Along with the report, it is necessary to submit evidence that will support the allegations, they say from the Prosecutor's Office. A report of this type of violence can also be filed with the police. Women who have suffered this type of violence can always turn to women's NGOs for legal assistance in order to receive support and information on filing a report and the procedures that follow, say the Autonomous Women's Center.

Jelena* says that she immediately blocked all profiles from which she received inappropriate messages and threats, and that she did not keep recordings of the message, because she partially felt ashamed. She also says that she did not report the case to the police, expecting that he would not take her seriously because she sent pictures to the guy herself.

It is important for women to try to preserve evidence, to make a screenshot or recording of such announcements and to keep them in a safe place. It is difficult to think about the evidence at first, because when you come to such content, the first urge is to delete it, if you can.

"But we always advise women to collect evidence, even if they do not want to report the case at that moment, because they may need that evidence," says the lawyer.

Serbia lacks a system that would enable easy, simple and anonymous registration, estimates Djordje Krivokapic.

"Every time someone posts someone's intimate video without permission, there must be a strong social response to the person who posted it, without questioning what part of that video is," he adds.

3.7. Digital Violence and the Telegram: Revengeful Pornography and Intimate Video Abuse - and How to Protect Yourself

Jelena* from Belgrade was 30 years old when someone manipulated her - she introduced herself as an ex-boyfriend on Instagram, and then shared her intimate videos with thousands of people on the Internet.

"I felt terrible, as if I had been raped," Jelena* told the BBC. Fear, guilt, shame, blackmail, depression and suicidal thoughts - victims of revenge pornography in Serbia have been going through all this for years. The problem came to the public's attention when several Telegram groups - in which tens of thousands of men from the Balkans exchange pornographic content - became the subject of a police investigation ordered by the Special Prosecutor's Office for High-Tech Crime. The Criminal Code in Serbia does not recognize revenge pornography as a criminal offense, but it does cover other offenses that fall under this type of violation of rights.

Only cases of child pornography, persecution, blackmail or sexual harassment are prosecuted ex officio, while for publishing and sharing other people's recordings without permission - which is often the case with revenge pornography - the victim must file a private lawsuit.

"That needs to change because violence against women and girls is happening more and more in the digital and online space, it has reached new proportions and can cause serious violations of rights," Diana Malbasa, a lawyer with the Autonomous Women's Center (AWC), told the BBC.

This organization provides legal, psychological and other types of assistance to women victims of violence. People have the freedom to live their own sex life as they want and to exchange what they want, but even when you trust someone 100 percent, warns lawyer Djordje Krivokapic, there is no guarantee that the picture you sent for several years will not be published. He adds that this can happen without violating trust, but when someone hacks your device or the company that collects and stores your data.

"You should always take that risk into account. "Everyone must be aware that the Internet remembers everything," Krivokapic, co-founder of the SHARE Foundation, which deals with the protection of digital rights and an assistant professor at the Faculty of Organizational Sciences in Belgrade.

The Special Prosecutor's Office for High-Tech Crime appeals to users of social networks to pay special attention to the protection of personal data. And that, they state, "they avoid publishing, exchanging or otherwise making their data available to others, as well as audio, photo and video material that may be misused."

During 2020, a larger number of reports was recorded than in 2019 for criminal acts related to the misuse of intimate images and recordings, according to the records of the Prosecutor's Office. Revenge pornography became a "new normality" during the pandemic, and data from SOS lines in the UK indicate an increase in such cases during quarantine.

What is revenge pornography?

In addition to harassment on social networks, digital harassment and hacking, revenge pornography is an increasingly present form of digital violence that affects women to a much greater extent, explains Mirjana Mitić, a social worker..

"Revenge pornography is any unauthorized recording, but also unauthorized sharing, as well as threats of sharing explicit content with a sexual character for which consent has been given for recording but not for its distribution," says Mitić.

It most often occurs after the termination of the partnership, but also in other situations - the distributor of that content can be a person whom the victim does not even know, she adds. Every tenth high school student has experienced someone posting photos or videos of her, which they sent privately and without consent to share further.

The girls were more exposed to blackmail - that their private information or recordings would be published if they did not agree to do something of a sexual nature in return. Compared to boys, girls are more likely to receive sexualized comments in the online world.

The term "revenge pornography" - which most often describes this type of violence - can be relativizing because it indicates that the perpetrator is taking revenge on the victim for something she did earlier.

4. The case of Telegram groups in Serbia and the Balkans - what happened?

At the beginning of March 2021, it was announced that there are almost a dozen groups on the Telegram application in which tens of thousands, mostly men from the Balkans, exchange various pornographic content.

The largest group among them - the EX YU Balkan Room, had about 36,000 members, and in the meantime, access to the history of correspondence and previously published content is limited. The content of other groups, some of which are dedicated to certain cities - so there is a group for Belgrade, Nis, Sumadija and other parts of Serbia. They mostly share pornographic videos and photos of women and girls. Private recordings of sexual relations or those downloaded from porn sites are also shared, as well as photos and videos from private messages on Instagram.

Stasa Ivkovic, one of the girls who introduced the public to these groups and initiated an investigation, claims that there was revenge pornography in the group, as well as footage of minors. "I found out about the group when a guy I don't know personally warned me that my Instagram profile was there," she told the BBC.

After joining this Telegram group, she saw members with posted Instagram profiles of girls asking if they provide sexual services for money, where they are from, what their address is, if anyone has nude photos or recordings, what she is like in bed or how many it's her price. When she started posting details from this group on Twitter, she became a target herself, so her photos, along with threats and insults, are still shared in groups on Telegram.

A similar fate befell other girls who pointed out this problem and tried to do something. Nineteen-year-old Andrijana says that she joined one of the groups with the intention of finding an administrator or one of the more active members in order for them to be responsible for their actions. Then her photo, in which she was fully trained, ended up in those groups with "rather unpleasant comments".

Stasa and Andrijana did not back down from the threats - which encouraged many women and girls to share their experiences with revenge pornography. Since then, Stasa's inbox has received daily messages from girls whose recordings, photos or personal data ended up in controversial Telegram groups. She says that some experiences are very painful to read because they are victims who, after a few years, still have terrible consequences.

"If one victim, after such a diversion of attention to a big problem in society, initiated a lawsuit and found the strength to take such a brave step, I think we have made a small step forward that carries weight and significance," Stasa said.

Shortly after the investigation was launched, the police announced that N. S. (1996) from Nis had been arrested on suspicion of publishing photographs and recordings of pornographic content "created by exploiting a minor" on Telegram as a group administrator.

A few days later, M. C. (1994), a suspect in several criminal offenses, was also arrested. He is suspected of harassing his ex-girlfriend, and when she refused contact with him, he threatened her, and then published her home address and intimate photos that she sent him when she was a minor.

What are the consequences for victims of revenge pornography?

When she was 14, Danica was blackmailed by her boyfriend and threatened to tell everyone that she had slept with him if she did not send him a picture of her breasts. She says that she was "blindly in love" with him and out of fear she sent a photo, and when she reached the group chat, Danica "the whole world collapsed".

"I tried twice to take my own life because I wasn't strong enough to deal with the comments of the environment, as if I was going through hell," says this young girl.

She lives in a small place, so the reactions of the environment were inevitable and unpleasant, she adds. They called her names, insulted her, labeled her, and she received support from her family and a few friends. At first she was afraid to seek help.

"I shut myself in and went through severe depression for several months," she recalls.

Only after some time, Danica turned to a psychiatrist, which, she says, helped her get out of the situation she was in.

"The consequences for the victim of revenge pornography do not differ much from what a person perceives as a victim of any other form of violence," says social worker Mirjana Mitic.

She explains that such violent practices degrade dignity through an attack on bodily autonomy, privacy and expression of sexuality. First of all, says Mitic, there is a feeling of helplessness and fear of the perpetrator, who can use the content to threaten and blackmail the victim for a long period of time, with the goal of destroying her self-confidence and taking control of her body and life.

"Women live in fear of being condemned by family, friends, partners, but they are additionally scared that they have the feeling that posting such content in an online space is unstoppable, and that the perpetrator can remain anonymous behind a device," explains Mitic.

It happens that the identity of the victim, address, phone number or profile on one of the social networks is openly stated with the shared content, which brings with it a wave of messages with humiliating offers, blackmail and threats, she adds.

People, especially young people, are often unaware of all the pitfalls of the digital world they can fall into. That is why it is important for the state to deal with prevention, for there to be a systemic response to such problems, and these topics should be included in upbringing and education, believes Krivokapić from the Share Foundation.

Consequences of the cyberbullying- Revenge photography is horrible for the victim

Her trust was betrayed - the victim sent content in the form of provocative images to her emotional partner, never realizing that it could be abused.

Humiliation and degradation - the one who distributes images of ex-partners in this way wants to humiliate the victim and degrade her. The number of people who see the photo is insignificant - whether it is just one person or thousands - the victim was not intimidated by such exposure to the public!

There is never a good intention behind vengeful pornography! NEVER!

Endangered privacy - The goal of the perpetrator is not to protect the victim, to cover her face. He wants her face and whole body to be seen because that strikes a blow. The abuser does not think about the victim's family, reputation, career, friends, he wants everyone to see the victim in an indecent issue.

Endangered security - The abuser often shares the victim's private information with photographs (recordings), such as place of residence, telephone number, residential address, where he is moving, working or studying.

Minors are often targeted

Before a photo or video goes public, the perpetrator blackmails the victim - blackmail may be for emotional reasons (the perpetrator blackmails the victim to return it), but financial blackmail is becoming more common. a friend blackmails another friend with pictures so that she can give her money from snacks, buy make-up and clothes.

Many victims do not even know that it was filmed secretly (during sleep, during the shower, and even on the street - remember the moment of the Spotted trend that was current in Serbia - that young girls are photographed on the street, above all, and that upload to the instagram profile, asking for the girl's information, such as name and surname).

5. Challenges for cybersecurity and Telegram Privacy Policy

Cybersecurity is essential to ensure the security and freedom of internet users. Protecting digital rights is crucial to make internet users safe. There are many cases with data breach such a big scandal is relation on Cambridge Analytica with Facebook where up 87 million of profiles including status, likes even private messages was obtained to Cambridges Analytica.³¹ Protecting private data can be done through encryption of communications as many communication platforms do. But, on the other hand as case on Telegram in this case there is possibility of creating groups/channels where admins doesn't have control of the shared content or intentionally is allowed shared private data sometimes pornographic contents even underaged. Although the use of a Telegram to post illegal pornographic content is prohibited under the Terms of Use of the Telegram³², this may still happen as is the case with so-called public room in North Macedonia. How should we act if digital rights are violated? In most cases it should be regulated with proper cyber rights legislation, effective and efficient law enforcement, strong cybersecurity private companies, CSO's and startups who are working on mitigating violating digital rights. Raising awareness from an early age in the schools and responsibility of each user to report cyberbullying, cyber threats, and inappropriate use of digital resources.

Telegram's main principles are, that Telegram doesn't use user's data to show them ads and user's data are stored explicitly just for the needs to function as a secure and future reach messaging service. Telegram is located outside of the European Economic Area, but it has registered one based group company as Telegram UK Holdings Ltd (71-75 Shelton Street, Covent Garden, London, England, WC2H 9JQ), as a representative to whom customers direct any issues relating to processing of users personal data, as well parent company is Telegram Group Inc, located in the British Virgin Islands; and Telegram FZ-LLC, a group member located in Dubai. Telegram is a communication platform which stores user's mobile number and basic account data (which may include profile name, profile picture and private information of the users). To make it easier for customer's contacts and other people to reach the customer, the screen name, profile picture, and customer username on Telegram are always public. There is a possibility to enable 2-step-verification for customer's accounts or store documents using the Telegram Passport feature; customers can opt to set up a password recovery email. This address will only be used to send to the customer a password recovery code if he forgets it. Telegram is a cloud service, it stores all content, messages, photos, videos and documents from customer's cloud chats on its servers. Customers can access their data from any of their devices anytime without having to rely on third-party backups. All data is stored heavily encrypted and the encryption keys in each case are stored in several other data centers in different jurisdictions. This way local engineers or physical intruders cannot get access to user data. Telegram also supports public channels and public groups. All public chats are cloud chats, all posts in public communities are encrypted, both in storage and in transit — but everything that is posted in public will be accessible to everyone. Telegram uses phone numbers of the customers as unique identifiers. Personal data of the customers from Europe are stored in data centers in the Netherlands, and all personal data is heavily encrypted.

³¹ See more for the scandal with Facebook and Cambridge Analytica at: <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>

³² Terms of use for Telegram available at: <https://telegram.org/tos>

To improve the security of user's accounts, as well as to prevent spam, abuse, and other violations of our Terms of Service, Telegram may collect metadata such as customer's IP addresses, devices and Telegram apps, history of username changes, etc. This metadata can be kept for 12 months maximum. To prevent phishing, spam and other kinds of abuse and violations of Telegram's Terms of Service, Telegram's moderators may check messages that were reported to them by their recipients. If a spam report - @Spambot is confirmed by moderators, that user account may be limited from contacting strangers – temporarily or permanently. In case of more serious violations, that account may be banned. If Telegram receives a court order that confirms user is a terror suspect, Telegram may disclose customer's IP address and phone number to the relevant authorities. So far, this has never happened. When it does, Telegram will include it in a semiannual transparency report published at: <https://t.me/transparency>. The Number of the members in Telegram group initially is 200 members, but it could upgrade into a supergroup which can have up to 200000 members. Maximum shared content can be up to 2 GB (doc. zip. mp3. etc), and an unlimited number of photos, videos and others files. Difference between Telegram groups and channels are that groups are for sharing stuff, all group participants can communicate with each other in the group and share multimedia files, while the admin holds the right to restrict member's interaction. Channels are a tool for broadcast messages to a large number of subscribers. There are no limitations on how many people can join a channel, but they cannot interact with each other. Telegram channel admins are the only ones with the right to post one-way messages³³.

6. Recommendations and preventive mechanisms

Based on the research findings, it is evident that perpetrators are using the Telegram platform to create a group where members share explicit content in order to misuse someone's personal information thereby harassing the victims of this crime throughout the wider online ecosystem. The anonymity of Telegram and the platform's negligent moderation policies highlight how relatively easy it is to manage these groups, as well as the absence of consequences for all who are directly or indirectly involved in this crime. When the shared content in that private group contains explicit content, child pornography, private personal data shared without the consent of the owner of that data, then we have a securely closed circle of electronic data that in itself originates from a crime, because they are shared without the consent of the owners of their data. These electronic data are electronic evidence, traces, which will lead us to the perpetrator who shared them in a private group. But the nature of digital evidence is vulnerable, their impermanence and susceptibility helps perpetrators evade the law, and it is sometimes very difficult to obtain adequate digital evidence in legal proceedings³⁴. In general social platforms share a massive volume of content, which then spreads at the moment when it is shared. It is not always easy to moderate the content if we know the fact that Telegram has over 500 million users, especially if the moderation is done by humans, it is a very slow and inefficient process. Telegram has no content moderation as Facebook or YouTube, whereby these contents would be automatically alerted or removed from the platform and that user's profile will be suspended. This is because Facebook and YouTube have automated methods, specialized algorithms that use artificial intelligence and machine

³³ See more for groups and channels on telegram at: <https://telegram.org/faq#q-what-39s-the-difference-between-groups-and-channels>

³⁴ Giancarlo Fiorella,* Charlotte Godart** and Nick Waters, Digital Integrity: Exploring Digital Evidence Vulnerabilities and Mitigation Strategies for Open Source Researchers, 2. A Fleeting Medium: Evidence Impermanence, available online at [Digital Integrity | Journal of International Criminal Justice | Oxford Academic \(oup.com\)](https://www.oup.com/digital-integrity)

learning will filter the posted contents automatically and recognize pornographic content. Facebook, unlike Telegram, utilizes software for automatic tools for content moderation, as image recognition, natural language processing (NLP) and language matching tools that seek to recognize the potential forbidden content, depending on the level of complexity and the degree of additional judgment needed, the content may then be checked by human moderators. Facebook has engaged huge number of content moderators who are part of 30 000 people who work on the safety and security of the users³⁵. Using AI can help platforms to identify a much larger set of posts which potentially are child pornography, hate speech, violence, disinformation, or other forms of harm. Most of the social platforms utilize similar algorithmic prompts methods, training them to spot and recognise specific content that is banned according to their policy. Of course, these algorithms are not 100% accurate and efficient. Thus exists container of potentially risky users and contents, If the user disagrees with the warning, they could simply confirm and continue to post his content anyway. In this situation, the post could be cued for eventual post hoc human review.³⁶

Telegram does not have an algorithm for recognizing forbidden content neither AI nor human moderators, creator and administrator from each group or channel have a duty and responsibility for content moderation which contains inappropriate contents according to their policy could be reported at abuse@telegram.org or dmca@telegram.org if the complaint is verifying then that groups or channels could be taken down. Although Telegram, according to its policy, bans groups and channels where porn bots are shared, terrorism (ISIS related), however local restrictions on freedom of speech are not forbidden. For example, if criticizing the government is illegal in some country, Telegram isn't allows to be a part of such politically motivated censorship³⁷.

Beside anonymity, this is the second reason why it is possible on Telegram to share explicit and pornographic content, even under-aged, which originates from private personal information who have not given consent for it, even if they don't know about it at the beginning. When the so-called "Public Room" first appeared in North Macedonia, the Ministry of Interior asked the Telegram to submit all the information about the creator, administrators and members of its own, but did not receive it due to their policy. According to the Telegram policy, protection of the data that is not covered by end-to-end encryption, uses a distributed infrastructure in many different places. Cloud chat data is stored in multiple data centers around the globe that are controlled by different legal entities spread across different jurisdictions. The relevant decryption keys are split into parts and are never kept in the same place as the data they protect. As a result, several court orders from different jurisdictions are required to force Telegram to provide any data.

This multi-state and complex structure of storing the data and decryption keys, ensures that no single government or block of like-minded countries can intrude on people's privacy and freedom of expression. Telegram can be forced to give up data only if an issue is grave and universal enough to pass the scrutiny of several different legal systems around the world. Telegram claims that until

³⁵ Everything in moderation, case study: Facebook, available at: <https://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/case-study-facebook>

³⁶ Platforms should use algorithms to help users help themselves, available at: <https://carnegieendowment.org/2021/07/20/platforms-should-use-algorithms-to-help-users-help-themselves-pub-84994>

³⁷ See more about illegal content of Telegram, available at: <https://telegram.org/faq#q-there-39s-illegal-content-on-telegram-how-do-i-take-it-down>

today have disclosed 0 bytes of user data to third parties, including governments.³⁸ This policy of Telegram in Macedonian cases makes investigation difficult for Macedonian authorities because Telegram doesn't cooperate with governments. Shared content in these groups is either false or harmful or both. Just with massive reporting of other members of this platform, but later not so quickly those groups would be suspended, but in the meantime the damage and trauma to the victims has already done.

Although with the amends in the changes of the Criminal Code and incrimination of a new criminal act - stalking, a step forward has been made in the processing of these crimes, still a set of measures is needed that should be implemented in the future in order to prevent and reduce this type of cyber violence. This research proposes a new path for future research as well as a set of measures that should be taken in order to prevent and mitigate cyber bullying. In this way I am striving to propose a secure and multi stakeholder approach of using cyberspace by highlighting the most dangerous aspects of internet users and technology.

1. Increased involvement of all stakeholders in the country and the region, government with relevant ministries (Ministry of Interior, Ministry of Labor and Social Policy, Ministry of Information Society, and Ministry of Education), civil society organizations, international organizations, academia, private company specialized in cyber security, in order to build capacity that would specialize in issues as online gender-based violence, online bullying, and cyber security. Continuous training and education of the new IT trends and challenges how to deal with, in order to build a more resilient society. Training for Police officers, Prosecutors, Judges, Teachers is essential to prevent and process this type of violence in legal procedure.

2. Raising awareness of online security and online violence from the earliest age in primary schools. According to a media literacy index, North Macedonia is on the bottom of the ranking North Macedonia (35th), Bosnia and Herzegovina (34th), Albania (33rd), Montenegro (32nd) and Turkey (31st). On the top of the ranking are Finland (1st), Denmark (2nd), Estonia (3rd)³⁹. By building knowledge for media and technology of the earliest age will increase perception for cyber security and reduce this type of violence done through the internet technology. People would be more aware that some digital record which is made, could sometimes in the future be used against them. Media literacy education is a part of the curriculum in some EU countries and US. By organizing workshops, debates, research and media campaigns on media literacy, cyber bullying and gender-based violence, will raise awareness of this type of violence and the need for appropriate response of institutions against this crime and raising cyber security in this area.

3. Timely adoption of new amendments to existing laws and adoption of new ones depending on the need relating to the new IT technology and cybersecurity. Information technology is evolving very fast. Telegram is developing its technological infrastructure in order to avoid the jurisdiction of one country, so it stores its data in several different countries and in case of request from official authorities there is no technical possibility to deliver them, because it really needs to be covered by jurisdiction from several states, which can rarely happen. That is, why timely change in law regulations is a step forward in order to mitigate this type of violence and crime. It may not be

³⁸ See more about How Telegram process data requests, available on: <https://telegram.org/faq#q-do-you-process-data-requests>

³⁹ See Media literacy index, available at: <https://osis.bg/?p=3750&lang=en>

completely suppressed this way, but it would certainly be reduced. Policy makers responsible for this issue should be aware of these threats and prevent them by bringing appropriate law on time.

On the individual level, some recommendations are as follow. If you need a physical repair of your personal device or if you change the device, make sure to delete the images and, if you can, physically destroy the internal memory, because even deleted photos can be easily "recovered" from the device's memory. If you need to repair the device, contact only a trusted service center.

Persecutors and voyeurs from the rooms for revenge pornography "download" images from LinkedIn. As much as photography is professional and non-sexual, women continue to be potential targets of vindictive pornography, doxing and spying on the internet. But as with all predators, the goal is not to make their "job" easier. For example, share pictures from the beach on social networks only with a small circle of friends.

Further tips are: no matter how safe the virtual space seems to you, be very careful in what you share with others. Almost one large and well-known women's forum, advertised as a forum exclusively for women, had the problem of persecution and espionage by male "members", which made it easier for them because girls publicly shared their photos thinking they were in a safe virtual space for women. Protect your webcams as they may be hacked.

The photos you post on social networks should contain a minimum of data through which you can be tracked. Lock profiles and pay attention when you accept a friend on social networks. Share your everyday photos only with a small circle of friends.


If you write on the Internet (forums, social networks), a pseudonym is an absolute recommendation, not a personal name and surname. Avoid any personal data through which you can be identified outside of virtual reality, e.g. do not put your name or nickname and year of birth. If you are exposed to verbal violence, report the abuser. Women suffer much more verbal and gender-based violence on the Internet - this is not a normal occurrence and should not be tolerated. Screenshot all examples of insults and violence.

And finally, the most important thing - a partner who demands naked photos and who puts pressure on you to send him naked photos is a big "red flag". No matter how nicely he prayed and how much he was a part of "seduction", do not share the data with anyone who exerts any kind of pressure to send him "offered" photos because this is the type of person who will most likely abuse that trust. It doesn't matter that "everyone does it", any kind of pressure, conditioning, and blackmail ("if you love me, you will do it", etc.) should be understood as a serious warning and a problem in itself. If you trust that person and decide to send your "nude" pictures, take pictures so that you do not see your face and no personal characteristics such as: tattoos, specific youth, an environment from which you can easily conclude where you live and who you are. Today's partner may become a vengeful ex tomorrow.

References

Convention on Preventing and Combating Violence against Women and Domestic Violence, Council of Europe - Istanbul Convention. (n.d.). <https://rm.coe.int/stalking-istanbul->

- convention-web-a5/1680925867
- Ecommerce.mk - Асоцијација за е-трговија на Македонија.* (2018, March 8). Асоцијација За Е-Трговија На Македонија. <https://ecommerce.mk>
- Everything in moderation.* (n.d.). New America. Retrieved January 24, 2022, from <http://www.newamerica.org/oti/reports/everything-moderation-analysis-how-internet-platforms-are-using-artificial-intelligence-moderate-user-generated-content/case-study-facebook>
- Fiorella, G., Godart, C., & Waters, N. (n.d.-a). *Digital Integrity: Exploring Digital Evidence Vulnerabilities and Mitigation Strategies for Open Source Researchers.* <https://academic.oup.com/jicj/article-abstract/19/1/147/6320889?redirectedFrom=PDF>
- Fiorella, G., Godart, C., & Waters, N. (n.d.-b). *How to Manage Anonymous Admin mode in Telegram Group.* (2021, April 1). TechMesto. <https://www.techmesto.com/manage-remain-anonymous-mode-telegram-group/>
- Most popular messaging apps.* (n.d.). Statista. Retrieved January 20, 2022, from <https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/>
- osis_m. (2021, March 14). *Media literacy index 2021.* Osis.Bg. <https://osis.bg/?p=3750&lang=en>
- Paul, C. (n.d.). *Platforms should use algorithms to help users help themselves.* Carnegie Endowment for International Peace. Retrieved January 24, 2022, from <https://carnegieendowment.org/2021/07/20/platforms-should-use-algorithms-to-help-users-help-themselves-pub-84994>
- RFE/RL. (2020, January 28). Чулев: Се уште не се познати администраторите на групата „Јавна соба“. Чулев: Се Уште Не Се Познати Администраторите На Групата „Јавна Соба“. <https://www.slobodnaevropa.mk/a/30402017.html>
- State Statistical Office. (n.d.). https://www.stat.gov.mk/pdf/2020/8.1.20.31_mk.pdf
- Stop bullying home page.* (2019, September 13). StopBullying.Gov. <https://www.stopbullying.gov/>
- Telegram FAQ.* (n.d.-a). Telegram. Retrieved January 24, 2022, from <https://telegram.org/faq#q-what-39s-the-difference-between-groups-and-channels>
- Telegram FAQ.* (n.d.-b). Telegram. Retrieved January 24, 2022, from <https://telegram.org/faq#q-there-39s-illegal-content-on-telegram-how-do-i-take-it-down>
- Telegram FAQ.* (n.d.-c). Telegram. Retrieved January 24, 2022, from <https://telegram.org/faq#q-do-you-process-data-requests>
- Terms of service.* (n.d.). Telegram. Retrieved January 24, 2022, from <https://telegram.org/tos>
- ‘The Great Hack’: Cambridge Analytica is just the tip of the iceberg.* (2019, July 24). Amnesty International. <https://www.amnesty.org/en/latest/news/2019/07/the-great-hack-facebook-cambridge-analytica/>
- WHAT DIGITAL RIGHTS ARE. ORIGIN.* (n.d.). Iberdrola. Retrieved January 24, 2022, from <https://www.iberdrola.com/innovation/what-are-digital-rights>
- ГЕВГЕЛИСКОТО ОБВИНИТЕЛСТВО НЕ МОЖЕ ДА УТВРДИ ДАЛИ ЖРТВАТА Е МАЛОЛЕТНА НА ИНТИМНАТА СНИМКА ШТО СЕ СПОДЕЛУВА, А НЕМА НАЛОГ ЗА ПРЕТРЕС НА ТЕЛЕФОНОТ И КОМПЈУТЕРОТ НА ПРИЈАВЕНИОТ.* (2021, February 9). Сакам Да Кажам. <https://sdk.mk/index.php/neraskazhani-prikazni/gevgeliskoto-obvinitelstvo-ne-mozhe-da-utvrdi-dali-zhrtvata-e-maloletna-na-intimnata-snimka-shto-se-spodeluva-a-nema-nalog-za-pretres-na-telefonot-i-kompjuterot-na-prijaveniot/>
- ДЕМНЕЊЕ НА ИНТЕРНЕТ СТАНУВА КРИВИЧНО ДЕЛО, ИЗМЕНИТЕ НА*

- КРИВИЧНИОТ ЗАКОНИК ПОМИНАА НА ВЛАДА.* (2021, July 27). Сакам Да Кажам. <https://sdk.mk/index.php/makedonija/demnene-na-internet-stanuva-krivichno-delo-izmenite-na-krivichniot-zakonik-pominaa-na-vlada>
- Државен завод за статистика.* (n.d.). Retrieved January 20, 2022, from <https://www.stat.gov.mk/>
- ЈАВНА СОБА* . (n.d.). Telegram. Retrieved January 24, 2022, from <https://t.me/javnasobamk>
- СЕДУМ МЕСЕЦИ МОЈОТ ЖИВОТ И МОЈАТА ТРАУМА ЛЕЖАТ ВО ФИОКА ВО ОБВИНИТЕЛСТВО, А ЗЛОСТОРНИКОТ МИ СЕ СМЕЕ, СВЕДОЧИ ГЕВГЕЛИЧАНКА ЧИИ ФОТОГРАФИИ СЕ СПОДЕЛУВАЛЕ НА „ГЕВГЕЛИЈАХАБ“.* (2021, February 6). Сакам Да Кажам. <https://sdk.mk/index.php/neraskazhani-prikazni/sedum-mesetsi-mojot-zhivot-i-mojata-trauma-lezhat-vo-fioka-vo-obvinitelstvo-a-zlostornikot-mi-se-smee-svedochi-gevgelichanka-chij-poraneshen-dechko-spodeluva-nejzini-fotografii/?fbclid=IwAR1XReQUgA1BECVcbLiJp-Ba7CHfo-cFk5WXDpCXkTXEhUi0CwBESQVAjfs#.YB5WGW-f1QA.facebook>
- „Телеграм“ ја затвори групата „Јавна соба“ на барање на МВР.* (2020, January 29). НОВА ТВ. <https://novatv.mk/telegram-ja-zatvori-grupata-javna-soba-na-barane-na-mvr/>
- (N.d.-a). https://www.stat.gov.mk/pdf/2020/8.1.20.31_mk.pdf
- (N.d.-b). [https:// Terms of Service \(telegram.org\)](https://Terms of Service (telegram.org))
- (N.d.-c). *Official Act of the Ministry of Interior for Free Access to Public Information, Register of MoI No.16.1.2-1330 from 02.11.2021.*
- (N.d.-d). <https://Libertas.Mk/Ana-Blazheva-Psiholog-Za-Slucha-Ot-Avna-Soba-Sramot-e-Kluchnata-Emoci-a-Shto-Na-Chesto-Gi-Drzhi-Zhrtvite-Celosno-Osameni-vo-Svo-Ata-Bolka/> . <https://libertas.mk/ana-blazheva-psiholog-za-slucha-ot-avna-soba-sramot-e-kluchnata-emoci-a-shto-na-chesto-gi-drzhi-zhrtvite-celosno-osameni-vo-svo-ata-bolka/>
- (N.d.-e). <https://www.instagram.com/tv/CKi6fl8jzJA/?hl=en>
- “Public Room” now is called “Just for adult” <https://republika.mk/vesti/crna-hronika/javna-soba-sega-se-vika-grupa-samo-za-vozasni-i-vekje-ima-rechisi-7000-chlenovi/>

Criminal Code in Serbia

Dok sajber nasilje nad ženama raste, sve potrebniija systemska rešenja

<https://startit.rs/dok-sajber-nasilje-nad-zenama-raste-sve-potrebniija-systemska-resenja/>

Sajber bezbednost u Srbiji, kaskanje za Evropom

<https://www.danas.rs/zivot/tehnologije/sajber-bezbednost-u-srbiji-kaskanje-za-evropom/>

Internet, hakeri i ucene: „Imamo vašu porno kolekciju“ - uspon programa za iznuđivanje

<https://www.bbc.com/serbian/lat/svet-56678398>

Digitalno nasilje i Telegram: Osvetnička pornografija i zloupotreba intimnih snimaka - i kako se zaštititi

<https://www.bbc.com/serbian/lat/srbija-56383660>

Šta je Internet osvetnička pornografija

<http://www.katarinajonev.com/sta-je-internet-osvetnicka-pornografija/>

"PLATI ILI ĆEŠ ZAŽALITI" Ćaskanje, lascivna fotografija, šakljiv video i, dok trepnete, u mreži ste SRPSKIH INTERNET UCENJIVAĀA

<https://www.blic.rs/vesti/drustvo/plati-ili-ces-zazaliti-caskanje-lascivna-fotografija-skakljiv-video-i-dok-trepnete-u/fysqpwy>