Trafficking in Persons Online, exploitation by the Dark Web and the forms of technical-legal combat

(extended abstract of the MSc dissertation)

Nathália Carvalho Schmidt de Deus
Information Security and Cyberspace Law
Instituto Superior Técnico

Advisor: Prof. Nuno Miguel Carvalho dos Santos

Abstract - From slavery through slave ships, one of the most profitable businesses at the time, to the recognition of the crime of human trafficking, the most lucrative crime today. Despite being considered one of the most barbaric crimes of humanity, with criminal provisions in several legal systems, illicit activity has been transformed by new technologies. The objective of this work will be to analyze how the Dark Web instrument complements the practice of human trafficking on the Internet, to evaluate the connection between the crime of trafficking in persons and the Internet and what can be done to combat this crime. Through the research, it is possible to perceive that several characteristics facilitate the practice of human trafficking when it occurs in the deepest layer of the Web. Among them, the guarantee of anonymity in the network and payment of cryptocurrencies, are some factors that favor the commission of the crime in high proportion. By definition attributed to this practice, it is clear that it is a multiple-action crime with the possibility of infinite illicit purposes. Several types of research have already been carried out in this area by UNODC, but with the origin of the pandemic, the crime has become more hidden and difficult to measure. The blocking and confinement measures influenced the concealment of the crime, and the Dark Web offers all the necessary precepts to contribute to this concealment. To understand why this barbaric crime is not fought more effectively, a comparative analysis of the legislation of Brazil and Portugal was carried out. There are still many changes to be made to combat this crime. The use of machine learning techniques to identify suspicious text messages, images, and videos will be an ally of the public power in the fight against human trafficking.

I – INTRODUCTION

The use of new technologies has changed the way criminals act and jeopardized the integrity and dignity of thousands of people, especially those in situations of economic vulnerability, whose personal data are used for various illicit purposes.

For the UN agency, there is a situation that represents a "human trafficking pandemic" [1] through a study on the impact of Covid-19, in which an increase in the number of victims of human trafficking during the pandemic was found, especially regarding the exploitation of children. Criminals take advantage of the global crisis, unemployment, and loss of income, to recruit and go after victims' adults and children who have spent more time on the Internet. The UN also warns that criminals transferred their activities to the Web instead of acting in public places.

So, what is the connection between human trafficking and the Internet? How does human trafficking occur on the Internet and Dark Web? What has changed in the crime of human trafficking with the instruments of technology in hidden services? Who are the victims and how can this type of crime be fought?

First, it is necessary to know these three layers of the Internet: Surface Web, Deep Web, and Dark Web, so that we can have the first idea of these virtual environments.

We will study the crime of illicit trafficking in persons, its elements, and its recognition in Public International Law. Then, we will differentiate between the surfing levels of the Surface Web, Deep Web and Dark Web, so that we can understand the crime of human trafficking on the Dark Web. We will then trace a circuit of the crime of human trafficking online.

For this, we will use the Tor Browser tool and the guidance of experts in the technical area of the IST (Instituto Superior Técnico) who can promote a true analysis of the sites that offer so-called hidden services and we will explain how this tool works, the experience obtained and its results.

In addition to the technical study, we will also make a critical analysis through the legal-legislative comparison between Brazil and Portugal. What still needs to be modified so that the crime is fought more effectively legally since many victims come from Brazil to Europe.

An analysis of Information Security is also necessary since illicit trafficking in persons can also be committed for the exploitation of the use of personal data.

Finally, we will analyze the measures to be adopted to combat the crime of trafficking in persons, among them, the use of machine learning to detect crime.

II- A CASE OF JUSTICE

A recent case[2] was found from the testimony of a victim of international human trafficking: Vitória, 19 years old, was recruited in the Rio Grande do Sul, Porto Alegre/Brazil, and through trafficking traveled to Belarus, where managed to escape and seek help at the Brazilian embassy in Minsk.

Today the aggressor is in prison and is serving time in Canoas, the Rio Grande do Sul. This aggressor took advantage of social networks on the Internet such as Tinder to meet the victim in question. The convict used the interactive means of the Internet to expose videos by webcam, in which he put the victim in a situation of sexual exploitation and torture for the entertainment of third parties, publishing them to profit from the access. The victim of the process was not the only one, as the aggressor supported himself through this means of exploitation, that is, he profited a lot financially from the crime

The convict had the practice of enticing girls for a long period, communicating through various profiles on various websites, most of them from outside Brazil, with the product videos, using physical and psychological violence.

The victim revealed that she had bad relationships with her family and, because she wanted to leave the house, she got involved with the criminal in Brazil. During this period, the victim was still a minor when the perpetrator involved her emotionally and kept her in a private prison.

Then, in early September 2020, the author transported the victim to Belarus and treated her with serious threats, violence, and abuse, for sexual exploitation on the Internet. The victim did not make money from the practice. The criminal practices only ended when the victim, fearing for her own life, managed to flee to the Brazilian embassy, where she found protection.

III- THE ELEMENTS OF HUMAN TRAFFICKING

According to Public International Law [3], we can define trafficking in persons as:

"*The recruitment, transportation, transfer, harboring or receipt of persons, through the threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power or a position of vulnerability or of giving or receiving payments or benefits to obtain consent for one person to have control over another person, for exploitation*".

As a classic reference for the crime of human trafficking, three key elements distinguish them from other similar crimes:

- *Action*: Recruitment, transport, transfer, accommodation, or reception of persons;
- *Means*: Threat, use of force or other forms of coercion, abduction, fraud, deception, abuse of authority or a situation of vulnerability, giving or accepting payments or benefits to obtain the consent of a person having authority over another;
- *The end*: Sexual exploitation, forced labor or services, slavery, servitude, removal of organs, tissues, and body parts, and other forms of exploitation (eg. to commit crimes).

All three elements must be gathered for it to be classified as trafficking in persons. This is a multiple action crime (or with varied or multinuclear content), as it describes several behaviors in the same article, that is, several verbs as nuclei such as recruitment, transport, transfer, shelter, or reception of people.

When trafficking is in children, the means indicated are irrelevant. A child's possible consent is considered irrelevant, regardless of the circumstances in which it may have been expressed. Therefore, in cases involving children, the two elements of actions and purpose of exploitation are sufficient to determine whether a case constitutes trafficking in children.

IV- THE MAIN VICTIMS AND THE MAIN ILLICIT PURPOSE

According to the UNODC report [4], "global patterns of trafficking in persons" were detected, in which the age, sex of the victims detected, gender, and origin (local or foreign, about the country of origin, were taken into account) of traffickers and the relative prominence of the various forms of exploitation.

In this work, we evaluated the UNODC surveys from 2007 to 2018.

Between 2007 and 2010, women already constituted the majority of victims of human trafficking detected globally.

In 2009, women accounted for 59% of victims of human trafficking globally; girls represented 17% of trafficking victims; men 14%; and boys, 10% [5].

In 2010, the percentage of female victims was even higher than in 2009. Women represented 66%; girls, 13%; men, 12%; boys, 9%.

In 2016, women accounted for 49% of global victims of human trafficking; girls, 23%; men, 21%; and boys, 7% [6].

The last and most recent survey was in 2018, in which women accounted for 46% of victims; girls, 19%; men, 20%; and boys, 15% [7].

With the Covid-19 virus pandemic that began in late 2019, there has been a significant increase in all forms of violence and exploitation, data that will take time to collect and fully assess. However, there is evidence of a large increase, called by UN Secretary-General António Guterres a "parallel pandemic", with the number of cases of violence against women and girls in 12 countries monitored by the United Nations being reported to several institutions, with an increase of 83 percent between 2019 and 2020, and cases reported to the police are up 64 percent [8].

With schools closing due to confinement, many children have spent more time on the Internet, for education, as well as on social media, and are more vulnerable to online recruitment and exploitation.

On the other hand, the most well-known purposes of human trafficking are sexual exploitation, forced labor or service, slavery, servitude, and removal of organs, tissues, and body parts, among other forms of exploitation, such as the commission of crimes.

As for the illicit purpose, according to a survey carried out by UNODC, which involved 148 countries around the world, between 2016 and 2018, of the forms of exploitation detected in human trafficking, 50% of them are aimed at sexual exploitation [9].

Figure 1: Research carried out by UNODC, between 2016 and 2018. Forms of exploitation among detected victims of trafficking.

V- THE HUMAN TRAFFICKING ON THE INTERNET

In the crime of human trafficking on the Internet, the trafficker's first concern is how to recruit the victim.

Social media platforms are used as virtual catalogs by traffickers to identify new victims and develop recruitment strategies, into possessing a significant amount of information about the psychological and personal history of users, such as education level, family ties, status economics, place of residence, a network of friends, among others, which are information frequently displayed and included with photos.

Through the Internet, it is possible to have access to a vast audience of people with countless possibilities of recruiting victims who go after attractive job offers that are accessible through simple search engines, instant windows (pop-ups), spaces of conversation (chat rooms) and unsolicited email (spam) [10].

To better understand the illicit trafficking of people through the Internet, it is important to make a small identification of the layers that compose it: *Surface Web, Deep Web and Dark Web*.

- *Surface Web*: is the Web content and services best known by users, which is generally accessible by search engines such as Google, Bing, and Yahoo!, by which it sends the user to a set of pages detected as a search result;
- *Deep Web*: Is the area of the Internet not accessible through widely-known search engines. It is made up of pages that may have been voluntarily excluded from search results on Surface Web search engines. It is simply invisible to the usual search engines, for

example, depending on the introduction of a keyword, like web-mails and Instant Messaging pages, or are pages that are not findable by accessing an external link (therefore not detected by search engine crawlers), or dynamically generated pages;

- *Dark Web*: Access to the Dark Web relies on specific software to access its content. The Dark Web consists of websites that are accessible using networks such as Tor ("The Onion Routing" project), created specifically for providing anonymous communication on the Internet.

The crime of online human trafficking can occur entirely on the Surface Web, where traffickers hide the content of exploitative services behind apparently lawful activities to avoid being discovered while increasing their customer base.

For our research, we seek to unravel the connection between illicit human trafficking and the deepest layer of the Internet, the Dark Web, through the Tor tool. We seek, through the search engine, to identify pages that may contain illegal content, simply by typing the words "woman" and "man". Nothing much could be identified with the insertion of the word "man", while in the insertion of the word "woman", several pages of dubious content were strangely displayed.

When browsing the Dark Web, we found evidence of illicit trafficking in people based on websites, as in the case of vulnerable and civilly incapable people, such as children or miserable people from underdeveloped countries, in the practice of zoophilia.

In other cases, we found people with physical disabilities being used for the sexual exploitation and entertainment of users. There is a preview of what is possible to access through the payment of bitcoins.

Our impression is that even if some pages have adult pornography, minors' content is always present for sale.

VI- THE CIRCUIT OF ILLICIT TRAFFICKING FOR EXPLOITATION ON THE DARK WEB

During the pandemic, in various regions of the world, women, and girls were recruited, often locally or online, for sexual exploitation, particularly exploitation in private apartments.

Another case of human trafficking, in addition to the Vitória case, was identified through the testimony of a Brazilian victim who was recruited in Spain. According to the latter, dating apps such as Tinder/Badoo, among all others, are the favorite means used by traffickers to entice victims to Europe[1].

There is a typical way for human traffickers to operate their business on the Dark Web. This route is made regarding the crime of trafficking human beings for exploitation on onion services pages.

Through the Surface Web, the victim assumes to be in a legitimate situation of a job offer, advertisement for the sale of articles on the Internet, or even a dating website or application. After already being involved in the situation, the victim is recruited into trafficking, which can take place with or without her consent. Due to threats and blackmail, or various other reasons, such as being alone in another country, withheld documents, and passports, private imprisonment, age, and fear of suffering penalties in a foreign country, she has no means of getting out of the situation alone without the help of the authorities. Thus, the victim becomes prey for the entertainment and profit of others.

As per UNODC's analysis, anyone can post or browse advertisements to sell or buy any service on online marketplace sites (from job vacancies to the sale of equipment, cars, and clothing) that are being used to advertise services obtained through victims of trafficking in persons [11].

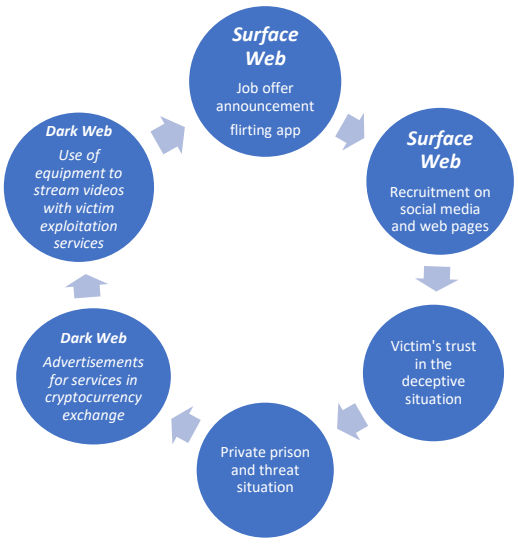

Figure 2: The circuit of illicit trafficking: Surface Web - Dark Web.

[1] Youtube: "SobreVivendo na Turquia". Available at: (274) DE 'CASAS' PEQUENAS À GRANDES MÁFIAS: "PRECISO CONTAR TUDO QUE VIVI", DESABAFA VÍTIMA DE TRÁFICO. - YouTube

There are some particular features of illicit trafficking in people for exploitation on the Dark Web:

(i) Payment in cryptocurrencies: The intention to reach a large number of viewers and means of payment in cryptocurrencies. The exploitation of victims of human trafficking usually aims at the huge profits that are obtained through cryptocurrencies, given their varied characteristics that facilitate crime. Cryptocurrencies, like bitcoins, are virtual or electronic currencies traded online. In addition to these, there are other advantages to trafficking in persons for other activities that are part of organized crime:

- Mixers can be used to clean illicitly obtained assets and make the tracking process more difficult, thus eliminating the need for money laundering [12];
- Despite having privacy, when a payment is made, it can be detected through the digital wallet that the amount has been transferred. But with the use of mixers, one user's cryptocurrencies are mixed with that of others, scrambling and making it difficult to track them [13];
- Digital currencies provide relative anonymity. The mixers most used by criminals, Absolutio, AudiA6, and Blender, are platforms that can be used on the Tor network to reinforce the privacy and anonymity of its users [14];
- Cryptocurrencies can be moved internationally, crossing borders with ease, thus bypassing the limitations of international transfers [15];
- Using multiple digital accounts, one for each transaction, creates additional challenges for law enforcement and anti-money laundering authorities to track transactions and monitor patterns, as it creates uncertainty as to whether the accounts belong to the same or multiple subjects;
- There is a reduced risk of a counterparty reneging on a transaction, as digital currency transactions are irreversible and can only be reimbursed to the receiving party [16];
- Large amounts of money make traffickers potential targets for other criminals (the use of cryptocurrencies involves new actors in the trafficking arena, such as crypto exchanges/exchangers; crypto trader, crypto mixer") [17].

(ii) The lack of need for a criminal organization: Considering that the illegal material to be marketed refers to images and videos of people there doesn't need to be a criminal organization or a place designed to receive customers. Everything is done remotely and, through the objectification of the human being, a single person can serve as a commodity more than once, for different customers worldwide, generating high profitability. One person is enough to traffic and publish images and videos for financial profit.

(iii) The lack of need for direct contact between the victim and the user paying for the service and a place designed for the illicit conduct: As the exploitation of the person is transmitted remotely, the user of the service does not need to contact the victim, because what he will consume are the images and videos made available on the onion services pages. Considering that the illegal material to be commercialized refers to images and videos of people, it is not necessary to have a place designed to receive customers.

(iv) the anonymity guarantee: With the installation of the Tor Browser, it is possible to easily access the pages that provide onion services and that guarantee the anonymity of the IP. This type of technology that underlies the Dark Web is a large-scale network that implements a message forwarding protocol, allowing the user to configure their browser to ensure anonymity. Through this tool it is possible to hide the IP address, using a set of proxies spread all over the world as a network. These proxies are called relays or also understood as message-sending nodes. Each relay only knows the next node through which it will send the message, and the only one who knows the entire path taken is the sender of the message. The sender chooses three of these nodes using the onion routing protocol system, that is, the browser client will establish a circuit, defining a path through this network and choosing three intermediate relays until the message reaches the recipient. Thus, the onion routing circuit is established.

This system handles a variety of bidirectional protocols. The sender sends the encrypted message based on the public keys of all relays on the circuit in combination with the TLS protocol to establish a circuit with symmetric key pairs between hops in the circuit. The sender chooses the sequence of

routers in which the path topology can be controlled. Then using security protocols use multiple layers of encryption to move message data along established circuits.

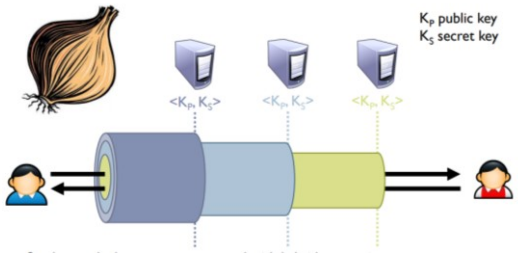

Figure 3: Tor system: onion routing circuit. Figure extracted from a cyber forensic security college degree.

The circuit protects the anonymity of the client's IP address. Tor when accessing sites that are not protected behind an onion service has the IP of the recipient known. The recipient will be protected behind an onion service, in which case the recipient's IP is hidden.

Onion routing derives its security from the fact (or assumption) that it is difficult for an adversary to view all nodes in the route. In case the adversary can see the entire path, onion routing loses its security, or even in case the adversary sees one node at a time, it may be able to correlate the traffic.

Thus, it is possible to verify that the route passes through several countries and each relay has a different IP until reaching the destination:

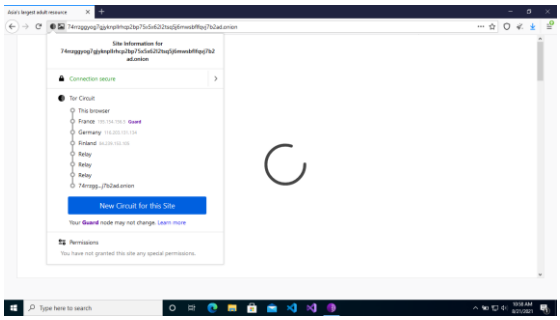

Figure 4: *Tor source circuit.*

(v) private prison of the victim: In addition to being housed in private apartments, during the pandemic, victims suffered various effects, such as difficulty in accessing essential services and without contact with the outside world.

(vi) unlawful purpose of exploiting the dignity of the human person, through sexual exploitation, torture, serious bodily harm (eg genital mutilation), and zoophilia:

Upon entering the Dark Web, it is clear that not only the illicit purpose for sexual exploitation and child pornography is predominant, but also other purposes that involve several other crimes, such as torture, bodily harm, and mistreatment of animals, to call the viewer's attention, through various forms of degradation of the human being.

(vii) The exploitation of people: disabled people, children, adolescents, and adults; mostly women and girls from around the world: Through research carried out on the Dark Web, it is possible to identify that access to images and videos of women, children, and animals in degrading and objectification situations are easily exposed through access for payment of bitcoins. It is evident, of course, that there had to be human trafficking for certain images and videos to be disseminated on the Dark Web, as in the case of vulnerable and civilly incapable people, such as children or miserable people from underdeveloped countries.

(viii) Massive Exploitation of Personal Data: Before recruitment, the victim's data is analyzed by the trafficker. There are personal data that can already be used for profit even without the victim's knowledge, if the victim makes available on the Internet, for example, images that may present profit from the trafficker's point of view. There may also be some carelessness on the part of the victim that will be used by the traffickers to blackmail them, such as the publication of images if the victim does not provide others.

In addition, the exploitation of personal data can occur in the case of identity theft, abuse of credit card data, and fraud through digital signatures for the commission of various crimes involving the personal data of victims of human trafficking. As they are victims who have lost their freedoms, personal data and information are vulnerable to any crimes.

Victims of trafficking in persons for exploitation on the Dark Web particularly suffer from the exploitation of their images and videos to be transmitted to users browsing these onion services pages. The profitability of the crime depends on the availability of this data on hidden pages that guarantee anonymity and the more users, the more accesses and views, the more profit the criminal will have. Therefore, there is a massive amount of personal data being used in the Dark Web layer.

(ix) Participation and profit of the users of the service: Easy access to these sites, both to offer illegal content and incite the practice of crime, in the sense of allowing the consumer to have the opportunity to upload images and videos on sites that promote activities related to the purpose of exploitation of the human person.

(x) Ease of free installation of Tor and access to onion services pages: It is possible to notice that anyone can install Tor for free and have access to these links that are accompanied by advertisements that try to stimulate the user's curiosity about crime and, also, for profit through the transmission of images and videos.

(xi) High profitability: With anonymity on the Dark Web and techniques to make tracking difficult when there is payment in cryptocurrencies, technology is an ally of traffickers to advertise services resulting from the exploitation of people, which naturally leads to an increase in victims per case. With all the characteristics that facilitate the practice of crime, we can say that it is the most lucrative crime, even today, even ahead of arms trafficking and drug trafficking. Through the objectification of the human being, a single person can serve as merchandise more than once, for different customers around the world, as the images and videos are in the possession of the trafficker, which generates high profitability. Unlike drugs that after being consumed cannot generate more profits.

VII- THE INFORMATION SECURITY

According to the aforementioned UNODC studies, women and girls are more vulnerable when using the Internet than men. Men and boys are victims in smaller proportions and with purposes more focused on labor exploitation, but they are also victims of sexual exploitation.

However, it is evident that for all victims of human trafficking there is no security regarding personal data entered on the Internet, such as in social networks, dating apps, sales, and job search sites.

The difficulty in accessing education and the job market places women in underdeveloped countries in a special situation of vulnerability. In the context of Internet services, victims are unaware of the criminal situation that they are inserted behind apparently legitimate services, as the recurrent availability of photos and data on public profiles or the search for jobs is enough to start a recruitment process.

Human trafficking can also be used to exploit personal data, such as identity theft, to commit data fraud, and tax evasion. As already happened in a case where vulnerable Romanians were recruited to Denmark for exploitative purposes, where they had their identities stolen to commit fraud against merchants and the tax agency SKAT (Danish Customs and Taxation Administration). They were kept in an abandoned building and forced to live in subhuman conditions. With false identities, criminals acquire and rent products from companies through abusive use of credit card information on websites, and fraudulently using digital signatures to file tax returns [18].

In the case of collective security, the population's acceptability and credibility were reached in the restrictive decisions imposed by the State, which act within the constitutional possibilities of a situation of public calamity, for example[2].

The “parallel pandemic” of human trafficking also needs effective State intervention to combat this “disease”. In the same field, it is assumed that the State's action will follow the same direction in the collection of personal data to achieve not only the fight against crime but its prevention, including policies that provide information security.

It is up to each EU Member State to legislate internally about the collection of personal data in connection with criminal offenses. According to *Considerando* No. 19 of the GDPR (General Data Protection Regulation), “t*he protection of individuals about the processing of personal data by the competent authorities for the purpose, investigation, detection, and prosecution, of criminal offenses or the execution of criminal sanctions, including the safeguarding and prevention of threats to public security, and the free movement of such data, is the subject of a specific Union legal act*. This Regulation should therefore not apply to processing activities for those purposes”.

In Brazil, the General Law for the Protection of Personal Data (LGPD) contains in its content, in article 4, item III, its non-applicability for the

[2] It is important to note that in the democratic regime itself, hypotheses of greater state intervention established by the Constitution are offered. Thus, both in Brazil and Portugal, the Constitution makes it possible for the State to intervene in the restriction of rights in certain cases. In Brazil, the intervention hypotheses (Title III, Chapter VI; Title V, Chapter 1). This is what happened, for example, with the intervention of the State in the declaration of public calamity, given the pandemic situation caused by the covid-19 virus. In the Portuguese Constitution, article 19 deals with cases of suspension of the exercise of rights.

exclusive purposes of investigation and prosecution of criminal offenses. However, in its §1, it specifies that *the processing of personal data embodied in item III "will be governed by specific legislation, which shall provide for measures that are proportionate and strictly necessary to meet the public interest, observing the due legal process, the general principles of protection and the rights of the holder provided for in this Law*".

Data can be critical to detection, investigation, and prosecution, and can help predict patterns of crime while preventing its non-occurrence [19].

For the exploitation of these data to be managed effectively, their collection must be done reliably.

In the search for data on trafficking in persons, although in most cases the data are not comparable, there are many obstacles to transport such as differences in measurement units, imprecise definitions, and improper classifications [20]. One of the main obstacles is when there is a lack of specific legislation on trafficking in persons, which leads to a lack of official criminal justice statistics on human trafficking cases [21].

VIII- CRIME FIGHTING

Several measures can be applied to combat the crime of trafficking in persons. The first one is the internal legal provision of each country. Then, the form of implementation of the law.

For this, we made a comparative study between the internal legal provision of Brazil and Portugal.

After that, we sought to study the forms of digital evidence for the investigation of crime.

We proposed some measures to be adopted in the fight against crime, among them, the use of machine learning to detect suspicious content of text messages, images, and videos; as well as to identify the main factors that determine the increase in the crime rate, such as unemployment and gender inequality.

IX- COMPARATIVE LEGAL ANALYSIS: BRAZIL-PORTUGAL

Portuguese domestic legislation, which deals with human trafficking, is provided for in article 160 of the Portuguese Penal Code (Decreto-Lei nº 48/95, 15 de março); while, in Brazilian legislation, the provision is in article 149-A of the Brazilian Penal Code (Decreto-Lei nº 2.848/1940, 7 de dezembro).

Portuguese legal doctrine classifies the crime of trafficking in persons as one that affects eminently personal legal assets (art. 30 of the CP), that is, assets that are rooted in the person himself, in his personality, and considers the correspondence of a victim for a crime.

Thus, Portuguese cybercrime law only provides for crimes about computer systems. Therefore, crimes that affect other legal interests, such as eminently personal ones, were not covered by this law.

Despite this, the cybercrime law itself refers to an order of the *Procuradoria Geral da República*, Order No. 14115/2013 such order is concerned with combating "the possession, manufacture, and distribution of child pornography, the instigation of minors to practice sexual acts, child prostitution, or the sending of material of an obscene nature to children".

However, according to the aforementioned order, the production of evidence to identify the criminal by the competent authorities is aimed at collecting data regarding the electronic mail and the IP address used. Such a procedure is ineffective when the crime occurs through onion services pages, using the anonymization of the user and the service itself.

In Brazil, computer crimes are embodied in the Penal Code. It also includes a legislative provision of specific crimes that are restricted to "invasion of a computer device", "electronic fraud"; "interruption or disturbance of telegraphic, telephone, computer, telematic or public utility information service". The concern about the exploitation of the human person through a computer system is contained in child pornography, through the ECA (Statute of Children and Adolescents) in article 241-A.

In Portuguese domestic legislation, the Penal Code deals with crimes of abuse against minors (article 171 and following, CP), even though the use of technologies (articles 176 and 176-A, CP), whose legal interest is freedom and sexual self-determination.

Therefore, the crime of trafficking in persons is restricted to traditional criminal legislation in both countries.

Some differences in the legislation can be observed: The crime in the simple form carries different penalties, while in Brazil the penalty is imprisonment from 4 to 8 years and a fine; in Portugal, the prison sentence is from 3 to 10 years.

In addition, Brazilian criminal law reduces the penalty from one to two-thirds if the perpetrator is a primary offender and does not belong to a criminal organization; allows parole if the convict is not a specific repeat offender in crimes of the same

nature, and if more than two-thirds of the sentence has been served (article 83, item V, CP/BR).

Both the cybercrime law and the Portuguese Penal Code, as well as the Brazilian Penal Code and the ECA, were omitted by failing to provide for illegal acts on the Internet that violate legal rights that protect the human person, when it comes to trafficking in persons online, but only as some of its illicit purposes. In this sense, illicit trafficking in persons, even if it has its beginning and end on the Internet, is being subjected to the old criminal legislation already in force.

Another specificity has to do with the issue of consent, brought in Portuguese legislation and ignored by Brazilian legislation.

Portuguese legislation provides in article 160, paragraph 3, for the penalization of conduct related to recruitment, transport, accommodation, and reception, regardless of the means, in the case of minors: "if the agent uses any of the means". There is no such provision in Brazilian legislation.

Unfortunately, for adult victims, these criminals can only be indicted for human trafficking if all three elements of the crime are proven to exist. There is still no legal provision for acts that occur separately, such as only the act of enticement on social networks, as there is no such autonomous criminal type, of enticement on social networks, without the realization of the other elements of the crime of trafficking in persons; as well as, there is no penalty for the use of adult pornography, for the financial gain of images and videos resulting from the exploitation of the human person. The only exception is for the illicit trafficking of minors and child pornography on the Internet.

X- THE USE OF DIGITAL EVIDENCE FOR FORENSIC INVESTIGATION

Prosecutors and investigative authorities can use digital evidence that will be taken to court to guarantee convictions through digital forensics.

There are useful and often incriminating sources of digital evidence such as [22]:

• Phone data – given the reliance of modern dealers and smugglers on their smartphones, which means that a large amount of evidence is available on these devices;
• Social media posts – Images, videos, contacts, associates, locations, and other information may be collected from social media accounts;
• Digital footprints – including browser history, personal computers, and IP addresses;
• Images taken with cell phones or digital cameras – as they contain metadata that can provide information about the camera used, as well as the images themselves, such as their dimensions and formats. Metadata can match images to devices in a suspect's possession. Additionally, metadata can help provide dates when images were captured and crimes committed. Geo-tagging can also be used to determine the location at which a material event occurred;
• GPS data can be used to track device location and history.

An example of the use of satellite technology is Geospatial: the Slavery Observatory project carried out by the University of Nottingham uses geospatial intelligence to detect cases of slavery. In 2016, the Telegraph reported that this research was used to uncover five hitherto unknown labor camps in Bangladesh suspected of child slave labor [23].

There was a case in the United States in 2011 in which a man pleaded guilty to human trafficking after posting commercial services of minors on the website Backpage (a site of sexual advertisements). Investigators used GPS data from the dealer's car to establish the locations of various customers [24].

XI- USING MACHINE LEARNING TO DETECT CRIME

a) Through techniques that detect suspicious content in text messages:

In a study carried out in Ecuador [25], using ML classifiers, more precisely the Naîve Bayes and SVM (Support Vector Machine) algorithms, using semi-supervised learning, it was possible to classify Twitter messages as "suspicious" or "not suspicious" for the related crime trafficking in persons for sexual exploitation.

The tweets were captured in real-time by the Tweety API (open source API), with data being stored daily for harvesting in a JSON (JavaScript Object Notation) file that is collected containing the tweet text, user information, mentions, associated URLs and the time posted.

Through the use of these machine learning algorithms, it is verified whether the tweets are targeted at the segment of girls under 18 years of age to be promoted for meetings with the illicit purpose. One of the factors used in this study was the age of the victim.

In addition to the associated age, other criteria were used taking into account the analysis performed on tweets and Facebook messages that have already been denounced as guilty of

trafficking for sexual exploitation of minors, such as the identification of keywords. Of the 100,000 tweets extracted, a total of 55,123 tweets were chosen that were most relevant because they had more than one hashtag selected, that is, keywords, as shown in the following table:

Hashtag	Numbers of occurrences
#escort	45604
#prepago	15890
#jovem	3456
#dulce	1256
#fresca	1456
#nueva	5743
#flaquita	6580
#lolita	867
#penguin	23980
#caldodepollo	45990
#cp	34562
Tweets with a URL link	1765

Spreadsheet 1: The most relevant tweets.

All downloaded messages contain at least one of the hashtags mentioned above and are stored locally in a local file.

The entire data mining process was designed to run the important software to detect the suspicion of messages via Twitter, but it could be used for any social network, as the criteria are the same.

Characteristics	**Reasons to consider them**
Quantities of words	Misleading messages have more words to make them forgettable
URL links and analysis if they are nightclub websites or massage therapy websites	This is to detect the use of Twitter to promote these sites
Third person use	Misleading messages have few self-references to avoid liability. On the other hand, other people could warn the service victims.
Same Twitter user talking about more than one victim	Cover up advertising of illicit activities
The number of hashtags considered to collect the data	Confirming the relevance of Twitter
The number of adjectives and verbs is an indication of a possible misleading message	This number is high compared to standard messages because misleading messages are very expressive
Similar ads from the same account promoting different women are a substantial advantage	Known sex trade signal
Woman's weight	Less than 100 pounds / 45.36 kilos can be a very young girl
One account is promoting more than two different women	Known sex trade signal

Spreadsheet 2: Characteristics and reasons to consider them

Through the Python program, it is possible to syntactically evaluate the highest frequency of adjectives and verbs in misleading message information, in addition to other resources such as 1) the number of words, probably always the maximum possible; 2) third-person speech recognition; 3) same Twitter user talking about more than one victim; 4) several defined hashtags present in the message; 5) mentions of girls from one country in messages from another country of origin; 6) several adjectives and several verbs; 7) similar advertising with the same words that promote different women; 8) mentions that might correspond to very young girls, and 9) an account promoting different women.

b) Through techniques that capture images:

A digital image can refer to a two-dimensional function that is sampled and quantified. The amplitude is quantified by a rectangular sampling mesh of equal distance and can be expressed by a two-dimensional matrix. In case we define a digital image as a digital representation of an object, then the pixel is a discrete unit and the quantized grey level is a digital quantity.

All images can be converted to codes. Colour images are also encoded. RGB is the abbreviation for an additive color system, in which red (Red), green (Green), and blue (Blue) are combined in various ways and reproduce a wide chromatic spectrum.

The importance of the RGB system for combating the crime of online human trafficking is due to its main purpose of color reproduction in electronic devices such as TV and computer monitors, digital cameras, as well as in traditional photography, among others, such as overhead projectors and scanners.

Therefore, it is easier to encode images from screens or computer screens and work with them using machine learning techniques for forensic investigation.

Child pornography detection: Machine learning techniques can be used, for example, to detect an object belonging to a victim, when a victim's teddy bear has been identified in a child pornography video; for facial recognition of a victim; or to differ adults from children, when the purpose is to identify images of child pornography online.

These are always hypotheses in which there is a large amount of data that is difficult to investigate individually. For this, deep convolutional neural

networks (CNNs) can be used, for example, to learn discriminative patterns directly from training data.

Deep learning proposes a better method than those based on hash and can be used in a complementary way. This is because the hash-based technique is effective in comparing similar content already annotated, but ineffective in identifying new content, not yet seen by the machine. Hash-based machine learning only identifies data that has already been processed, but for new data entered, other methods must be used to identify content from unsupervised machine learning, such as neural networks.

Thus, the two techniques can be used in a complementary way, since the contents are the most varied when the images are of sexual exploitation on the Internet, and may or may not present novelties not yet recognizable by the machine.

For the content to be recognized as child pornography, 2-level solutions can be used, with adjusted neural network weights, where an image of pornographic content is differentiated from an image of non-pornographic adult content (adults/pornographic vs. non-pornographic content), and then the classification of child pornography (child pornography vs. adult and non-pornographic content) [25].

For training (source network), an order of millions of images is required. For target networks (tier 1 and 2) a smaller amount of images containing child pornography content and content that does not contain child pornography are required for fine-tuning.

For automatic detection of sexual exploitation images, for any new activity, we must rely on content-based methods and not other filename pattern-based methods. It is also recommended to avoid methods that have a high number of false negatives and false positives. Thus, learning methods with rich and discriminative patterns are envisaged, which are not based solely on one or two patterns, such as skin color or eyeball to differentiate children from adults.

XII- CONCLUSIONS

Usually, it is through the Surface Web that traffickers hide the crime behind lawful activities to avoid being discovered, such as selling equipment and offering jobs over the Internet. Therefore, the Surface Web serves both for recruitment for classic human trafficking, as well as for human trafficking for online exploitation.

We can identify a circuit for the victim to follow to reach the Dark Web. Firstly, the victim is recruited through the Surface Web, through various means, from job search, dating apps, advertisements for sales of articles on the Internet, and virtual friendships on social networks.

In turn, the victim is confident that she is in a situation of legality, where the true intention of the trafficker is not yet been revealed. Then, through threats or blackmail, the victim becomes aware of the situation, but for various reasons, has no means of going out alone without outside help.

It was possible to verify that there is not much difficulty for the Dark Web layer to be accessed for free, through the Tor tool, which guarantees anonymity. This guarantee favors the profitability of managers through the abuse of children and adults, especially women and girls, for sexual exploitation.

However, sexual exposure through the Dark Web entertains the most diverse aspects that go beyond prostitution or sexual exploitation, containing torture, bodily harm, and contempt for human dignities, such as zoophilia and genital mutilation, degradingly exposing images and videos for financial gain.

Therefore, exploitation on the Internet also serves to exploit personal data. Consent for any illicit purpose does not exclude the crime of trafficking in persons, as provided for in the Palermo Convention.

Websites offering onion services contain illegal content and incite crime to allow the consumer to upload images and videos for their financial profit.

The Dark Web thus contributes to profitability through the practice of illicit exploitation of people and exposure through payment in bitcoins. Cryptocurrency payment also offers advantages for crimes.

Although the largest number of victims of trafficking in persons are adult women, according to previous research, the legislation of Portugal and Brazil is not concerned with foreseeing crimes that jeopardize the dignity of these people on the Internet.

Both in Brazil and Portugal, the legal provisions for computer crimes are concentrated on specific crimes, aimed exclusively at those that jeopardize legal interests related to the security of computer systems. Other crimes, which put other legal assets at risk, such as life, physical integrity, or personal freedom, were not foreseen in crimes perpetrated in digital media, which are now foreseen in common crimes. Except when it comes to child pornography, there is already concern about instituting crimes of this nature in the computerized system.

When illicit trafficking occurs against adults and, mainly, women (considered the most affected

by previous research), the conduct of the action should be considered illicit, regardless of the means used to achieve the illicit ends of exploitation, thus not requiring the completion of the three constituent elements of the crime. Illicit conduct could be considered autonomous.

Regarding the investigation, the qualification and more hiring of women in the use of techniques to combat and prevent digital crimes would be essential for the effectiveness of the fight against crime.

The machine learning technique serves both to prevent and fight crimes. The methods used when there is a large amount of data, such as the use of hashing in addition to the advanced technique of deep convolutional neural networks, are our hope in the present day for the fight against crime.

ACKNOWLEDGMENT

To my family for all the support. To my advisor for having agreed to advise on a particularly challenging, and for his courage. For that, my respect and my admiration. Thank you for all the encouragement given.

REFERENCES

[1] United Nations, UN News, Global Perspective Human Reports, "UN Agency warns of impacts of a "human trafficking pandemic", July 9, 2021. Available at: https://news.un.org/en/story/ 2021/07/1756122.

[2] Tribunal Regional Federal do Brasil, da 4ª região, TRF-4, HC HABEAS CORPUS Nº 5049468-92.2020.4.04.0000/RS, RELATOR : DESEMBARGADOR FEDERAL JOÃO PEDRO GEBRAN NETO, IMPETRADO : JUÍZO SUBSTITUTO DA 22ª VF DE PORTO ALEGRE.

[3] Article 3, paragraph 'a', Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children.

[4] UNODC (United Nations Office on Drugs and Crime), *Global Report on Trafficking in Persons*, United Nations, New York, 2012, p. 9.

[5] *Ibidem.*

[6] UNODC, *Global Report on Trafficking in Persons* 2018, (United Nations publication, Sales No. E.19.IV.2), p.10. Available at: https://www.unodc.org/documents/data-and-analysis/glotip/2018/GLOTiP_2018_BOOK_web_small.pdf

[7] UNODC, *Global Report on Trafficking in Persons* 2020, (United Nations publication, Sales No. E.20.IV.3), p. 31. Available at: https://www.unodc.org/unodc/data-and-analysis/glotip.html

[8] United Nations, UN News, Global Perspective Human Reports, "A global model to combat violence against women", Opinion article published in the British newspaper Independent, June 29, 2021: "UN Secretary-General António Guterres discloses opinion article on what it calls a "parallel pandemic". Available at: A Global Model for Combating Violence Against Women | UN News

[9] UNODC, *Global Report on Trafficking in Persons* 2020, *ob.cit*., p. 11.

[10] COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS, COM(2012) 286 final, Brussels, 19.6.2012 (European Union Strategy for the Eradication of Trafficking in Human Beings 2012 2016), item 2.5 (3) Action 3: Understanding Internet recruitment.

[11] UNODC, *Global Report on Trafficking in Persons 2020, ob. Cit*., Chapter V, p.120.

[12] Dácio Castelo Branco; Claudio Yuge (eds.), *Entenda o que são mixers de criptomoedas e por que são usados por criminosos*, BleepingComputer, Intel471, novembro de 2021. Availabe at: Entenda o que são mixers de criptomoedas e por que são usados por criminosos - Canaltech

[13] *Ibidem.*

[14] Felicity Gerry QC; Peter Shaw, *Emerging and Future Technology Trends in the Links between Cybercrime, Trafficking in Persons and Smuggling of Migrants,* First International Conference on Transdisciplinary AI (TransAI), 2019, p.4.

[15] *Ibidem.*

[16] *Ibidem.*

[17] *Ibidem.*

[18] Court case 414 – Denmark, 2017; Eastern District Court of Denmark, Case numbers: AM2017.05.29H; AM2017.06.30Ø, AM2016.03.14B, AM2017.11.10B, AM2018.01.19Ø, AM2016.07.12B. Conviction, 2016 – 2018. URL: https://vidensbasen.anklagemyndigheden.dk/h/6dfa19d8-18cc-47d6-b4c4-3bd07bc15ec0/VB/61db3c73-f3c2-49c5-a551-b755b9f-cfc31?showExact=true; Denmark, City Court, ref. 9-3441/2015, conviction 14 December 2015.

[19] Felicity Gerry QC; Peter Shaw, *ob. Cit*., p.6.

[20] Kangaspunta K., *Collecting Data on Human Trafficking: Availability, Reliability, and Comparability of Trafficking Data*, in Savona E.U., Stefanizzi S. (eds) Measuring Human Trafficking, Springer, New York, NY, 2007. Available at: https://doi.org/10.1007/0-387-68044-6_4

[21] *Ibidem.*

[22] Felicity Gerry QC; Peter Shaw, *ob. Cit*., p.6.

[23] See Mark Latonero, Ph.D., *Human Trafficking Online The Role of Social Networking Sites and Online Classifieds,* USC (University of Southern California), Center on Communication Leadership & Policy, 2011, p.19.

[24] Myriam Hernández-Álvarez, *Detection of possible human trafficking in Twitter*, Departamento de Informática y Ciencias de la Computación - DICC Escuela Politécnica Nacional Quito, Ecuador, 2019 International Conference on Information Systems and Software Technologies (ICI2ST). Available at: https://orcid.org/0000-0003-4718-0400

[25] Paulo Vitorino, Sandra Avila, Mauricio Perez, Anderson Rocha, *Leveraging deep neural networks to fight child pornography in social media*, Journal of Visual Communication and Image Representation 50, Science Direct, Elsevier (2018), pp. 303-313 (p. 306).