Behind the screens

Analysis of human trafficking victims'
abuse in digital surroundings

Behind the screens:

Analysis of human trafficking victims' abuse in digital surroundings

Review based on the experiences of 178 girls and women in the period from 2015 until 2020 in Serbia

Content

Acknowledgment

Organisation Atina's team owes deep gratitude to the girls and women who shared their authentic and valuable experiences with us, and thus enabled a creation of this document. It is quite rare to gather so many views of girls and women with the experience of human trafficking in a single place. For that reason, it is a true privilege to be a part of this endeavor. All 178 testimonies of abuses experienced in digital surroundings before, during, and after the trafficking situation serve to provide a deeper understanding and examination of the phenomenon itself, but also the creation of meaningful responses to growing challenges in this area.

We would also like to thank our colleagues: Sofija Todorović, Danilo Krivokapić, Bojan Perkov, Bojana Kostić, and Nataša Jović for their support during this process. Thank you for your commitment, encouragement, and faith in us and our work.

We owe special gratitude to the Sigrid Rausing Trust for their patience and support, especially in the moments that were crucial for development of our organization. Thank you for allowing us enough time and space to devote ourselves to this analysis. It would not be possible without you.

Finally, we would like to thank everyone who will take into consideration the importance of this topic, abuse of human trafficking victims in digital surroundings, think on it, and help build a future tailor-made to us all.

Organisation Atina's team

Introduction

For organisation Atina, it is of utmost importance that the voices of girls and women with the experience of trafficking are heard. And not only heard but understood and appreciated as well. That is why we created this document *Behind the screens: Analysis of human trafficking victims' abuse in digital surroundings*, which includes experiences of 178 girls and women who were using Atina's support and protection programs in the period from 2015 until 2020.[1] Such a number of respondents in the field of human trafficking victims' protection is an extremely important sample, and it should be noted that data collection process was marked by exceptional motivation of these girls and women to participate in it. It is also important to point out that this analysis was carried out during the pandemic, when a large part of global communication moved to the digital space, and the risks of violence and exploitation increased.

The results of this analysis confirm high prevalence of abuse in digital surroundings these girls and women have been exposed to prior, during and after the trafficking situation. Specifically, 42% of respondents survived some form of digital violence (such as cyberbullying, vengeful distribution of explicit/pornographic content, impersonation, etc.), while for 31% of them digital violence was directly related to the trafficking situation, both for the purpose of recruitment and exploitation. Of the total number of respondents, 65% were also exposed to digital threats, which were most often aimed at intimidation in order to change or withdraw a testimony or statement in criminal proceedings (a total of 59%). In addition to the high frequency of violence in a digital sphere, the analysis also shows that this specific type of violence

---

[1] Organisation Atina has, since 2003, been implementing a program of long-term social inclusion of human trafficking victims, as well as victims of all forms of gender-based violence and exploitation, that is based on respect for human rights and conducted with full participation, consent, and cooperation of the beneficiaries.

has become an almost indispensable form of coercion used by perpetrators of violence and traffickers to blackmail, threaten, belittle the victims, unauthorizedly record, or distribute pornographic material involving children as well. In this regard, the purpose of the analysis is to prevent digital abuse from becoming a "new normal" and a phenomenon to which the public, due to its frequency, becomes indifferent to, under the slogan - virtual is less real, and therefore less important.

The main pretension of this analysis, which Atina's team considers to be introductory, and represents a current situation in practice, is that the fight against violence and abuse in digital surroundings in the context of human trafficking should become a priority on the agenda of all actors who are a part of official mechanism for support and protection of human trafficking victims in Serbia. The document itself is intended for interested and professional public, representatives of state institutions working in this field at the national and local level, as well as civil society organizations, private sector, media and the general public. And not only that, from Atina's point of view it is necessary for this topic to finally take its own place in all the relevant national documents that will be created in the coming period, particularly in the future National Strategy for Combating Trafficking in Human Beings, and accompanying Action Plans, considering that this topic does not have such a place in the current strategy. It is also our wish for this analysis to serve as a basis for further, more extensive research on the topic of abuse in digital surroundings in the context of human trafficking in Serbia, and to shed a light on many of the concepts this paper has only touched on.

Bearing in mind that terminology is crucial in deliberating this sensitive topic, its development should correspond to the essence of phenomena being described, and emphasize the responsibility of perpetrators, i.e. those causing them. In this regard, it is important, both in our country and beyond, to invest particular efforts in development of terminology that accompanies this topic, and thus stop the use of archaic, inaccurate and incorrect terms that do not correspond to the essence of the phenomenon, such as "child prostitution and pornography", considering that a child cannot voluntarily participate in such a thing, and that those cases are a matter of sexual exploitation and abuse of children, persons under 18 years of age; thus, in this particular case, it would be more correct to use the terms abuse of children in prostitution, and exploitation of children for pornographic purposes.

We believe that many of you will come across terms in this document that explain various phenomena related to abuses in digital surroundings you have not heard before. For this reason, less known forms of abuse in digital context, such as doxing (targeting), catfishing (luring)

and others, are explained in detail hoping they will find use within professional and general public, and contribute to the identification, reporting and provision of adequate assistance and support to the victims. We hope that this analysis will encourage professionals to further reconsider their roles in the process of victims' protection in the context of digital abuse, and that this topic will become an obligatory part of the approach to the phenomenon of gender-based violence.

Jelena Hrnjak, programme manager of the organisation Atina
In Belgrade, October 2020

Analysis methodology

For the purposes of creating this document, a sample has been analyzed consisting of 178 trafficking victims who survived some form of abuse in digital surroundings. Within this analysis, particular attention was paid to types of abuse in digital surroundings, their perpetrators and the manner of inflicting harm. The aim of the analysis was to show the prevalence and forms of violence in digital surroundings in order to gain a fuller insight into the risks and challenges girls and women are exposed to, draw conclusions and make recommendations to improve the existing system of detecting such cases and protecting the victims.

Participation in this analysis was completely anonymous, and the sample was selected based on two pre-established criteria. The first condition was that respondents currently use some of Atina's support programs, or have used them in the past five years, while the second selection criterion was that respondents are formally identified as victims of human trafficking.[2] The sample in this analysis is representative[3] in relation to the total number of identified victims of human trafficking in the Republic of Serbia. Respondents were girls and women, 16 to 56 years of age, some of whom are members of Atina's Advocacy Group of women survivors of human trafficking. In the process of data collection, a Guideline for collecting data on abuses in digital surroundings (hereinafter: Guideline) was created and used. This document consists of 13 questions that target individual experiences of girls and women who participated. Guideline was the basis for conducting interviews

---

[2] Since 2011, formal identification of human trafficking victims in Serbia is being conducted by a social protection institution Center for the Protection of Trafficking Victims.

[3] In the period from 2011 until the end of 2019, following the statistics of the Center for the Protection of Trafficking Victims, data show that a total of 641 victims have been formally identified; http://www.centarzztlj.rs/.

with the respondents from the sample. It defines types, perpetrators, and content of abuses in digital surroundings to which these girls and women were exposed.

Researchers from organisation Atina gathered information from the beginning of February until the end of August 2020, in a form of semi-structured interviews. Principles of voluntariness, informed consent, and full participation of respondents were particularly respected, with the option not to answer a question if they did not wish to. From the very beginning, all interviewed girls and women were informed about the purpose of the analysis, and the manner in which collected information will be used. During the interviews, they were asked whether they had experienced a certain type of abuse on the Internet, or through information and communication technologies, and researchers were offering definitions of types of abuse in digital surroundings, as well as differences between them. Researchers also offered categories of responses related to sub-forms of violence, periods when the violence occurred, perpetrators of violence, and the media through which violence was committed. Despite the fact that findings show the respondents mostly recognize different forms of violence, particular attention was paid to the prevention of the risk of retraumatization, and interviews were conducted by representatives of Atina's team who have already established a relationship of trust with the respondents.

Collected data were sorted out quantitatively and presented in percentage values, having in mind the experiences of respondents. Given that this is a basic analysis, questions did not address all forms of violence in digital surroundings but only their most common forms, according to the testimonies of girls and women victims of trafficking in the period before the analysis was created. Quotes used in the analysis represent statements of the respondents made during the interviews and consultations conducted in Atina's Reintegration Center[4] on the topic of prevention of digital violence, its reporting, and processing. Responses of girls and women represent the basis for main findings and conclusions in this analysis.

---

[4] Reintegration Center represents the backbone of the program organisation Atina has been implementing in Serbia for 17 years now. Within this program, individual plans of service are being developed for all victims of human trafficking and gender-based violence. Within this space, they receive support through the case management method, as well as the service of psychological counseling. Beneficiaries of the program can also receive legal support, as well as assistance in further education, economic empowement, gaining independence, resolving civil legal issues, safe accommodation and other types of assistance and support.

Normative framework referential for abuse in digital surroundings

The term 'digital content' primarily refers to information that can be shared or downloaded via electronic media, but many believe that digital content is actually everything that can be published. Following that line of thinking, every tweet, Facebook status update, photograph, video, blog post, audio file, game, ebook, or text message represents digital content. If digital content encompasses everything that is published, it again means that everyone who is present on the Internet certainly creates digital content.[5]

Digital surroundings include information and communication technologies (hereinafter: ICT), including the Internet, mobile and related technologies and devices, as well as digital networks, databases, content and services.[6]

Digital abuse, in this context, is any form of abuse that has occurred on the Internet, through a telephone, computer, laptop, tablet or any other means of electronic communication, which aims to intimidate, harass and harm another person.[7] In this regard, legislation of the Re-

---

[5] Mullan, Eileen, "What is Digital Content?", EContent Magazine, Information Today Inc, 2011.

[6] Available at the Council of Europe website: https://search.coe.int/cm/Pages/result_details.aspx?ObjectId=09000016808b79f7.

[7] Law on Foundations of the Education System in Article 111 defines that digital violence and abuse, in the sense of that law, means: abuse of information and communication technologies that may result in injury to another person and endangerment of dignity and is achieved by sending emails, SMS, MMS, through a website, chat, engaging in forums, social networks and other forms of digital communication.

public of Serbia integrates and recognizes some of the forms of digital abuse, and their overview is presented below.

Constitution of the Republic of Serbia[8] guarantees that human life, physical and moral integrity is untouchable, as well as that human dignity is inviolable and that everyone shall be obliged to respect and protect it. The importance of these rights is also shown by the fact that the Constitution allows the right to freedom of opinion and expression (which is also guaranteed by the Constitution) to be restricted in cases when life, integrity and dignity are endangered.

Criminal Code[9] defines the following terms: computer data, computer network, computer program, computer virus, computer, and computer system. Criminal offenses that include these terms most often encompass offenses against computer data security, although there are other offenses that can be considered high-tech crime.

Within the Law on the Organization and Competences of the State Organs in Combating Organized Crime,[10] high-tech crime is defined as perpetration of criminal offenses in which computers, computer systems, computer networks, computer data, as well as their products in material or in electronic form serve as an object or means of execution.[11]

Regulations defined by this Law shall also apply to criminal offenses in which products in material or electronic form appear as objects or means of execution, namely: criminal offenses against intellectual property, assets, economy and legal transactions, as well as those offenses which due to the manner of execution or means used may be considered criminal offenses of high-tech crime, in accordance with the above-mentioned definition: criminal offenses against freedoms

---

[8] "Official Gazette of RS" No. 98/2006.

[9] Criminal Code, "Official Gazette of RS" No. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019; Article 112, in points 17-20, points 33 and 34, Articles 298, 299, 300, 301, 303, 304, 304a.

[10] Law on the Organization and Competences of the State Organs in Combating Organized Crime, "Official Gazette of RS", No. 61/2005 and 104/2009.

[11] "Serbia has also ratified Budapest Convention, by adopting the Law on Ratification of the Cybercrime Convention
("Official Gazette of RS", 19/2009), in March 2009". More can be read in the author text "Cybercrime and police cooperation in the EU", by Danilo Krivokapić and Andrej Petrovski, in publication "Guide through cooperation in internal affairs of the European Union", pages 187–209.

and human and civil rights, sexual freedom, public order and peace, and constitutional order and security of the Republic of Serbia.

Criminal offenses against freedoms and human and civil rights are, among others: endangering security, stalking, unauthorized wiretapping and recording, unauthorized photographing, unauthorized publication and display of other people's writings, portraits and recordings, unauthorized collection of personal data.[12] In this way, the legislation implies protection from various forms of violence that can occur in real time and space, as well as in digital sphere. It is especially important to point out that later use of acquired content from digital surroundings opens a space for the perpetrator to intimidate and disturb victim's wellbeing in the long run. This phenomenon is inherent in the experience of many human trafficking victims, which is confirmed by the findings presented in this analysis.

Furthermore, criminal offenses against sexual freedom also include the following: displaying, obtaining and possessing pornographic material, and exploiting a minor for pornography, inducing a child to witness sexual acts, using a computer network or communication by other technical means to commit criminal offenses against sexual freedom toward a minor.[13]

Criminal offenses against public order and peace[14] include, among others, causing panic and disorder, while inciting national, racial and religious hatred and intolerance is a crime against the constitutional order and security of the Republic of Serbia.[15] All the cited forms occur (most often) in digital surroundings as well, and as such must be equally sanctioned regardless of the space in which they are perpetrated.

At this point, it is justified to mention the Law on Personal Data Protection.[16] This law envisages a set of protection measures aimed to preserve the integrity, privacy and confidentiality of a person's data in a digital sphere as well. In addition, this law defines terms such as:

---

[12] Articles 138, 138a, 143, 144, 145 and 146 of the Criminal Code

[13] Rape, sexual intercourse with a helpless person, sexual intercourse with a child, sexual intercourse through abuse of position, prohibited sexual acts, pimping and procuring, mediation in prostitution, showing, procuring and possession of pornographic material and juvenile pornography, inducing a minor to witness sexual acts.

[14] Article 343 of the Criminal Code

[15] Article 317 of the Criminal Code

[16] "Official Gazette of RS", No. 87/2018

personal data,[17] processing personal data, profiling, consent of a person, violation of personal data. The above-mentioned law, aside from these definitions, also states the right of a person to deletion, i.e. limitation of the processing of personal data.[18] In this way, the legislation provided protection even in cases when the consent of the person for data processing was previously obtained.

In practice, the right to privacy and data confidentiality of human trafficking victims in Serbia is a major stumbling stone. Despite recommendations,[19] binding regulations and laws, institutions conducting (pre) investigative proceedings fail to prevent information leakage[20] and media coverage which includes confidential and sensitive data, directly violating safety and integrity of victims. An additional issue lies in a mass non-compliance with the Law on Public Information and Media,[21] Law on Electronic Media,[22] Rulebook on the Protection of the Rights of Minors in the Provision of Media Services,[23] Rulebook on the Protection of Human Rights in the Provision of Media Services, Serbian Journalists' Code of Ethics[24] and other documents protecting the privacy and personal data in media reporting, along with mass violations of numerous human and children's rights by the manner of media reporting. Since this issue requires a separate analysis, it will be further elaborated in other documents to be published soon.

---

[17] Law on Personal Data Protection ("Official Gazette of RS", No. 87/2018), Article 1, para. 1, 3, 5, 12 and 13

[18] Law on Personal Data Protection, Articles 30 and 31

[19] GRETA report on the implementation of the Council of Europe Convention Against Human Trafficking for Serbia: second evaluation round adopted on November 24, 2017, published in January 2018.

[20] Having in mind the negotiation process with the EU, we emphasize the obligations of Serbia from the Action Plan for Chapter 23, in the recommendation of the Screening Report No. 3.5.2, which calls on the state to take "urgent measures to stop threats and violence against journalists, as well as leakage of information on ongoing or planned criminal investigations". The activities to which the state has committed itself to are extremely important here, especially those from 3.5.2.15. to 3.5.2.21. as directly related to this issue.

[21] "Official Gazette of RS", No. 83/2014, 58/2015 and 12/2016

[22] "Official Gazette of RS", No. 3/2014 and 6/2016

[23] "Official Gazette of RS", No. 25/2015

[24] Available at: http://www.savetzastampu.rs/cirilica/kodeks-novinara-srbije.

Defining forms of abuse in digital surroundings

Theory and practice define different forms of violence and abuse in digital surroundings. As this analysis deals with the correlation between these forms of abuse and human trafficking, the following forms of abuse are not only causally related to human trafficking (e.g. online recruitment) but also represent different types of abuse human trafficking victims have been exposed to even before they were trafficked, as well as after exiting the situation of exploitation.

Less known types of abuse that have not yet found a recognizable place in domestic terminology are mentioned here, such as: cyberbullying, doxing, cyberstalking/cyberbombing, hacking (unauthorized access to other people's data), impersonation, catfishing, revenge porn (vengeful distribution of explicit/pornographic content) and sextortion (threat of publishing explicit materials for the purpose of extortion), as well as recruitment via the Internet, exploitation through information and communication technologies, unauthorized recording, distribution and use of digital content as a means of coercion in the context of human trafficking.[25] It is important to note that these are not all existing forms of abuse, only the most common ones Atina's team encountered while working on the protection of human trafficking victims.[26]

---

[25] Different classifications can be found in theory, and the types of digital abuse listed here were chosen because of their association with human trafficking, based on the classification used by Pen America, available at:

https://digitalnoharassmentfieldmanual.pen.org/defining-digitalno-harassment-a-glossary-of-terms/.

[26] For a detailed categorization of types of digital abuse, consult: https://womensmediacenter.com/speech-project/online-abuse-101.

Cyberbullying (cyberharassment)

This is a term that encompasses numerous disturbing behaviors on the Internet. Cyberbullying is mostly present among young people and can involve threats, shaming or humiliation in digital surroundings. It is often considered to be bullying on the Internet, where an individual or group of peers aims to belittle another person and harm their reputation, personality, and dignity.

Doxing (doxxing/targeting)[27]

Doxing (also doxxing) is an act in which one person (doxer) collects information about another person, analyzes and tendentiously shares them usually with the intention to present the targeted person in a negative light that suits the doxer, given that the doxer's goal is to cause harm to another person. Doxing also includes publication of personal information, such as address or contact information (telephone number), in order to enable others to harass or otherwise harm that individual.

Cyberstalking/Cyberbombing

Cyberstalking refers to a series of harassing behaviors committed repeatedly or with regularity, which usually cause the victim to suffer fear, anxiety, humiliation and extreme emotional harm. This includes sending messages, calling, sending voice messages in order to keep the person who is the target of the attack in a state of anxiety and fear. It is important to emphasize that cyberstalking does not have to include direct threats, but also refers to those activities that cause a feeling of helplessness and continuous stress. In the further course of this analysis, we will use the term cyberstalking for all such activities.

---

[27] Available at: https://www.economist.com/the-economist-explains/2014/03/10/what-doxxing-is-and-why-it-matters.

Hacking (unauthorized access to other people's data)

Hacking represents unauthorized access, intrusion into someone else's electronic device or network. It is often carried out with the intent to attack and incriminate another person, and to harm them by stealing data or violating their privacy.

Impersonation (imitation / false representation)

Impersonation can refer to creation of a false profile, as well as the use of someone else's identity. The purpose of impersonation is to make arrangements on behalf of the impersonated person or to misrepresent that person.

Catfishing

The term catfishing is used to describe a situation in which a person is lured into a meeting or relationship using a fictitious online identity. The difference compared to impersonation is that in the case of catfishing a third party is lured to a meeting or provision of information.

Revenge porn (vengeful distribution of sexually explicit/pornographic content)

Revenge porn, i.e. vengeful distribution of explicit/pornographic content, is a type of abuse that involves publishing content without the consent of the person who is in the video or photograph. The perpetrator uses their relationship with the victim, thanks to which they came to a possession of disputed content, in order to further harm the victim. One of the sub-forms of this type of violence is sextortion, which is the threat of publishing explicit materials (information, photographs) for the purpose of extorting money, or humiliating the victim.

Other types of abuse in digital surroundings

In addition to the above-listed types of digital abuse/harassment/ violence, in modern literature we often find terms such as trolling (continuous posting of, mostly negative, comments), DoS attacks (Denial of Services - overloading/attacking a network to cause a system to crash), SWATTing (fake reports of fires/bombs to the police and other institutions, in order to cause panic and fear).[28] These concepts certainly require a deeper and more detailed analysis, however, having in mind our thematic focus, we will only enumerate them here.

---

[28] Online Violence: Listening to Children's Online Experiences; Teresa Sofia Pereira Dias de Castro (University of Minho, Portugal) and António José Osório (University of Minho, Portugal); 2005.

Findings of the analysis

"Human trafficking has been on the rise for years, which only serves to show that traffickers are adapting to changes in society faster than those who should prevent them from committing it."

Ana, 20, member of the Advocacy Group of girls and women, human trafficking survivors

Information and communication technologies, as well as digital sphere, have greatly influenced the way in which human trafficking occurs today, as well as how victims can be reached. A research of the US nongovernmental organization "Polaris Project" from 2018 focuses on the analysis of the role of social media and their impact on human trafficking. The findings show that victims are recruited through these media and the Internet, that traffickers's activities are expanded in this way[29] and that victims are controlled through restrictions on the use of media, impersonation, as well as through other abuses.[30]

Human trafficking and abuses in digital surroundings

This analysis considers forms of abuse in digital surroundings that can be directly linked to the criminal offense of human trafficking. In that context, it is particularly important to highlight three key phases of

---

[29] In relation to this, there are as much as 750,000 predators on the Internet at any given moment! Available at: https://tijana.rs/trgovina-ljudima-internet-sajber-jazbine/.

[30] Available at: https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf.

trafficking: recruitment, transit and exploitation.[31] Following are the findings in relation to perpetrators of various abuses, prevalence of certain types of abuse in digital surroundings, and types of abuse in the context of human trafficking.

Perpetrators of abuse in digital surroundings

Results of this analysis show that, in terms of perpetrators of abuse in digital surroundings, most dominant is the violence committed by an unknown person. In this context, an unknown person is considered a person whom the victim first met via the Internet. In the second place are perpetrators known to the victim, i.e. partners (20%), wider social group (8%), family members (8%), and helpers (4%).[32]

Perpetrators of abuse in digital surroundings

Helper 4%
Family member 8%
Wider social group 8%
Partner 20%
Acquaintance 20%
Unknown person 40%
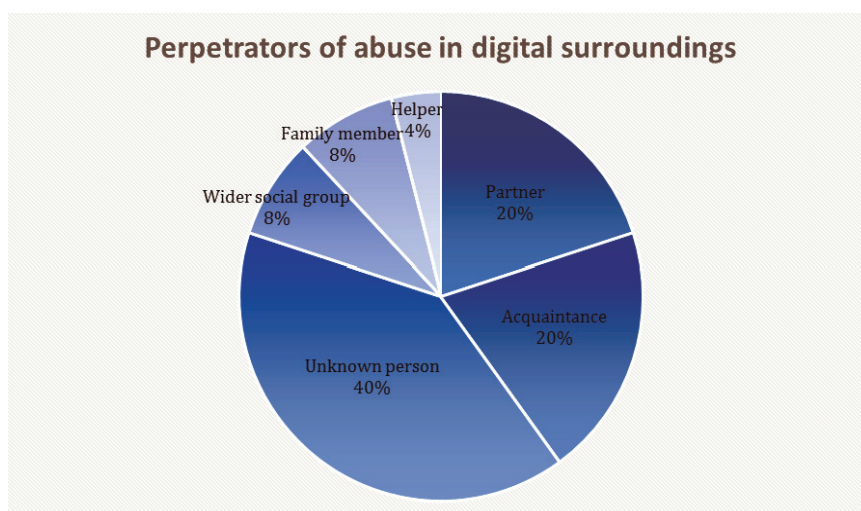
Graph 1: Perpetrators of abuse in digital surroundings

---

[31] Available at: Republic of Serbia, Ministry of Justice, https://www.mpravde.gov.rs/sr/tekst/17551/sta-je-trgovina-ljudima.php

[32] Respondents cited only members of the police as helpers who perpetrated abuse in digital surroundings.

Perpetrators of stalking in digital surroundings

"Stalking encompasses two forms of violence. On the one hand, it endangers physical freedom of a person, while simultaneously causing permanent psychological consequences."

*Sara, 24, member of the Advocacy Group of girls and women, human trafficking survivors*

Stalking has been recognized as one of the most common types of abuse in digital surroundings by the majority of respondents. Criminal Code defines stalking as an act in which someone "unauthorizedly follows or undertakes other actions in order to physically approach a person against their will; against the will of another person seeks to establish contact directly, through a third party, or through means of communication; abuses personal data of another person or a person close to them to order goods or services; threatens life, body or freedom of another person or a person close to them; undertakes other similar actions in a way that may significantly endanger personal life of the person against whom the actions are taken".[33]

For the purpose of this analysis, stalking is viewed only from the perspective of stalking in digital surroundings, which means that cited data illustrate the number of human trafficking victims who have experienced stalking through information and communication technologies (ICT). Stalking was also analyzed in relation to the perpetrators.

Of the total sample of persons who survived abuse in digital surroundings in the context of human trafficking, 55% also experienced stalking. In relation to the perpetrators, stalking was most often committed by acquaintances. In the context of this analysis, acquaintances are persons whom the victim knows, i.e. with whom they have established communication in real life. Perpetrators of stalking were also family members (23%) and partners (18%). Further findings show that unknown persons committed stalking in 9% of the cases, and helpers in 5% of the total sample.

---

[33] Article 138a of the Criminal Code.

Perpetrators of stalking in digital surroundings

- Family members 23%
- Acquaintances 45%
- Partners 18%
- Unknown persons 9%
- Helpers 5%
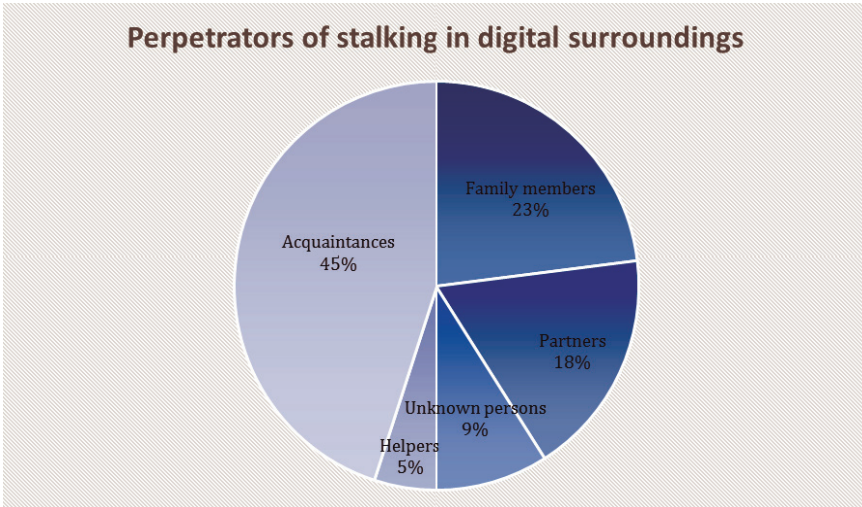
Graph 2: Perpetrators of stalking in digital surroundings

In this regard, it is significant to mention an extensive research on this topic conducted by the European Agency for Fundamental Rights in 2014.[34] The research included 42,000 women from 18 to 74 years of age, and showed that 18% of respondents had experienced some form of stalking, as well as that women from 19 to 29 years of age were at increased risk of digital stalking. The fact that all these data, regardless of their individual differences, probably do not even come close to the real situation can be concluded from the findings of another relevant research "The Dark Figure of Stalking" from 2017, which presents a worrying fact that stalking is not reported in 50% to 80% of the cases worldwide.[35]

---

[34] European Union Agency for Fundamental Rights, "Violence against women: an EU-wide survey," Publications Office of the European Union, Luxembourg 2015, 81.

[35] P. Brady, M. Nobles, "The Dark Figure of Stalking", Journal of Interpersonal Violence, Vol. 32, 2017, 3152.

Threats in digital surroundings and their content

"A threat that safety of a person will be endangered by attack on the life or body of that person, or someone close to them, is punishable by the Criminal Code as a criminal offense of endangering safety. Elements of other criminal offenses can also be found in a threat of violence, particularly in the area against human and civil freedoms and rights."

Special Prosecutor's Office for High-Tech Crime of the Republic of Serbia

In relation to the topic of this analysis, threats in digital surroundings are considered to be all types of messages (text, images, voice messages, calls) that aim to intimidate, harass, and harm another person. Defined as digital threats, all threats received through ICT have been considered in this context. Of the total number of human trafficking victims who survived some form of abuse in digital surroundings, 65% of them also received digital threats. Threats were most often aimed to intimidate the victims to change/withdraw report/statement or testimony in criminal proceedings (59%). Threats also referred to publication of a content created in a private context (29%), and direct threats to life and health, aimed to endanger safety (12%).

Content of threats in digital surroundings

- Direct threats to life and health aimed to endanger safety 12%
- Threat that a private content would be published 29%
- Intimidation of victims to change/withdraw report/statement or testimony 59%
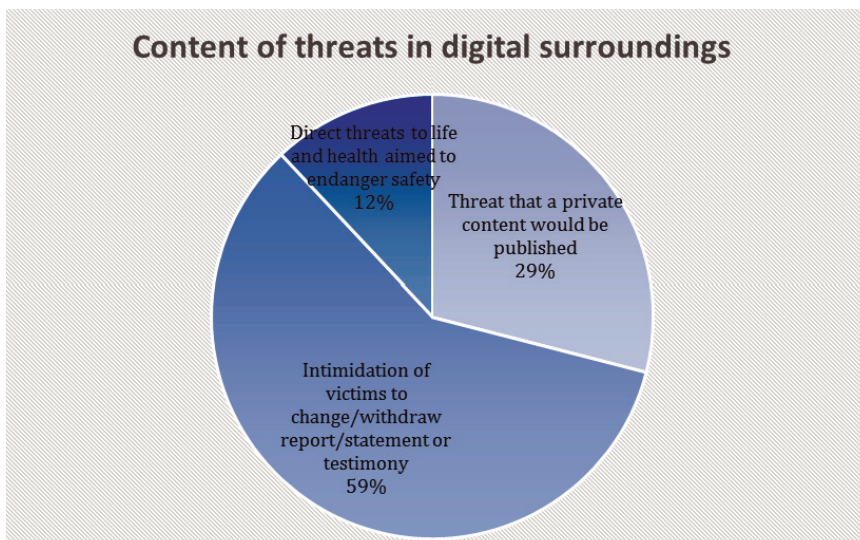
Graph 3: Content of threats in digital surroundings

Such a form of abuse in digital context can be described as a behavior aimed at intimidating and/or blackmailing a victim who participates in criminal proceedings, most often as the injured party/witness[36] to withdraw from further participation or change/withdraw previously given statement/testimony. At this point, it is important to note that threats in this context do not imply exclusively an explicit threat in the criminal law sense, but a range of behaviors and activities that are aimed at pressuring the victim.

Reporting these and similar situations usually entails initiating a separate procedure for an offense from the Criminal Code, preventing and obstructing evidentiary actions,[37] however experiences of respondents show that unless a direct threat was made in relation to a request to withdraw/change a statement/testimony, this form of violence is difficult to prove.[38]

Recording and distribution of digital content without consent

The act of committing this criminal offense[39] in the form of abuse in digital surroundings, includes content that was recorded and further distributed without the consent of an adult. In this analysis, any distribution of content in which actors are minors, and for which the consent of the child/[40] guardian/parent has not been obtained in advance, is considered unauthorized and represents a criminal offense. When it comes to pornographic, explicit and criminal content in which the actor is a child, any recording and further distribution can be considered

---

[36] Criminal Code of RS, Article 2, para. 11.

[37] Criminal Code of RS, Article 336.

[38] Available at: https://www.vreme.com/cms/view.php?id=342947.

[39] Criminal Code of RS, Article 145: Whoever publishes or publicly presents another's text, portrait, photograph, film or a phonogram of a personal character without consent of a person who has drawn up the text or to whom it is related, or without consent of the person depicted on the portrait, photograph or film or whose voice is recorded on a phonogram, or without consent of the person whose consent is mandatory by law and thereby significantly violates the private life of that person shall be punished...

[40] Article 16 of the Law on Personal Data Protection regulates consent of a minor in relation to the use of information society services.

unauthorized, as it can harm the child's reputation, development, and well-being.

Of the total sample observed, 63% of beneficiaries suffered this form of abuse in the context of human trafficking. Regarding the content that was distributed, in most cases (64%) it was content with elements of pornography, while in 20% of cases information and content were distributed to reveal a location and/or identity of the victim in a way that endangers their safety. In 16% of the cases, private content, such as photographs and messages, was distributed without authorization, but also without an element of explicitness.

In the context of human trafficking, these contents may have previously been made by deceiving or forcing the victim to participate in their creation. On the other hand, as already mentioned, consent of the victim in the context of human trafficking does not abolish the perpetrator.

Recording and further distribution without consent

Private content (messages, photographs) without an element of explicitness
16%

Content which reveals the location and/or identity of the victim and endangers their safety
20%

Content with elements of pornography
64%
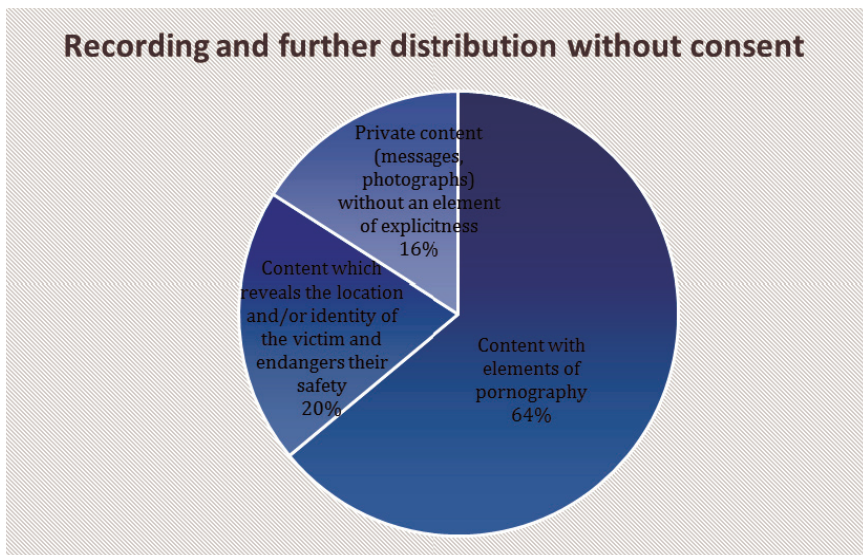
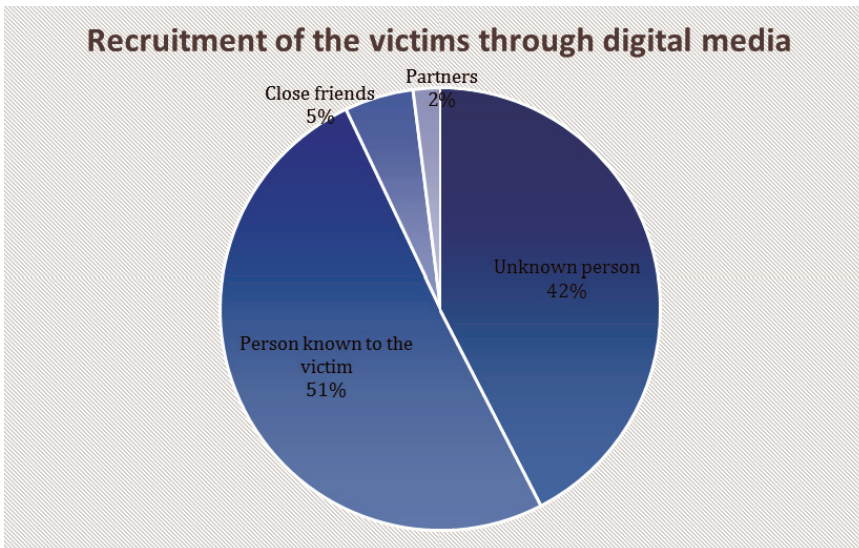Graph 4: Recording and distribution of digital content without consent

Recruitment of the victims through digital media

Recruitment represents the first stage in human trafficking. There are different ways of recruiting. In the last ten years, the most common has been impersonation for the purpose of recruiting via the Internet.[41]

In the total sample examined, we conclude that 30% of human trafficking victims were recruited on the Internet. Of this percentage, 70% of girls and women were recruited for the purpose of further exploitation (human trafficking), while 30% were recruited in order for some other form of violence to be committed against them (rape, robbery, physical violence...).

Regarding the perpetrators of recruitment for the purpose of further exploitation, the analysis of the obtained answers shows that in the majority of cases they were persons known to the victim (51%), followed by unknown persons (42%), and to a smaller extent close friends (5%) and partners (2%).

An example of recruitment through ICT are certainly false advertisements, but also getting to know via the Internet, false business proposals offered by acquaintances, financial assistance, and the like, which in the following stages turns into exploitation of the victim for the purpose of gaining benefit.
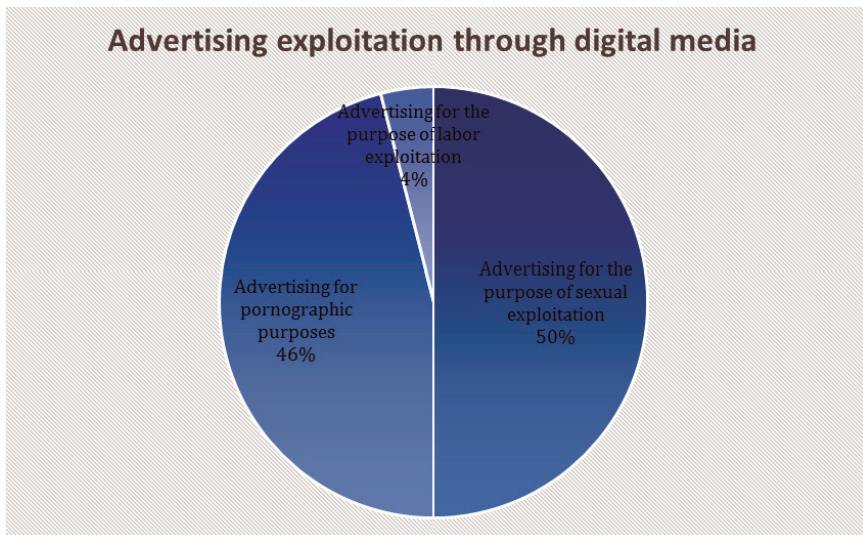

Graph 5: Recruitment of the victims through digital media

---

[41] Available at: https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf.

Advertising exploitation through digital media

Observing the forms of exploitation, we analyzed the number of cases where exploitation was advertised in digital space. Obtained answers lead to a conclusion that out of the total sample 40% of human trafficking victims were exposed to online advertising during the exploitation. Of this percentage, 46% were exploited for pornographic purposes, 50% were exploited for sexual purposes, while 4% had their work advertised during the situation of labor exploitation.

Advertising exploitation through digital media

Advertising for the purpose of labor exploitation 4%

Advertising for pornographic purposes 46%

Advertising for the purpose of sexual exploitation 50%

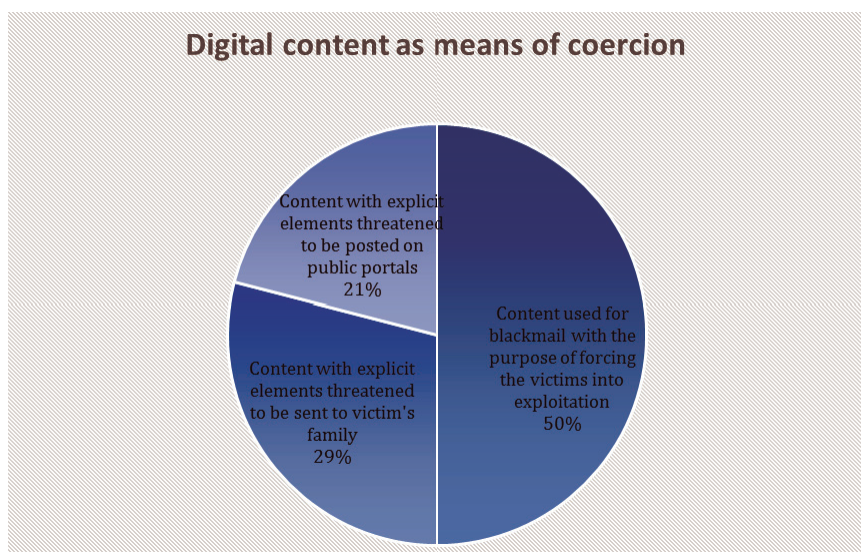Graph 6: Advertising exploitation through digital media

Digital content as means of coercion

"In the context of coercion in a situation of human trafficking, the content trafficker owns may represent the source of his power."

Marijana Savić, director of "Atina"

Of the total sample, 50% of human trafficking victims stated that, while they were in a situation of exploitation, the person who trafficked them possessed content used to blackmail them and force them into various types of exploitation. As many as 29% of the total number of respondents stated that they were blackmailed by being told that the explicit content they are in, or information about them, will be sent to their family members, and 21% of them were threatened that the content would be published on public portals.

Digital content as means of coercion

- Content with explicit elements threatened to be posted on public portals 21%
- Content with explicit elements threatened to be sent to victim's family 29%
- Content used for blackmail with the purpose of forcing the victims into exploitation 50%

Graph 7: Digital content as means of coercion

Other forms of abuse victims have been exposed to in digital surroundings

Types of abuse in digital surroundings presented at the beginning of this analysis were examined in the overall sample of respondents, without a necessary correlation with the situation of human trafficking. Of the total number, 15% of girls and women stated that they were also victims of impersonation (imitation of another person), while catfishing was present in 5% of the cases, and doxing (targeting) in 3% of these cases. Furthermore, cyberbullying was experienced by 32% of respondents, while 57% of surveyed trafficking victims experienced cyberstalking. When it comes to hacking (unauthorized access to other people's data), 42% of them encountered this phenomenon. Digital abuse recognized as vengeful distribution of explicit content, such as videos and photographs with pornographic elements (revenge porn), but also messages (sextortion), was experienced by 31% of respondents.
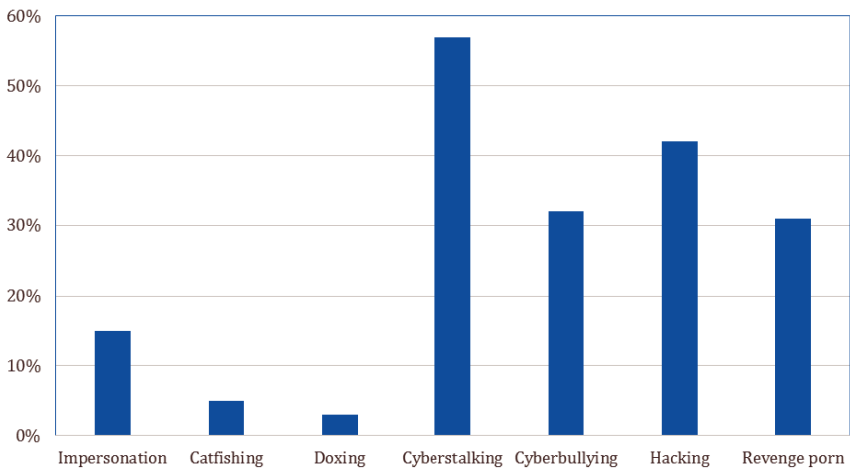
Graph 8: Other forms of abuse in digital surroundings

Conclusion

The results of this analysis show that human trafficking victims most often suffer violence in digital surroundings from strangers, i.e. persons they meet on the Internet. However, according to their testimonies, stalking is the most common form of violence in digital surroundings, while the stalker is in most cases a person whom they met in real life. In the second place, human trafficking victims are most often faced with threats in digital surroundings; i.e. threats aimed at intimidating them to change or withdraw a previously given statement in criminal proceedings. During the period of exploitation, human trafficking victims (including children) were exposed to recording and further distribution of content with elements of pornography, without their consent. Observing the stages of human trafficking, a number of respondents were recruited through digital media, while 30% of them were recruited in order to have other forms of violence committed against them (rape, physical violence, robbery, etc.). Recruitment for the purpose of exploitation was most often carried out by persons known to the victim. In the exploitation phase, more than half of the surveyed victims experienced advertising for the purpose of sexual exploitation through digital media. Looking at the ways in which coercion was carried out, half of the victims in the sample stated that traffickers had digital content which they used to blackmail them and force them into various forms of exploitation. When it comes to other forms of abuse in digital surroundings which human trafficking victims experienced during and after the situation of exploitation, and even after the court proceedings ended, cyber stalking, hacking and cyberbullying were highlighted as the most common forms of violence. It is important to note that human trafficking victims were not immune to other forms of abuse, such as vengeful distribution of explicit/pornographic content (revenge porn), sextortion, doxing, etc.

Finally, in order to fully understand this analysis, it is important to know the context in which human trafficking victims live even after exiting the trafficking situation, and even years after the court rulings; and that is the fear of using digital media - anything from opening a profile on social networks with their full name, posting photographs or videos that reveal their place of residence; posting photographs with people close to them, so as not to expose them to potential revenge of traffickers; taking photos in public places, events; answering calls from unknown numbers, and the like.

In addition to the forms of violence which have been reviewed in the context of this analysis, we believe it is important to mention observed trends, such as cyber trafficking, i.e. live streaming of sexual exploitation. This form of cybercrime includes human trafficking, i.e. live transmission of sexual exploitation. Cyber trafficking deserves to be found in the plans and strategic documents in the field of protection of human trafficking victims in the context of the fight against human trafficking and the transition to the online sphere of functioning and interaction, particularly fueled by the global COVID-19 pandemic.

This type of abuse differs from other forms of human trafficking in that traffickers are abusing victims both in the real and digital space, forcing them to perform sexual acts by themselves or with other people, and keeping them in sexual slavery. Another form of such abuse is rape in front of the cameras, which is often committed by a trafficker or another person who paid the trafficker for it. This form of human trafficking can take place in real time, or it can be recorded and posted on the internet as a type of pornographic content. Similar cases have already been recorded in Serbia, in which scenes of sexual abuse of a child are broadcasted through "cyberdens"[42] live and with monetary compensation.

There is still not much data on the prevalence of this form of human trafficking in the world. Detection of cyber trafficking cases is still under development and there is a lack of legal solutions to combat this type of crime. It is estimated that this is the most lucrative form of human trafficking, as once a video is posted on the Internet, it can reach thousands of paid views. Also, paying a trafficker for someone's exploitation is accompanied by development of online transactions and payments in cryptocurrencies that can further "accelerate" ex-

---

[42] Cyberden represents digital abuse of children through prostitution or pornography. Human traffickers and other criminal groups recruit children of primary and secondary school age, from poor and deprived families, as well as children from minority groups.

ploitation in the unregulated zone of the economy. Finally, global crisis caused by the COVID-19 pandemic, experts believe, will additionally affect the expansion of this form of human trafficking by affirming and accelerating the shift of demand to the digital sphere. Organisation Atina will continue to monitor and analyze these and similar phenomena in the future.

Some governments have launched advocacy and media campaigns aimed at raising awareness of this crime. However, at the national and international level, crimes in digital space are not recognized in equal way as those committed in the physical space where every criminal act is precisely defined without hesitation. Civil society organizations, on the contrary, believe that no distinction should be made between violations of rights in digital and physical space.

Sources

1. Anthony Brittany, "On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking", Polaris, 2018
https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking-Social-Media.pdf

2. Brady Patrick Q, Nobles Matt R, "The Dark Figure of Stalking", Journal of Interpersonal Violence, Vol. 32, 2017, 3152.

3. C. S-W, "What doxxing is, and why it matters", The Economist explains, 2014.
https://www.economist.com/the-economist-explains/2014/03/10/what-doxxing-is-and-why-it-matters

4. European Union Agency for Fundamental Rights, "Violence against women: an EU-wide survey", Publications Office of the European Union, 2015

5. Criminal Code, "Official Gazette of RS", No. 85/2005, 88/2005 – amended, 107/2005 – amended, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019.

6. Mullan, Eileen, "What is Digital Content?", EContent Magazine, Information Today Inc, 2011

7. Krivokapić Danilo, Petrovski Andrej, "Cybercrime and police cooperation in the EU", in publication "Guide through cooperation in internal affairs of the European Union", Belgrade Center for Security Policy, 2016

8. Republic of Serbia, Ministry of Justice, https://www.mpravde.gov.rs/sr/tekst/17551/sta-je-trgovina-ljudima.php

9. Pen America, Defining "Online Harassment": A Glossary of Terms. https://onlineharassmentfieldmanual.pen.org/defining-online-harassment-a-glossary-of-terms/

10. Perry Jennifer, "Digital stalking: A guide to technology risks for victims", Network for Surviving Stalking and Women's Aid Federation of England, 2012. https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/onlinesafety/

11. Pereira Dias de Castro Teresa Sofia, Osório António José, "Online Violence: Listening to Children's Online Experiences", University of Minho, 2005.

12. Recommendation CM/Rec(2018)7 of the Committee of Ministers to member states on guidelines for respecting, protecting and exercising the rights of the child in digital surroundings, Council of Europe, 04/07/2018

13. Constitution of the Republic of Serbia, "Official Gazette of RS", No. 98/2006

14. Law on the Organization and Competences of the State Organs in Combating Organized Crime, "Official Gazette of RS", No. 61/2005 and 104/2009.

15. Law on Personal Data Protection, "Official Gazette of RS", No. 87/2018.

16. Law on Public Information and Media, Official Gazette of RS", No. 83/2014, 58/2015 and 12/2016.

17. Law on Electronic Media, "Official Gazette of RS", No. 3/2014 and 6/2016.

18. Rulebook on the Protection of the Rights of Minors in the Provision of Media Services, "Official Gazette of RS", No. 25/2015.

19. Rulebook on the Protection of Human Rights in the Provision of Media Services, "Official Gazette of RS", No. 55/2015.

20. GRETA report on the implementation of the Council of Europe Convention Against Human Trafficking for Serbia: second evaluation round adopted on November 24, 2017, published in January 2018 https://rm.coe.int/greta-2017-37-frg-srb-srb/16807809fe

21. Action plan for negotiating Chapter 23 https://www.mpravde.gov.rs/tekst/9849/finalna-verzija-akcionog-plana-za-pregovaranje-poglavlja-23-koja-je-usaglasena-sa-poslednjim-preporukama-i-potvrdjena-od-strane-evropske-komisije-u-briselu-.php