

CYBERCRIME OF TRAFFICKING IN PERSONS: AN ANALYSIS OF THE PROTECTION OF FUNDAMENTAL RIGHTS IN SOCIAL NETWORKS

Marco Aurélio Farias da Silva¹

Vanessa Alexsandra de Melo Pedroso²

Abstract

The purpose of this study was to investigate how human trafficking occurs in the digital age, exploring the use of victims' data obtained from social networks by traffickers. Despite the security mechanisms of big techs, crimes persist online. In this research paper, we sought to understand how digital platforms are used for this crime, examining how sensitive data is exploited, identifying manipulation techniques, and suggesting preventive measures. The central issue was to identify how human trafficking materializes based on information on social networks. The initial hypothesis pointed to the inefficiency of operational protection in cyberspace. The general objective was to understand the use of social networks in the commission of this crime. Specifically, the objectives were to analyze the exploitation of sensitive data, identifying manipulation techniques, and suggesting prevention. The methodology was dialectical at the exploratory level, with a literature review and a documentary analysis on fundamental rights, criminal dogmatics, and journalistic reports. Results indicated the need for continuous awareness about the risks of using these technologies and demanded state action. In the conclusion, the aim is to broaden the understanding of the phenomenon, emphasizing the development of technological tools in order to guarantee individual rights.

Keywords

Crime of trafficking in persons. Personal data protection. Privacy rights.

¹ PhD. Candidate, UNICAP - BR

² Professor, UNICAP - BR

Summary

1. Introduction; 2. The crime of trafficking in persons; 2.1 Internet offers and use for social networking; 3 Goals for capturing sensitive data; 3.1 Personal data available on telecommunication platforms; 3.2 Human trafficking on internet-mediated social networks; 3.2.1 An illustration of Brazilian reality; 4 Closing statements.

1 INTRODUCTION

Human trafficking for purposes of slavery started to be prohibited in Europe in the 19th century, notably in England in 1807 (UK, 1807), however it spread to other parts of the world. Nevertheless, other purposes and ways began to appear with the development of new technologies, which demanded new confrontation strategies, aiming for the best adequacy to the environment in which people are more susceptible to the actions defined as criminal acts.

During the time of the great navigations, mainly when the colonization of the Americas has given a boost to economic development in agriculture, slavery came to be combated for it was a measure to reduce production costs, although William Wilberforce's work in defense of human dignity is recognized in the English Parliament in the 19th century (*Encyclopaedia Britannica*, 2020).

Nonetheless, the fact is that Europeans started to face such practices for they caused a seemingly unfair competition for the agricultural producers from the Old Continent, and the signature and implementation of international treaties in order to extinguish the traffic of enslaved people from Africa to the Americas was one of the

three strategies advocated by the economic sector (Willians, 1944, p. 136), with the regulation and inspection of the maritime means of transportation being the effective way to prevent authorities from confronting this exploitation of man by man, especially in Brazilian territory, even though in this land slavery remained legal until 1888. Concerning other nations, during the 20th century, The United Nations (UN) has created dialogues and has adopted conventions and additional agreements to combat trafficking in persons, although it has not yet elaborated specific regulations to hold governments accountable for the conduct carried out by the media, notably with the use of information and communication technologies (ICTs), that have been utilized on a global scale by the International Computer Network.

The use of the ICTs meets various service modalities in cyberspace, with the concern about information released to the public not always being an object of moderation, therefore, as there is a lack of control and inspection dynamics regarding the possibility of private information collection in profiles or documents that circulate in the virtual environment, which would be intended to protect the personality rights holder.

The internet environment is, without a doubt, essential to the current society and a mediator of various social networks, with the same domain of the big companies when providing ICTs that should offer a safe environment to its users, and the promotion of public and private preventive campaigns, by means of inspection and accountability for the provision of services by public agencies, in order to reduce the possibilities of personal data capture, because the absence of monitoring interferes directly with the fundamental rights of the

people who socially interact in this space, that is, in digital citizenship, placing it in a vulnerable situation to criminal actions.

Thus, given the evolution and use of ICTs, already integrated into the diverse systems of our modern society, and if well used they can even contribute to the fight against crime, safeguarding personality, property and existential rights is what was intended to carry out this work under the perspective of identifying some already used strategies to capture individual profiles, registered on some available internet platforms, and used to violate the rights of users themselves.

Hence, in light of this context, despite security technologies already available by the big techs, there is a concern about what should be reported daily to all the people who interact socially via the internet, with the purpose of knowing at a minimum what the risks of capturing your personal information are, aiming to reduce risks for potential victims of human trafficking, and this is the reason why we ask: how the crime of trafficking in persons has occurred based on information contained on digital social media platforms?

Therefore, the main objective is to understand how these platforms were used to commit the crime under study; and, as specific objectives: to examine how sensitive data posted on some online platforms were taken advantage of by traffickers to deceive people; to identify internet user manipulation techniques; and, suggest prevention measures against these typical actions.

The rationale for this research derives from the rise of social networks on the Internet and, particularly with regard to personal information, it is important to note that the services offered on the dark web facilitate the recruitment of victims by human traffickers through the use of false promises, presentation of misleading visual information

(e.g. fabricated photos, false images), scams that prevent the victims from verifying the authenticity of the offer of these services.

The methodology comprises the dialectical method, based on a qualitative approach, with the exploratory research on the topic, drawing upon data collected from several scientific studies and journalistic reports, on which a literature review and a specialized document analysis, regarding the subject matter, were carried out.

Expected results were the organization of minimum information to disclose, in the academic and social spheres, the possible risks of criminal activity against those people who interact on social media networks in the online environment, regarding their personal data posted on profiles or messages.

The first chapter addressed the presentation of the crime within the national arena, as well as the scientific contributions regarding how the internet started to be used by major corporations and later became the main interaction channel on social networks, that is, how its offer turned into a way of attracting social network platforms, which began to be a way of entrepreneurship due to profile monetization, that was also utilized illegally in one of the means of communication of great importance and usage nowadays.

The second chapter discussed the possibilities of user personal data capture, featuring the main illegal and criminal usage; and some contributions for the minimum secure use of services made available to the public on the World Wide Web.

The conclusion considered that the risks involved on digital platforms should not be synonymous with prohibition of its use, however it demands the constant elaboration of user complaint analysis in order to have their fundamental rights safeguarded, as well as the

improvement of protocols based on cases of trafficking in persons mediated by these technologies, as a way to prevent these crimes.

2 THE CRIME OF TRAFFICKING IN PERSONS

The Brazilian penal code provides, in Art. 149-A³, that the crime of trafficking in persons violates the principle of human dignity, distinctively regarding its individual freedom, and it is initiated by one of the following conducts: ‘agentic, grooming, recruiting, transporting, transferring, purchasing, harboring, or receiving persons’; connecting them to one of the following means: ‘serious threat, violence, coercion, fraud or abuse’; to achieve one of the following goals on the victims: ‘remove their organs, tissues or body parts; subject them to conditions analogous to slavery; subject them to any type of servitude; illegal adoption; or sexual exploitation’ (Brasil, 2016).

For the legal definition of this crime, the Brazilian criminal legislator stemmed from the concept of the crime in study provided by the

³ In Brazil, the crime of trafficking in persons is provided for in Art. 149-A of the Criminal Code:

Art. 149-A. Provide agency services, groom, recruit, transport, transfer, purchase, harbor or receive persons, through serious threat, violence, coercion, fraud or abuse, with the purpose of:

I – remove their organs, tissues or body parts; II – subject them to conditions analogous to slavery;

III - subject them to any type of servitude; IV -illegal adoption; or V – sexual exploitation.

Sentence - imprisonment, from 4 (four) to 8 (eight) years, plus a fine. [...] (Brasil, 2016).

Palermo Protocol, a UN-led initiative, in their strategy to combat organized crime. Nevertheless, carrying out a comparison between the texts of the Palermo Protocol and the law that created the Art. 149-A, differences between these two kinds of directives are found, especially concerning the means adopted, and Brazilian criminal law chose such a 'low-cut neckline style' that leaves the victim in a situation of insufficient protection (Farias da Silva, 2024, p. 125). In its definitions, the provisions of the Palermo Protocol are:

'Article 3

Definitions

For the purposes of this Protocol:

a) 'Trafficking in persons' shall mean the recruitment, transportation, transfer, harboring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude or the removal of organs;

- b) The consent of a victim of trafficking in persons to the intended exploitation set forth in subparagraph a) of this article shall be irrelevant where any of the means set forth in subparagraph a) have been used;
- c) The recruitment, transportation, transfer, harboring or receipt of a child for the purposes of exploitation shall be considered 'trafficking in persons' even if this does not involve any of the means set forth in subparagraph a) of this article;
- d) 'Child' shall mean any person under eighteen years of age (Brasil, 2004).

On the other hand, the Constitution of the Federative Republic of Brazil of 1988 (CFRB), in its Art. 5, item III, declares: 'no one shall be submitted to torture or to inhuman or degrading treatment' (Brasil, 1988); then, the arrangement provided for in Art. 149-A of the Penal Code also possesses a constitutional basis, because it is one of the ways to tackle the inhuman or degrading treatment, protecting the individual liberty chiefly, in addition to other distinct legal assets incorporated in each one of the purposes.

Moreover, human dignity is extremely important to the Brazilian legal order, since CFRB provides for its existence in Article 1, III (Brasil, 1988), fact that emphasizes the constitutional basis of the existence of

the criminal offense in a much broader way than the protection of individual freedom.

The consummation, or even the attempt, of the crime of trafficking in persons reveals a way to devalue the human being to an economically ratable object, and that is the reason why it became the scope of human rights, notably in terms of defending human dignity and fundamental rights.

Given its essential structure, the criminal offense definition contemplates basic elements: objective, subjective (intent), purposes and means, as mentioned at the beginning of this item, nevertheless, the means provided for in criminal law are interrelated, and therefore, strictly mandatory for the consummation of the crime, with such strictness being considered a requirement for typicality, but it is misguided according to Bitencourt (2016, p. 24), who attributes the deficiency of the legislative techniques to bias.

Nonetheless, the manner of execution of agenting, grooming, recruitment and buying people is not linked to a specific form of communication, that is, direct, indirect, face-to-face or remotely; as well as the related means: serious threat, coercion, fraud and abuse, which are not only connected to its existence in the typical action, but can also be committed remotely, fact that gives rise to the incident investigation whenever it has been committed in the field of telecommunications, especially through ICTs.

Under such circumstances, in explaining the Final Theory of the Action, Roxin (1997, p. 199) highlighted that its essentiality lies on systematic action structure, due to the fact that men anticipate their conduct mentally as they select the means, controlling the causal chain towards a specific goal.

To emphasize the importance of the resources to be used for the commission of the criminal offense in question, Rodríguez (2018, p. 40) pointed out that media use, initially, makes the victim convinced to consider the ideas of the trafficker, who will continue to dominate the victim for their purposes, practically nullifying the victim's autonomy.

With regard to means of communication for the performance of some conducts and their referred means, it is possible use telecommunication technologies, through the use of ICTs, especially when social networks are mediated by platforms available on the World Wide Web.

2.1 OFFER AND USE OF THE INTERNET FOR SOCIAL NETWORKS

The internet is the primary medium for marketing and running information and communication platform-based services, in which the social networks gain ground in interaction and dissemination, according to its rules and in accordance with the country laws.

The social networks constitute a methodology used by cultural anthropology and in sociological studies, but not exclusively, in order to analyze the relational structures of society, that is, how interactions and relations among people occur (Marteleto; Tomaél, 2005, p. 81).

It should be highlighted that the social networks precede the Internet era, and they can be recognized by means of two elements: their actors (people, institutions or groups, the network node) and their connections, ways of interaction or social ties; then, the expression

social network follows the metaphor from the anthropologist Alfred Radcliffe-Brown's perspective, utilized in the analysis of connection patterns that are built in a social group (Recuero, 2009, p. 24).

The concept of social network can be extracted from Moreno (1934, p. 10), who, after sociological studies with the application of the sociometric method, identified the social relations from the children generational group, progressing in his research for other social groups, systematizing the observation about the network communication.

As technology evolved, social networks shifted to electronic social media, which are digital internet-based platforms that enable the creation and sharing of information and contents by people and for people, who are, at the same time, producers and consumers of information (Torres, 2009, p. 113).

While the purpose of social media interactions is intended to be lawful, it cannot be ignored that such interactions can serve as a means to, for example, lure the victim of the crime of trafficking in persons, even if it appears to offer merchandise sales services or people recruitment.

However, Baudrillard (1997, p. 18-19) expressed concern over generative artificial intelligence (AI), calling attention to the consequences of hypercommunication as a landmark of the post-contemporary era with the main emphasis on shifting human control to a neural network of intelligent machines, which will be able to command the post-real reality autocratically. The highlight is, without a doubt, the potential of generative AI usage based on information posted on internet communication platforms.

The increase in offerings from the most varied platforms on the internet has facilitated rapid public interest in accessing them, with

the possibility of using some free services subject to prior registration, generating the user profile, and the same space for communication and services was rapidly targeted by criminal organizations, which even utilized the best-known social media platforms, for example Facebook, Twitter, renamed to X, and WhatsApp, which are the preferred tools of criminal agents (Rhodes, 2017, p. 23).

When analyzing the rise of the internet in the social environment, Hannigan (2014) noticed that this development not only provided humanity with fast access to information, but also enabled faster, more efficient operations for organized crime, making networks the preferred environments for the actions of criminals and especially terrorists. Social networks include Facebook, Twitter (currently known as X) and WhatsApp.

A sample of how these criminal actions are taking place is the example of pornography, especially child pornography, a real 'industry' creating the conditions for the crime of human trafficking worldwide. According to estimates, fifty years ago, if someone wanted to buy a magazine with pornography, they would have to go to the crime scene or the corner store to buy it, but today they can access pornographic material on social media from anywhere, including their own home (Rhodes, 2017, p. 23).

Rhodes (2017, p. 24) indicates that the internet, through its sales platforms, can be a chosen place for the actions of human traffickers who, by means of stratagems, lead their victims into error, luring them into captivity, being able to use services such as Backpage, Craigslist, Facebook and diverse chat rooms, some of which are dedicated to intimate dating and companionship services.

The platforms available on the internet can also be used by traffickers as a tool of apparent help in obtaining a job placement, but in reality, they aim to recruit their victims for another form of exploitation. In these cases, the human traffickers use social media to gather information about the victims and to create fake profiles in order to generate virtual relationships with them (potential victims), whether for the purpose of sexual exploitation, servitude, or forced labor in slave-like conditions (Rhodes, 2017, p. 25).

Pimentel (2023, p. 41) has pointed out that, in the digital environment, people no longer feel watched and they are acting without hesitation; consequently, individuals are sidelining their own privacy and are being tracked by algorithms capable of capturing information and prescribing human behavior, by knowing the users' profile so well, they start receiving the information they have always dreamed of, taking them away from reality, leading them to pseudo-empowerment and social stardom, causing a merely reactive and robotic behavior of posting, reading, and commenting on other users' social media posts.

In order to better describe how surveillance occurs, Pimentel (2023, p. 69) emphasized that the interaction with the internet through social media, which represents the majority of the cases, enables the internet users to be appreciated and influenced because their posts, audios, pictures, videos can be captured and, with such elements, their data and metadata can be utilized, revealing their preferences based on the accumulation of data in gigantic databases (big data), in which there is data processing, the raw material for business, political, religious, and ideological actions, as well as for organized crime.

Human traffickers have been treated like 'brilliant social engineers' by Mitnick e Simon (2003, *passim*), for managing to gain their victims'

trust by accessing private information, because they crafted seemingly innocent questions, offering to assist the victim, who started feeling understood and developed a sense of intimacy with their tormentor, but it was actually a trap. The entire logic of 'social engineers' was built based on the dreams and desires already revealed by victims in the information posted on platforms they previously accessed. Therefore, the help becomes apparently logical and safe to the victim. There are also cases in which the traffickers use information, intimate or compromising photos to blackmail them. It is through manipulation of the victim that traffickers achieve their intentions (Rhodes, 2017, p. 24-25).

Despite the warnings about the risks described so far, it is important to highlight that the web environment reported is the one that can be accessed by search engines like Google e Bing, in other words, it is where most common users' daily activities occur; users lacking knowledge of how data is transmitted and accessed on the global computer network.

The digital environment permeates the world that interacts in the form of a large virtual network, and its inhabitants are organized into different layers of indexed communication, platform offered on the web, or unindexed, located at the deep web level. The web receives, in general, the social media platforms, or rather, it is located in an indexed environment that observes logical communication protocols, in turn, standardized by hypertext, and that is how 'social media has not only become a perfect ecosystem of social incorporation and integration, but also a perfect ecosystem of identitarianism, tracking, surveillance and control of its users' (Pimentel, 2023, p. 78).

It is widely estimated that a part of the internet known as deep web is 500 times larger than the surface web, and it contains the non-searchable part of the web. Below this layer, there is another subsection of the web called the dark web, which is a portion of the internet kept intentionally hidden and provides perfect cover for illegal activities, including the crime of trafficking in persons (Rhodes, 2017, p. 25).

The great potential of the dark web is that it almost guarantees the anonymity of its users with the application of multi-layer encryption technology called onion encryption, named for the ‘onion’ domain and for working in layers like an onion, where each of these layers hide the user’s computer identification address, also known as Internet Protocol (IP); it is encrypted and moved to another volunteer server to generate the next layer. With this procedure, since the destination website receives only the last IP address in the routing process, the former never knows who it is initially communicating with; actually, this technology should be used to ensure that certain professionals, such as journalists and government agents, do not put themselves at risk in the line of duty, but, unfortunately, it has come to be used for committing crimes (Rhodes, 2017, p. 25).

Technological surveillance, based on access to and control of the personal data of internet users, according to Pimentel (2023, p. 73-74), is superior in efficiency to that of biopower, practiced ostensibly by human beings with the use of disciplinary and regulatory mechanisms, such as the panopticon, explained by Foucault⁴.

⁴ Cf. FOUCAULT, Michel. *Discipline and Punish: The Birth of the Prison*. Trans. Raquel Ramalhete. Petrópolis, Vozes, 1998.

According to Farahany (2023, p. 18), in no time the last domain of privacy can be lost, because new technologies are already capable of collecting our data, going beyond that, they have reached people's brains under the guise of making them faster, more efficient, safer, healthier, less stressed and even more spiritual, through the simple act of granting access to their web search history to free, powerful technology-driven internet browsers, which may want to share the data the devices have collected.

Rhodes (2017, p. 26) revealed some advancements in developing tools to combat cybercrime on both the surface web and dark web, as was the case with *Spotlight*, which is a tool to collect publicly available internet information, for analysis and use to assist law enforcement authorities, focusing on child trafficking data; thus, observing the possibilities of capturing information in the virtual environment, one now proceed to analyze the purposes for collecting personal or sensitive data.

3 PURPOSES FOR CAPTURING SENSITIVE DATA

Statistical models require high-quality data collection to achieve an objective application, regardless of whether that application is illicit, as used legally and successfully in US baseball, known as *Moneyball*, since this sport have attracted mathematicians throughout its history, during decades, science facts were placed on the back of baseball cards. From the 1980s, statisticians began investigating what these numbers, along with a new avalanche of others, actually meant: what victories

symbolized and how business executives could maximize the success of their investments (O'Neil, 2020, p. 20).

Although the *Moneyball* model represents a statistical approach in fields formerly governed by instinct, as claimed by O'Neil (2020, p. 8), it provides a useful contrast to toxic models, and coined the term Weapons of Math Destruction (WMDs), which are emerging rapidly in many areas of modern life (O'Neil, 2020, p. 21). And, based on the use of WMDs, other applications began to emerge on a large scale in an illegal way of acting in the virtual environment.

WMDs have already caused problems in the *U.S. News Best Colleges* ranking, because for-profit colleges stood by the most vulnerable population, and the internet used to give them the perfect tool for this; an example was the investment of more than US\$ 50 million in Google advertisements only, among which the University of Phoenix targeted the poor with the bait of social mobility, conveying a message rife with implicit criticism that these individuals were not doing enough to improve their circumstances and achieve results, since between 2004 and 2021 registrations tripled, and the for-profit sector, at that time, accounted for 11% of university students in the USA (O'Neil, 2020, p. 74).

Considering that these campaigns are online, the promotion speeds up, because the internet provides advertisers with the largest laboratory that has ever existed for consumer behavior research. An example can be feedback, in which each disclosure reaches the public within seconds, faster than conventional means; therefore, in hours, an advertising campaign can reach the target audience with nearly immediate returns (O'Neil, 2020, p. 80).

That's why, thanks to the internet, people worldwide have been generating quadrillions of words about their lives and work, friendships, ways of doing business and, in doing so, the most extensive training collection for natural language machines is being built involuntarily, as paper gives way to email and social media, machines are able to study our words, compare them to others, and deduce something about their context (O'Neil, 2020, p. 81).

Nonetheless, this whole advertising process can have a component like a WMD, which becomes harmful to the lives of many people, particularly those who used internet services, and begin to receive this type of predatory advertisement, as well as in the case of North American Universities, the damage does not begin until students start taking out large loans to pay tuition and other costs (O'Neil, 2020, p. 84).

This was the perspective of using WMDs by for-profit colleges, in order to reach and deceive the most needy population, with the selling promise of education and a tantalizing glimpse of social mobility, plunging this population into even more debt, taking advantage of the urgent needs of poor families, their ignorance and aspirations, and then exploited them on a large scale, frustrating their aspirations, promoting hopelessness and discouragement, along with skepticism regarding the broader value of education (O'Neil, 2020, p. 86).

O'Neil (2020, p. 100) analyzed that justice cannot be calculated from a WMD, because its widespread use causes several injustices, and lectured: 'If you think of a WMD as a factory, injustice is that black stuff coming out of the smoke stacks. It's a type of toxic emission'.

Another example of how the WMDs can cause harmful results-personality tests were taken as a model, because they are seemingly

easy to bypass. Then, O'Neil (2020, p. 114) worked from the assumption that someone would answer the *Five Factor Personality Test*, starting with the question: 'Do you have frequent mood swings?'. In the beginning, it would be wise to answer 'very imprecise'. Another question: 'Do you get irritated easily?'. Once again, the recommended answer would be 'no'. Now, there are few companies that would hire hotheads. In fact, companies can face problems by selecting candidates based on such questions. Given these possibilities, the regulatory authorities of Rhode Island have discovered that CVS Pharmacy was illegally turning away candidates with mental distress, whenever the personality test asked respondents to agree or disagree with statements, such as: 'People do many things that make you nervous' and 'There's no point in having close friends; they always disappoint you'. Probably for such reasons, questions in these tests have become more difficult to cheat, in order to collaborate with the interests of the companies.

O'Neil (2020, p. 148) noted that, since Fair e Issac⁵, the use of findings from data collected on the internet has spread without control. Because of it, uses are multiple. Currently, personal information is literally added together in every possible way as statistical models support, and such mathematical products are organized based on ZIP codes and online shopping patterns.

In this regard, companies like RealPage can generate revenue by creating and selling reports based on freely available internet data. In this context, internet users are not merely customers, because their

⁵ O'Neil (2020, p. 147): 'Earl Isaac and his engineer, Bill Fair, conceived a model they called FICO to evaluate the risk of an individual failing to pay a loan'.

personal data and preferences have become products. Even though such situations are liable to legal action, the record in the Stokes case was not rectified until legal proceedings were initiated. And even after the resolution of the case involving RealPage, it is unknown how many other data brokers might be selling files containing even misinformation. The data security of internet users has become an unknown factor up to the present moment (O’Neil, 2020, p. 157-158). In an action to combat human trafficking, especially the trafficking of children for sexual exploitation purposes, Rhodes (2017, p. 24) reported on the work of the UN organization Thorn, founded by Aston Kutcher and Demi Moore to drive technological innovation; the group conducted research on victims of sexual exploitation to uncover the role of technology in this type of crime. The study found that 63% of interviewees reported being recruited, or more accurately, literally sold via an online platform (Thorn, 2015, p. 19).

The Thorn initiative is significant not only for the specific reality its results have demonstrated but also as a model for public authorities in their cybercrime prevention efforts. For this reason, the issue of personal data collection will be further explored.

From these lessons, it becomes clear that literally all information posted on the internet, including that shared on social media web platforms, can serve to develop statistical models for economic leverage, as well as be exploited for criminal activities.

3.1 PERSONAL DATA MADE AVAILABLE ON TELECOMMUNICATION PLATFORMS

When personal data travels across the internet, there is always the possibility of it being captured and used, legally or illegally, through access to Big Data. However, as previously highlighted, people navigate the virtual environment under the belief that they are not being monitored, placing their trust in Big Techs. This trust is essential for digital citizenship and is even vital for a better quality of life.

Furthermore, since our focus lies on criminal practices, the unauthorized use of personal data may compromise well-being initiatives dependent on the internet of things. A clear example is the U.S., where health and mental wellness programs are incentivized through wearable tech, such as Apple Watch, Fitbit and other sensors, which retransmit vital physiological data. The idea stems from good intentions and is encouraged by that government, such as through the Patient Protection and Affordable Care Act, commonly known as Obamacare, which invites companies to engage employees in wellness programs and even provides incentives for healthy behaviors. The law stipulates that employers may offer rewards and impose penalties of up to 50% of the total cost of coverage. According to a study by the Rand Corporation, more than half of all organizations with fifty or more employees have wellness programs in place (O'Neil, 2020, p. 180).

Scenarios such as these lead individuals to provide additional data on internet-hosted platforms, this time for personal healthcare purposes, which has a direct influence on purchasing behavior and personal aspirations. This information serves as the raw material for various actions, including illicit ones, as previously presented.

The capture of information and the control and regulation of technologies occur through the modulation of collected data.

According to Lazzarato (2006, p. 84), this constitutes a process that reveals the users' desires and beliefs, facilitating their integration through a form of cooperation between these technological systems. On the other hand, when large companies put their brands on the provision of the service, as in the case with search engines, it was observed that 73% of North Americans used and believed in the preservation of their data, as identified in a Pew Research report. It is believed, then, that companies like Google would not risk their own reputation, because such an act could attract regulatory representation if they were to tamper with results in favor of a political or business outcome (O'Neil, 2020, p. 189).

However, it is O'Neil (2020, p. 190) who raised an important question: 'How would anyone know if a large-scale company was selling its users' data?' Especially because its algorithms represent vital trade secrets. The thesis holds that it would not be credible for the algorithms of companies like Facebook or Google to use WMD; nonetheless, there is vast potential for abuse, as the process unfolds in code and behind users' imposing firewalls.

Thus, machines possess the mechanism to adjust time, and devices are capable of intervening in events through a strategy of modulating the forces involved in this cooperation, thereby becoming a necessary condition for the process of constituting the users' subjectivity (Lazzarato, 2006, p. 85-86).

On the other side of the world, the situation is no less concerning. The 1989 Chinese protests in Tiananmen Square helped spur investment and collaboration with multinational corporations to equip the fragmented policing system with network computing technology. In 1994, even before widespread consumer internet access, the Chinese

public security department began to be interconnected through what would become known after 1998 as the Golden Shield Project (*Jindun Gongcheng*). This project had access to data telecommunications, customs records, and tax information entered into government programs via rudimentary networks (Hui, 2024, p. 189).

At that historical moment, as state planners observed falling birth rates and hoped to induce families to welcome up to three children, the same questions remained: information can be obtained, though confirming it is difficult; and whether sending information back into the system to affect change would be reliable remains to be seen. However, we currently live in a state where mobile internet technology and surveillance are ubiquitous; artificial intelligence has entered the scene, bureaucratic information sharing has improved, and mechanisms exist to integrate the private sector with government data. This did not sharpen the sensors as much as it inundated them. Even with high-quality data and massive computing power to process it all, the problem of how to identify the key signals and what to do with them remains (Hui, 2024, p. 195).

Corroborating Hui's view, though drawing from Western theory, it has been observed that personal feelings and dreams can facilitate the operations of organizations acting illicitly. This is because First Modernity suppressed the growth and expression of the self in favor of collective solutions, whereas in Second Modernity, the self is all one has. The new sense of psychological sovereignty burst onto the world long before the internet, which appears only to have amplified its claims. Through trial and error, we learn how to weave our daily lives together. Nothing is given. Everything must be reviewed, renegotiated, and reconstructed in terms that make sense to us: family,

religion, sex, gender, morality, marriage, community, love, nature, connections, political participation, career, and nutrition, as Zuboff (2018, p. 40) argued.

In fact, it was this new mentality and its demands that summoned the internet and the growing information apparatus into our everyday lives. The burdens of life without a fixed destination directed us toward the information-rich power accumulated in digital spaces, as they offered new ways to amplify our voices and forge our own chosen patterns of connection (Zuboff, 2018, p. 40-41).

Ultimately, as corporations faced scrutiny over their violations, they began to frame the use of user data as a necessary quid pro quo for providing free-to-use internet services. In this case, privacy was the price one had to pay for the abundant rewards of information, connection, and other digital goods, whenever, wherever, and however you wanted them. These explanations distracted everyone, and a radical shift emerged that rewrote the rules of capitalism and the digital world (Zuboff, 2018, p. 55).

For Lazzarato (2006, p. 106), it is capitalism that seeks to control the global virtual environment. Within this space, through the variation and continuous modulation, it becomes possible to alter the behavior of internet users; this is due to the power of modulating technologies, which undergo constant daily variation to reshape subjectivities.

In 2015, Tim Wu joined Harvard Business School and conducted an academic study on legal aspects of the internet alongside Michael Luca and a team of data scientists from Yelp. They investigated hidden data and mechanisms embedded within Google Search with the aim of expanding crucial information-provisioning functions. The academic team discovered that Google systematically corrupted search results to

favor its own content and ‘downstream products’ (Zuboff, 2018, p. 131).

These lessons demonstrate that there is no absolute security guaranteeing the protection of personal information on internet-mediated electronic platforms. This reality prompts an investigation into how the crime of human trafficking has already manifested within the environment of electronic social networks.

3.2 HUMAN TRAFFICKING ON INTERNET-MEDIATED SOCIAL NETWORKS

Despite UNASUR's efforts to regulate and promote digital sovereignty through the South American Fiber Optic Ring, an initiative aimed at reducing dependence on U.S.-based technological infrastructure, the project was halted. The gradual decline of the organization, precipitated by the end of the so-called 'pink tide' of governments (e.g., Presidents Correa in Ecuador, Morales in Bolivia, Mujica in Uruguay, and Dilma Rousseff in Brazil), resulted in the fragmentation of regional cyber defense strategies (Hui, 2024, p. 233).

Facebook, as one of the largest social media platforms, has already observed the practice of human trafficking for servitude within its environment. According to Duffy (2021), the platform had struggled for years to combat content related to domestic servitude, which, in reality, is a form of luring a person to work in a household through fraud, coercion, or deception. ‘Traffickers are quick to adapt their business model to meet their needs and increase their profits, so it is clear that they follow online trends’ explains Crittin (2021), Crime

Prevention and Criminal Justice Officer at the United Nations Office on Drugs and Crime (UNODC).

According to Crittin (2021): ‘Currently, traffickers are using technology to profile, recruit, control, and exploit their victims, in addition to using the internet, especially the dark web, to hide illegal materials resulting from trafficking and their real identities from investigators’.

As stated by Crittin (2021), several websites offer live chat options, allowing traffickers to have immediate contact with potential victims, as well as the opportunity to obtain personal information, such as passport details, which increases their power of persuasion. Such victims can be repeatedly exploited through live streaming on multiple websites, as there is no limit to the number of contact channels. Furthermore, the global nature of human trafficking, driven by the misuse of technology, hinders the efforts of public authorities to confront this criminal offense.

In order to highlight the importance of international cooperation in this type of crime, Crittin (2021) explains:

‘When a crime is planned in one country, with victims in another country and a customer in a third, law enforcement authorities face practical challenges, such as finding and protecting evidence, as any investigation requires cross-border cooperation and a certain level of digital expertise.’

According to an assessment for the UNODC by Crittin (2021): ‘In the US, approximately 40% of sex trafficking victims are recruited online,

identifying the internet as the primary location for victim recruitment.

In these scenarios, the importance of regulating the responsibility of large companies in the virtual environment regarding their users' sensitive data is demonstrated, especially when observing that this facilitates crimes across national borders. In the words of Crittin (2021): 'The trafficker then sexually abuses a child in front of the webcam, while the offender in the United States watches a live stream of the abuse'.

The Covid-19 pandemic provided more opportunities for traffickers due to the intensive use of the internet during that period, particularly social networks and online gaming sites, as the number of users of these services continues to grow. For this reason, there is a call for adequate social media regulations, and according to Crittin (2021): 'However, when investigators enter the digital world of citizens, they have access to personal information. It is, therefore, crucial to have rigid frameworks around this access and use of data to ensure that the right to privacy and human rights are respected'. This is the current challenge: combating crime without violating fundamental rights.

A background document produced by the UNODC highlights several examples of existing or promising partnerships and tools that countries are using or developing. These include, notably, digital forensics, data scanning tools, smartphone applications, and successful collaborations with technology, social media, and the internet companies (Crittin, 2021).

UNODC collaborated in the creation of *DataJams*, partnering with the global computing giant IBM and the Colombian non-governmental organization *Pasos Libres*. In this project, students competed online to

develop technology-based solutions to identify and protect victims of human trafficking, as well as to provide support to authorities interacting in judicial proceedings (Crittin, 2021).

Other cases were reported on The Exodus Road website, with figures from 2000 to 2020, showing that 30% of sex trafficking survivors in U.S federal cases were recruited by their traffickers via social media. In 2021, this number rose to 41%, highlighting an upward trend (Nikkel, 2024).

Nikkel (2024) reveals that The Exodus Road has successfully uncovered that human trafficking is increasingly occurring across internet-mediated social networks. Through their anti-trafficking operations in Brazil, India, Latin America, the Philippines, Thailand, and the United States, they highlight that despite mounting pressure for enhanced sectoral regulation, companies associated with Meta, Snapchat, TikTok e Discord continue to evade accountability.

As has already been revealed, traffickers, before approaching their victims, scout social media, specifically looking for expressions that reveal their needs, whether in profiles or messages. Examples include those referring to: financial stability or employment; romantic partnership; love and affirmation; housing; and physical safety, which is common when the victim is in a situation of domestic violence, local political instability, or war. Once the victim's desire is identified, the proposal is generally design specifically to satisfy it, offering various initial facilities.

The exploitation within social media communities is undeniable, including when it comes to employment. In addition to modeling, other professions are also promoted, such as cleaning, hospitality, restaurant services, or agriculture, with the promise of long-term

stability. However, in reality, these job opportunities can quickly give way to sex trafficking, labor trafficking, and debt bondage (Nikkel, 2024).

The way traffickers operate can be direct or indirect. In the latter case, after capturing the victim of their crime, they take control of the victim's social media accounts. In the National Survivor Study conducted by Polaris, 32% of survivors of sex trafficking reported that their traffickers monitored their social media use and controlled their electronic devices. Sometimes, traffickers co-opted the accounts as if they were their own, turning them into a kind of virtual trafficker as well, even deceiving the victims' families (Nikkel, 2024).

3.2.1 An illustration of Brazilian Reality

The National Report on Combating Human Trafficking for the period from 2021 to 2023 highlighted that the use of technology in the virtual environment was identified as a factor that increased traffickers' profit margins, because it enabled efficient and agile operations on a global scale, with a significant recruitment of more victims at the same time. This was especially due to social media platforms, such as Facebook and WhatsApp, which began to be accessed by people in contexts of socioeconomic vulnerability, susceptible to accepting deceptive labor promises. During the launch of the aforementioned Report, the Fourth National Plan to Combat Human Trafficking was also presented, and following that ceremony, the national seminar entitled 'A New Chapter in the National Policy to Combat Human Trafficking'

(EBC, 2024) took place, as part of the government's efforts to confront this tragic reality.

Garcia (2020) had already shown that women from all over the world have for years been deceived by false promises on the Internet, and currently social networks have amplified the actions of human traffickers, because they began to select their victims, and Brazil may be one of the countries with the highest number of victims of the crime of human trafficking.

According to Garcia (2020), the work of criminals in getting to know their victims, as well as their preferences and aspirations, was facilitated by access to social media profiles, since the victim's vulnerability could be discovered while using Internet services. This is because, if the victim is seeking love, the perpetrator creates a fake profile with the attributes desired by the victim. If the victim is looking for a job, the active agent of the crime will lure them with a job offer. And children, in general, are attracted by fake profiles of other children.

Regarding the fate of these victims, there is a tendency toward intense cruelty, because the crime of human trafficking aims at sexual exploitation and even organ removal. Garcia (2020) reveals that a 30-year-old man was arrested for keeping at least 240 sex slaves in 12 Brazilian states, committing the crimes through the use of Internet platforms.

For the Civil Police in Belo Horizonte, the accused offered up to R\$10,000 to obtain intimate photos of the victims, using the trick of sending a false proof of bank deposit, and from then on began extorting the victims. He himself even went on to meet and rape his victims (Garcia, 2020).

Human trafficking has also been occurring at the international level, as Brazilian women were lured in 2019 through the use of social networks and the false promise of employment as dancers in Japan, which has become a destination for dozens of young women deceived by sex traffickers under the promise of careers as models or dancers (Garcia, 2020). In this case, the apparent employer offered plane tickets, accommodation, and a high salary, but when the women arrived on Japanese soil, their passports were illegally confiscated, and they were enslaved for sexual exploitation and forced to use drugs as a way to reduce their resistance to the violence they suffered.

Some warnings or publicity campaigns can be carried out to reduce the risks of people becoming victims of human trafficking through the Internet. Garcia (2020) notes that avoiding leaving social media profiles in public mode, being suspicious of new friendships with many promises of ease, and periodically monitoring children's use of the Internet, since they are among the main victims of this crime, are ways of acting preventively.

4 CLOSING STATEMENTS

As described, the use of the virtual environment requires personal care, especially to avoid registering on platforms that do not ensure the confidentiality of personal information or exchanging information with unknown people before establishing contact in that environment, since these situations may expose individuals to criminal organizations engaged in human trafficking or other illicit activities. Preventive behaviors against these crimes should be

encouraged among everyone, as well as the demand for State action in carrying out preventive campaigns, monitoring the services provided, and applying criminal and administrative penalties.

This is a matter of defending fundamental rights, and as such, Internet users must be warned that their information should be protected by big tech companies, because it is evident how difficult it is to stay away from the activities of the large corporations providing the services under investigation. These companies store users' data and manage the main platforms available to the general public, and therefore, the implementation of protocols to protect the privacy of such sensitive information must be demanded.

In this regard, it is believed that, with respect to large companies, given that their brands are internationally recognized, their businesses should not be put at risk by selling the data contained in users' individual account profiles. However, they are not safe from the actions of intruders, who may illegally access such systems and cause harm to Internet users. The responsibility for defending against these possible invasions must lie with the big tech companies, which should create prevention mechanisms and collaborate with coercive institutions (administrative and criminal) to improve the security of the virtual environment and protect users' fundamental rights.

In the field of Fundamental Rights, following the implementation of the Civil Framework for the Internet (Federal Law No. 12,965 of April 23, 2014); Brazil's General Law on the Protection of Personal Data (LGPD), Federal Law No. 13,709/2018, which establishes the prevention of damages that users may face (Art. 6, item VIII; Art. 11, paragraph 'g'; Art. 26, item V); and, finally, Constitutional Amendment No. 115/2022, which clarified the constitutional nature

of the protection of sensitive data stored in the virtual environment, at least at a symbolic level, the State must provide protection to citizens, making it necessary to propose ways to ensure its effectiveness.

In this regard, it was considered that the virtual environment requires daily measures to protect users' fundamental rights, and State protection for citizens who use this type of service must be constantly updated. In other words, protection in this environment must operate on two levels: first, at the level of service providers, who must also be held accountable for damages suffered by their users, whether caused by the company itself or by third parties; and second, at the level of the State, with the capacity to carry out inspections and impose fines on service providers available to Internet users, as well as suspend services that expose users to risk situations, within the scope of Administrative Law.

In criminal law, the use of the virtual environment for committing crimes should long ago have been considered a general aggravating factor for all criminal offenses. Specifically, regarding the crime of trafficking in persons, at the very least, a cause for increasing the sentence is advisable, because, as noted by Rhodes (2017, p. 28), it is one of the crimes that makes extensive use of the technologies currently available; therefore, it must be discouraged.

Human traffickers in the virtual environment operate across all layers—whether the web, dark web, or deep web, mastering new tools to carry out grooming, recruitment, and the agenting of victims, delivering them to the destinations of their criminal enterprises. In addition, they hinder law enforcement efforts, a fact that highlights the need to intensify discussions on ways to confront such human brutality.

The value of the actions already undertaken in this struggle must be recognized, but there is no doubt that much remains to be done each day that a new tool for work in the virtual environment is launched. It is necessary to think about reducing the opportunities for human traffickers to act continuously in the virtual environment, as exemplified by the initiatives carried out by Thorn and IBM reported in this research.

Thus, hoping to have contributed to the dissemination of studies on the understanding of situations that may hypothetically occur, it is necessary, in the field of developing these technologies, to ensure the proper training of public agents, as well as appropriate international cooperation, in addition to the constant development and implementation of preventive actions against crimes that can be committed directly in the virtual environment, such as the examples addressed, especially by encouraging research in these areas.

REFERENCES

BAUDRILLARD, Jean. **Tela total: mitos-ironias na era do virtual e da imagem**. Trad. Juremir. Machado da Silva. 4. ed. Porto Alegre: Sulina, 1997.

BITENCOURT, César Roberto. A Nova e Equivocada Tipificação do Crime de Tráfico de Pessoas. **Revista Paradigma**, Ribeirão Preto-SP, a. XXI, v. 25, n. 1, p. 2-26, jan/jun, 2016

BRASIL. **Constituição da República Federativa do Brasil de 1988** (CRFB). 5 out. 1988. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em 30 nov. 2024.

BRASIL. **Decreto 5.017, de 12 de março de 2004**. Promulga o Protocolo Adicional à Convenção das Nações Unidas contra o Crime Organizado Transnacional Relativo à Prevenção, Repressão e Punição do Tráfico de Pessoas, em Especial Mulheres e Crianças. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/decreto/d5017.htm. Acesso em: 15 dez. 2024.

BRASIL. **Lei 13.344, de 6 de outubro 2016**. Dispõe sobre prevenção e repressão ao tráfico interno e internacional de pessoas e sobre medidas de atenção às vítimas; altera a Lei nº 6.815, de 19 de agosto de 1980, o Decreto-Lei nº 3.689, de 3 de outubro de 1941 (Código de Processo Penal), e o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); e revoga dispositivos do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal). Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13344.htm#art13. Acesso em 30 nov. 2024.

BRASIL. **Agência Gov**. Tecnologia ampliou alcance do crime de tráfico de pessoas, mostra relatório do MJSP. 30 jul. 2024. Disponível em: <https://agenciagov.ebc.com.br/noticias/202407/relatorio-nacional-divulga-dados-sobre-trafico-de-pessoas-de-2021-a-2023>. Acesso em: 30 nov. 2024.

BRITANNICA, THE EDITORS OF ENCYCLOPAEDIA (BRITANNICA). William Wilberforce. **Encyclopedia Britannica**, 07

dez. 2024. Disponível em: <https://www.britannica.com/biography/William-Wilberforce>. Acesso em: 20 dez. 2024.

CRITTIN, Tiphannie. Traficantes abusam da tecnologia online, alerta agência de prevenção ao crime da ONU. Entrevista cedida à **Notícias da ONU Perspectiva global Histórias humanas**. 30 nov. 2021. Disponível em: <https://news.un.org/en/story/2021/10/1104392>. Acesso em: 30 nov. 2024.

DUFFYD, Clare. Documentos revelam que Facebook sabia sobre tráfico de pessoas em anúncios de trabalho. 25 out. 2021. **CNN BRASIL**. Disponível em: <https://www.cnnbrasil.com.br/tecnologia/documentos-revelam-que-facebook-sabia-sobre-trafico-de-pessoas-em-anuncios-de-trabalho/>. Acesso em: 30 nov. 2024.

FARAHANY, Nita A. **The Battle For Your Brain**. New York: St. Martin's Press, 2023. *E-book*.

FARIAS DA SILVA, Marco Aurélio. Crime de tráfico de pessoas no Brasil: lacunas na tutela penal e propostas de inclusão do protocolo de palermo. **Revista Brasileira De Ciências Criminais**, 203, p. 109–135, 2024.

GARCIA, Maria Fernanda. Perigo: brasileiras são enganadas na internet e viram escravas sexuais. 18 nov. 2020. **Observatório do Terceiro Setor**. Disponível em:

<https://observatorio3setor.org.br/perigo-brasileiras-sao-enganadas-na-internet-e-viram-escravas-sexuais/>. Acesso em: 25 nov. 2024.

HANNIGAN, Robert. 2014. 'The Web Is a Terrorist's Command-and-Control Network of Choice'. **The Financial Times**, 03 nov. 2014. Disponível em: <https://www.ft.com/content/c89b6c58-6342-11e4-8a63-00144feabdc0>. Acesso em: 30 nov. 2024.

HUI, Yuk. **Cybernetics for the 21st Century Vol.1 Epistemological Reconstruction**. Hong Kong: Hanart Press, 2024.

LAZZARATO, Maurizio. **As revoluções do capitalismo**. Tradução: Leonora Corsini. Rio de Janeiro: Civilização Brasileira, 2006.

MATTELART, Armand; MATTELART, Michèle. **História das teorias da comunicação**. 9. Ed. São Paulo: Loyola, 2006.

MITNICK, Kevin D.; SIMON, William L. **A arte de enganar**. Trad. Kátia Aparecida Roque; revisão técnica: Olavo José Anchieschi Gomes. São Paulo: Pearson Education do Brasil, 2003.

MORENO, J.L. **Who shall survive? A New Approach to the Problem of Human Interrelations**. Washington, D. C: Nervous and Mental Disease Publishing Co. 1934.

NIKKEL, Mary. Tráfico de pessoas e mídias sociais. **The Exodus Road**. 2024. Disponível em: <https://theexodusroad.com/pt/human-trafficking-and-social-media/>. Acesso em: 30 nov. 2024.

O'NEIL, Cathy. **Algoritmos de destruição em massa: como o big data aumenta a desigualdade e ameaça à democracia**. Trad. Rafael Abraham. 1. ed. Santo André, SP: Editora Rua do Sabão, 2020. *E-book*.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Traficantes abusam da tecnologia online, alerta agência de prevenção ao crime da ONU**. 30 out. 2021. Disponível em: disponível em: <https://news.un.org/en/story/2021/10/1104392>. Acesso em: 30 nov. 2024.

PIMENTEL. Alexandre Freire. **TRATADO DE DIREITO E PROCESSO TECNOLÓGICO - (VOL. 02) - Big Data, Justiça 4.0 e a Digitalização da Processualização; Ciberespaço, Metaverso, Legal Design e Visual Law: O Direito Processual Tecnológico**. 2 ed. Recife: Editora Publius, 2023.

RECUERO, Raquel. **Redes sociais na Internet**. Porto Alegre: Sulina, 2009.

RHODES, Leanne Maree. **HUMAN TRAFFICKING AS CYBERCRIME**. *AGORA International Journal of Administration Sciences*, n. 1, 2017, p. 23-29.

RODRIGUEZ, Laura Zúñiga. *Trata de Seres Humanos y Criminalidad Organizada Transnacional: problemas de política criminal desde los derechos humanos*. *RDPJ*, Brasília, a. 2, n. 4, p. 9-58, jul-dez, 2018.

ROXIN, Claus. **Derecho Penal Parte General Fundamentos. La Estructura de la Teoría del Delito**. Madrid: Civitas, 1997. T. 1.

THORN Digital Defenders of Children. **A Report on the Use of Technology to Recruit, Groom and Sell Domestic Minor Sex Trafficking Victims**. *In* collaboration with Dra. Vanessa Bouché. January 2015. Disponível em: https://www.wearethorn.org/wp-content/uploads/2015/02/Survivor_Survey_r5.pdf. Acesso em: 30 nov. 2024.

TORRES, Cláudio. **A Bíblia do Marketing Digital**. São Paulo. Editora Novatec, 2009.

UNITED KINGDOM (UK). Slave Trade Abolition Bill. HC. **Parliament**, v. 8, p. 945-95, deb/feb, 1807. <https://api.parliament.uk/historic-hansard/commons/1807/feb/23/slave-trade-abolition-bill>. Acesso em: 15 dez. 2024.

WILLIAMS, Eric. **Capitalism & Slavery**. Richmond: The William Byrd Press, 1944.

ZUBOFF, Shoshana. **The age of surveillance capitalism: the fight for a human future at the new frontier of power**. 1. ed. New York: Public Affairs, 2018. *E-book*.