Universitat Autònoma de Barcelona

Faculty of Political Science and Sociology

Bachelor Thesis

NEW THREATS TO HUMAN SECURITY IN THE EUROPEAN UNION:

EMERGING TECHNOLOGIES AS TOOLS IN HUMAN TRAFFICKING

Author: Aina Arqué Pascual

Tutor: Juan Pablo Soriano Gatica

Bachelor in International Relations

20th May 2022

CONTENTS

INTRODUCTION

Human trafficking is one of the most deplorable crimes, affecting millions of lives in both developed and developing countries. It is believed to be the third largest criminal enterprise in the world, following drug trafficking and counterfeiting, with a $150 billion annual revenue, according to the 2014 report of the International Labor Office. The same study reported a $46.9 billion annual revenue in developed economies and the European Union (EU). In addition, technologies, especially Internet, have expanded the ability of criminals to traffic persons for different types of exploitation (EUROPOL, 2014; Latonero et al., 2011; OSCE, 2020; UNODC, 2021). This accelerates the transnational nature of crime and operations involving transnational organized criminal groups and networks.

The aim of this research is to study how technologies are used to facilitate the crime of human trafficking, and what new threats this misuse poses for human security in the EU.

According to the art.3.a) of the United Nations (UN) Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children,

> "'Trafficking in persons' shall mean the **recruitment, transportation, transfer, harbouring 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 labour or services, slavery or practices similar to slavery, servitude or the removal of organs" (emphasis added).

Traffickers prey on people's desperation to escape not only from poverty, but also from natural disasters, conflicts, or persecution (UNODC, 2022a). It is important to distinguish between trafficking in persons and migrant smuggling. In contrast to human trafficking, which can take place domestically and internationally, "'smuggling of migrants' shall mean the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident" (art.3.a), UN Protocol Against the Smuggling of Migrants by Land, Sea and Air).

Migrant smuggling does not involve coercion by the smuggler; migrants agree to enter the country illegally, either voluntarily or as an escape from vulnerable situations. However, it is common that the crime starts as smuggling but turns into trafficking if the migrants are exploited, by being held for ransom, or to pay off a smuggling debt (UNODC, 2022b; UNHCR, 2022).

According to the European Commission (2020), during 2017 and 2018 there were 14.145 trafficked victims reported by EU Member States (MS), a higher number than the previous period (13.461 between 2015 and 2016), not counting that many victims remained undetected. Almost half of the victims of trafficking in the EU are European citizens. The top five EU countries in terms of citizenship of victims by were Romania, Hungary, France, the Netherlands, and Bulgaria. The top five non-EU countries in terms of victims' citizenship were Nigeria, China, Ukraine, Morocco, and India (European Commission, 2020). The urgency and concern are also reflected in the EU Strategy on Combating Trafficking in Human Beings 2021-2025:

> "trafficking in human beings remains a serious threat in the European Union, endangering thousands of individuals every year, particularly women and children. Traffickers prey on social inequalities as well as economic and social vulnerability of people, which have been exacerbated by the Covid-19 pandemic, making it easier for perpetrators to find victims. The pandemic also hindered victims' access to justice, assistance, and support, and hampered the criminal justice response to the crime. Moreover, traffickers moved to a new **business model of online recruitment and exploitation of victims**, making it more difficult for law enforcement and the judiciary to respond" (emphasis added).

We are at a moment of historical change in which technologies are changing the way we act by accelerating the flows of people, goods, capital, and ideas. Technological advances are an improvement in countless ways, but a threat to basic rights if misused. They remove physical and time-based barriers, leave no trace, and allow perfect document forgery and impersonation, among other things. In the case of human trafficking, new and emerging technologies make it easier for criminals to recruit, control, advertise and exploit victims, as well as to collect profits (OSCE, 2020). According to the UNODC (2021), the OSCE (2020) and the EUROPOL (2014, 2017, 2021) the most used technologies in human trafficking are information and communication technologies (ICTs), that allow

communication with victims and consumers, location tracking systems and surveillance devices, to monitoring victims, and cryptocurrencies, that permit moving criminal proceeds.

Human trafficking is a crime against the individual that violates fundamental rights and freedoms. Hence, I decided to conduct the study with security of people at the center of concern, and this is enabled by the concept of human security. Human security is "to protect the vital core of all human lives in ways that enhance human freedoms and human fulfilment" (UNCHS, 2003). A human security perspective invites protecting what we care most about in our lives: our basic needs, our physical integrity, our human dignity; "human security is about living **free from want, free from fear and free from indignity**" (UNDP, 2022).

In its 2022 special report, the UNDP includes the threats from digital technology among the new threats to human security, and advocates a human security perspective on how technology can undermine people's well-being, rights and capabilities.

In light of the above, this paper aims to provide recommendations to EU law enforcement agencies by answering the central question: **how does the use of new technologies in the human trafficking business threaten human security in the European Union?**

In order to answer this question and identify threats, I have made an extensive literature review, including documents of international organizations, such as UN organizations, policy papers and academic articles. When examining the application of technologies, I have relied mainly on reports from EU organizations.

This work is structured in four parts. First, I present the concept of human security and explain its applicability and relevance to the crime of human trafficking and to digital technology threats. Secondly, I identify and analyze which technologies are used the most in human trafficking, how they are used, how they can transform the crime and how they threaten human security. Thirdly, I briefly contextualize the EU efforts to face digital transformation and threats. Finally, I present conclusions of the study and a series of recommendations to EU law enforcement agencies to address technology-facilitated human trafficking from a human security perspective.

1. ANALYTICAL FRAMEWORK

In this section, I will explain the applicability and relevance of human security as a framework for the analysis of the threats posed by new and emerging technologies used for human trafficking activities.

1.1- ORIGIN AND SCOPE OF HUMAN SECURITY

Within International Relations studies, security has focused for many decades on the state interest, mainly in military terms (Baldwin, 1997; Neak, 2017). From this perspective, a state is secure if it can defend itself from any intrusion of its sovereignty by another state and citizens are safe if state is safe in this regard (Wylie, 2006). The post-Cold War era resulted in geopolitical changes that changed the approach to security and prompted the reformulation of the concept of security: a new unipolar power distribution; intra-state conflicts and violent non-state actors; social and environmental problems; and globalization (Caballero-Anthony, 2015).

The concept of “human security” was popularized and operationalized in the United Nations Development Programme's (UNDP) *Human Development Report 1994 (HDR 1994)* (Neak, 2017). This emerging concept criticizes State-centered approaches to security and advocates putting individuals, their rights, needs, welfare and development, at the centre of the study. In fact, the term understands security broadly: it is no longer about defending territory or the state, but about **ensuring the security of people in all its dimensions**, and that most threats to human security cannot be resolved without addressing structural violence and the underlying political, social and economic causes.

The report highlighted seven dimensions of security: economic security, food security, health security, environmental security, personal security, community security and political security. It further stated that human security is made up of freedom from fear and freedom from want.

Despite criticism of the ambiguity of the concept (Paris, 2001; Newman, 2016; Wibben, 2016), it generated important political changes thanks to its promotion by the UN. Thus, the *HDR 1994* was followed by other documents and institutions

aimed at shifting the formulation of security. We can highlight the UN Commission on Human Security, created in 2001, and its first report *Human Security Now* (2003), which included the need for empowerment of individuals to make choices concerning their security and introduced the freedom to live in dignity. With this, there is a consensus within the UN system that three are the pillars of human security, shown in table 1:

Table 1: the three pillars of human security.

FREEDOM FROM FEAR	FREEDOM FROM WANT	FREEDOM FROM INDIGNITY
Conditions that allow individuals and groups protection from direct threats to their safety and physical integrity, including various forms of direct and indirect violence, intended or not	Conditions that allow for protection of basic needs, quality of life, livelihoods and enhanced human welfare.	Conditions where individuals and groups are assured of the protection of their fundamental rights and allowed to make choices and take advantage of opportunities in their everyday lives.

Source: UNDP Special Report 2022 *New threats to human security in the Anthropocene*, 2022.

In the recent special report *New threats to human security in the Anthropocene*, the UNDP (2022) aims at "expanding the human security framework in the face of this new generation of threats". Among these new threats, the UNDP highlights conflict dynamics, dimensions of inequality, challenges to health systems and threats from digital technologies. Regarding the latter, the UNDP stresses the need to move the focus from a national security perspective to a human security perspective to determine the security implications of digital technologies for people.

1.2- HUMAN SECURITY FRAMEWORK TO TECHNOLOGY FACILITATED HUMAN TRAFFICKING

Considering the great technological changes that humanity is undergoing at an overwhelming speed, we must ask ourselves whether the concept of human security is broadened to include the threats arising or intensifying from the use of technologies, and whether security in the digital world will become a new dimension of human security where the international society has to promote

human rights, needs, opportunities and dignity. The UN and scholars are already calling for this adjustment of the concept.

Human trafficking has existed since time immemorial, but has now evolved with the use of technology in its perpetration. In order to explain the relevance of the human security paradigm to the case study, I will first explain its applicability to the phenomenon of human trafficking, and then its applicability to the specific case of digital technologies and ICT threats.

On the one side, analyzing the applicability of human security to human trafficking makes it possible to identify threats to human security posed by this crime. On the other side, analyzing the applicability of human security to technology risks permits the identification of threats to human security created or intensified by the use of technologies. As a result, a framework is developed to understand the relevance and seriousness of the use of technologies in accelerating human trafficking.

a) Human security framework to human trafficking

Trafficking is a threat for the state, as it undermines state's borders, sovereignty, autonomy and capacities (Adamson, 2006, as cited in Jonsson, 2008). However, the traditional state security approach is too narrow to explain the consequences of human trafficking on states involved, as it does not consider the implications of human trafficking for the well-being of individuals, their rights and needs. The human security perspective does comprehend the social, political and health costs to countries as it focuses on the consequences of human trafficking on individuals (Shelly, 2008).

Some of the political consequences of human trafficking are human rights violations, authoritarianism exercised by criminal groups and the impact on the guarantee of democracy and welfare state. Social threats include increased violence, distrust, poverty, and marginalization. Public health costs are based on the spread of diseases and damage in their workplaces, not to mention the psychological damage suffered by the victims and their families. These are few consequences of human trafficking, along with attacks on human rights like the right to life, liberty and security, freedom from slavery, freedom from torture, freedom of movement or the right to the highest attainable standard of physical

and mental health. All this hinders the enjoyment of freedom from fear, freedom from want, and freedom to live in dignity that compose human security.

b) Human security framework to technological threats

Digitalisation means turning processes, practices and structures into information-based ones (Brennen and Kreiss, 2014), it alludes to the development in which ICTs become used in practically all areas of human life. Cybersecurity refers to “the security of the digital environment, which constantly interacts with operations in the physical environment” (Limnéll et al., 2015). Indeed, ICTs suffer from systemic dysfunctions, errors in their use, abuses, and intrusions that are commonly approached from a national security perspective (Liaropoulos, 2015, as cited in UNDP, 2022). By bringing the concept of cybersecurity closer to that of human security, it would not only focus on protecting the design of infrastructures and national interests, but also interests, fears, rights, and needs that people experience in the digital world (Salminen and Hossain, 2018).

Human rights can be attacked in their digital or online dimension, as people can be scammed, supplanted, spied on, harassed, or threaten, among other attacks, through technological and online networks. It is necessary to remember that already in 2012 the Human Rights Council stated that "same rights that people have offline must also be protected online" (UNGA, 2012).

Following Salminen et al. (2020), as a policy tool, “human security is able to identify urgent issues, thereby allowing the adoption of measures to repel threats and promote security” and allows for a better realization of human rights in a changing environment, like the current technological revolution. This dynamic and broadened conceptualization presents an agenda that allows individuals to define what they perceive as threats and opportunities (Salminen and Hossain, 2018) and demand improvements (CHS, 2003).

c) Relevance and applicability of human security in the case of technology facilitated human trafficking

The arguments given above prove that human security approach allows an analysis of the ways in which human rights are violated throughout the trafficking cycle. If the misuse of technologies facilitate the violation of rights, they must be

understood as a source of threat to human security. We are talking about a change in operational modality to which the agenda must adapt to include the dangers that may arise from it.

At the same time, when formulating policies under human security, the objective is to articulate **people-centered, comprehensive, context-specific and prevention-oriented responses** that strengthen the protection of rights and freedoms (UNDP, 1994), as well as to identify States' obligations and contribute to their fulfillment. To this purpose, it is crucial not to neglect the digital world, where people currently exercise rights, duties and needs.

In essence, using human security as heuristic tool in the case study permits identifying the threats that the use of technologies in human trafficking poses to the well-being, rights and needs of people, complementing the national security perspective.

2. ANALYSIS

This section explores what new and emerging technologies are used to facilitate human trafficking, how they transform the crime and how, in doing so, they pose and increase threats to human security.

This section is organized in four subsections. The first subsection explains the role of most used technologies in human trafficking. The second concerns emerging technologies that may be used to facilitate crime in the future. The third explains the transformations resulting from this misuse of technologies, while the fourth analyzes the treats to human security arising from these transformations, taking as analysis dimensions the three pillars that made up human security.

2.1- TECHNOLOGIES FACILITATING HUMAN TRAFFICKING TODAY

In the following paragraphs, I will briefly explain how perpetrators and their associates use technologies to recruit, control, advertise, and exploit victims and to move criminal proceeds (OSCE, 2020).

a) Recruitment

The Internet and online platforms are the most used technologies for victim recruitment. In fact, according to the UNODC (2021) Global Report on Trafficking in Persons (GLOTIP) of 2020, recruitment of victims is almost devoid of physical violence, as traffickers frequently use deception. This report distinguishes two recruitment strategies: “hunting” consists of the trafficker pursuing a victim, usually through social media, pretending to seek friendship with them in order to manipulate them; and "fishing" consists of advertising fake job offers and waiting for victims to respond.

Internet enables anonymity and forging identities, as it can be challenging to identify the individual posting advertisements or texting in social networks (UNODC, 2021; ICAT, 2019). Traffickers rely on clearnet websites (visible pages indexed by conventional search engines) to contact victims as it offers access to more Internet users. Online platforms provide information that traffickers may use to profile potential victims and tailor their manipulation strategies (QC and Shaw, 2019; Latonero et al., 2012; Antonopoulos et al., 2020).

Smartphone applications (apps) also play an important, as they offer the same interaction opportunities as online platforms and many allow GPS tracking, which provides location of possible targets (Q.C. and Shaw, 2019).

b) Control

Technology makes it possible to avoid face-to-face contact, which hampers the investigation of human trafficking. Virtual monitoring of victims is common and includes threats via online or telephone, surveillance by monitoring phone records and access to platforms or apps, or tracking victims' location through phone tracking apps.

Hardware devices, such as cameras or microphones, are used to surveil the victim and the exploitation from any location. Cameras are used to obtain compromising images of the victim as means of gaining control through blackmail and threats. Another scenario is the hijacking of victims' social networks to post sexual content and damage their reputation, which serves as coercion, undermines the victim's credibility, and can result in account shutdown, causing isolation (QC and Shaw, 2019).

c) Advertisement

Traffickers advertise victims and “services” on the clearnet and the dark web. "Clearnet" refers to the Internet known to most users, consisting of publicly accessible pages indexed by conventional search engines. "Deep web" is the 90% of the Internet escaping search engines, such as pages protected by a paywall, databases or private areas. "Dark web" is the 0.1% of the deep web, and consists of hidden pages hosted on darknets. Darknets require specific software and use systems that anonymize IP addresses; therefore, they are shelter for illicit activities (EUROPOL, 2017; UAM 2022).

The clearnet allows reaching a larger number of users, where raffickers advertise their victims' “services” under the guise of a legitimate job (e.g., massage service, escort, cleaning and domestic service) to avoid detection (UNODC, 2021).

Traffickers cannot easily disguise other types of exploitation such as forced marriage, forced criminality, organ trafficking or child trafficking. Hence, they conduct these activities on darknets (OSCE, 2020), which play a major role in the distribution of child abuse material (EUROPOL, 2021; UNODC, 2021; Raets and Jenssen, 2021; Antonopoulos et al., 2020).

d) Exploitation

“Clearnet” and “darknet” platforms are used for exploitation, especially sexual exploitation. Some sites make possible to livestream abuses and acts of exploitation, reaching a large base of consumers in different locations and with unlimited views and audience (UNODC, 2021; Antonopoulos et al., 2020; Latonero et al., 2011; Raets and Janssen, 2021). The larger the client base is, the more profits increase. This type of exploitation is known as “cyber trafficking”.

Indeed, Internet allows traffickers to connect themselves, victims and final consumers across geographical distances. Cyber trafficking may or may not require transporting the victim out of their country or place of residence, as traffickers may keep the victim in captivity, or even while the victim is at their home, they can be forced through threats and coercion.

e) Movement of criminal proceeds

Darknets and cryptocurrencies have been identified by EUROPOL (2015, 2017, 2018, 2021) as key enablers of crime in the 21st century. As darknets hide and encrypt IP addresses, they make it very difficult to identify who is behind the

transactions, which can be released using prepaid debit cards or cryptocurrencies.

Cryptocurrencies are increasingly being misused, whether on the darknet or on the clearnet, to fund crime or launder the proceeds of illicit activities (EUROPOL, 2021). Cryptocurrencies, such as Bitcoin, are virtual currencies founded on online technologies, cryptography and blockchain, that allow secure and direct transfer systems without intermediaries (EUROPOL, 2022). Cryptocurrencies eliminate the need to launder cash, which is difficult in most states due to regulations on cash declaration and money laundering compliance. In addition, the use of multiple digital "wallets," one for each transaction, challenges the authorities to track transactions (EUROPOL, 2015, 2018, 2019; OSCE, 2020).

2.2- FUTURE TRENDS

So far in this study, I have reviewed the technologies currently used to facilitate human trafficking. There are, however, certain emerging technologies that may play a role in the future of human trafficking. This section aims to identify them and briefly discuss their potential role.

a) Artificial Intelligence

“Artificial Intelligence (AI) is the simulation of human intelligence processes by machines, especially computer systems. These processes include learning, reasoning and self-correction” (OSCE, 2020). Thereby AI systems can take or suggest actions with certain autonomy (EUROPOL, 2019).

AI enables applications such as device and system security, machine translation, facial and voice recognition, and medical diagnostics. Human traffickers could use AI to customize and automate the search and identification of potential victims, automate the monitoring of victims and services, advertise and sell illicit services, distribute content, interact with consumers, and calculate profits (EUROPOL, 2019; QC and Shaw, 2019).

b) 5G and Internet of Things

One of the most important developments in our digital society is the fifth generation of telecommunication systems (5G). 5G enables exceptionally low latency, which is the delay between the sending and receiving information, which

goes from 200 milliseconds with 4G, to 1 millisecond with 5G (Deutsche Telekom, 2022).

5G will enable devices to connect and communicate with each other without operator networks in between, making it difficult for law enforcement to access information. For example, 5G will replace identifiers on cell phone cards that enable location tracking. Consequently, it may render certain investigation techniques obsolete, facilitating the commission of illicit activities (EUROPOL, 2018, 2019).

The 5G network will boost Internet of Things technology (IoT), which refers to the growing network of interconnected physical devices that enable Internet connectivity and communication between them. IoT devices benefit from AI, ML and real-time analytics that enable automation of functions and cost reduction (Gillis, 2022). In the case of human trafficking, IoT could facilitate the connection, communication and coordination between devices such as cameras, microphones, and home appliances such as sensors, and smart doors and windows, which would facilitate the control of victims and their exploitation.

c) New transport infrastructures

As EUROPOL (2015) reports, in the future, the convergence of digital technologies with transport infrastructures will be crucial to guarantee efficient and effective transport networks and new types of vehicles, such as unmanned automated vehicles.

Criminals will use intrusion into technological infrastructures to manipulate transport routes, infiltrate supply chains and collect valuable data. In the case of human trafficking, victims could be transported in unmanned automated vehicles to travel by land, sea and air without engaging in physical contact with facilitators.

2.3- TRANSFORMATION OF HUMAN TRAFFICKING THROUGH TECHNOLOGY

This section summarizes the transformation that new and emerging technologies produce in human trafficking. The first question to be answered is whether the use of technologies transforms human trafficking into an entirely new crime and

threat, or whether it has exacerbated an existing one. To answer this question, we must consider the three elements that constitute trafficking in persons according to the art.3.a) of the UN Protocol to Prevent, Suppress and Punish Trafficking in Persons, listed in table 2. For a definition, see the Introduction of this paper.

Table 2: Three core elements that constitute the crime of human trafficking.

ACT	MEANS	PURPOSE
The trafficker must do one of the following to people: - Recruit - Transport - Transfer - Harbor - Receive	**Using these methods** - Threat or use of force - Coercion - Deception - Fraud - Abuse of a position of vulnerability - Giving payments or benefits - Abduction	**For exploitation**

Source: art.3.a) UN Protocol to Prevent, Suppress and Punish Trafficking in Persons (UN, 2000).

As developed in the previous sections and summarized in table 3, technologies can be used to achieve each of these elements. Traffickers use technologies to deceive, defraud, coerce, and threaten victims in order to exploit them, on occasions also through technologies. As for future trends, they would serve the three elements because they personalize and automate these processes of deception, fraud, use of force, control and exploitation.

Table 3: the analyzed technologies and their use in human trafficking stages.

	Recruitment of victims	Control of victims	Advertisement of victims	Explotation of victims	Movement of criminal proceeds
Current use					
Internet "clearnet" platforms and smartphone apps	✓	✓	✓	✓	
Internet "darknet" platforms			✓	✓	✓
Telephones		✓			
Cameras and microphones		✓		✓	
Cryptocurrencies					✓
Future trends					

Artificial Intelligence (AI)	✓	✓	✓	✓	
5G and Internet of Things (IoT)		✓		✓	
New transport infrastructures		✓			

Source: author's own elaboration.

In this light, technologies do not add any additional element that substantially modifies the crime so as to make it a new one. Therefore, we are talking about a transformation of the crime. At least, for now.

This transformation through technologies has achieved three major impacts:

a) Facilitation of recruitment and control of victims

The possibility to recruit victims without face-to-face interaction and eliminating distances expands the crime to the digital domain and to new territories being able to reach more victims Traffickers may use information from victims' social networks to tailor their grooming strategy to deceive and defraud.

Technologies allow traffickers to shift from traditional violent methods to more subtle forms of victim control and manipulation, and to move from on-site control to control from any location.

b) Expansion of the market and profits

Human trafficking can be perceived as an illegal market where people are commodities. Internet permits the maximization of profits, on the clearnet and the darknet, where advertising is cheap, even free, fast, and allows a large reach. The exposure of the online market permits traffickers to investigate and penetrate areas with higher demand and profitability. Additionally, technology enables new "services", such as cybersex trafficking, which allows reaching a larger customer base and, therefore, increasing profits.

c) Reduction of the risk of detection

Criminals can create fake online identities to deceive and communicate with victims, buyers and associates. Virtual interactions decrease the chance of detection by law enforcement, as they take place through disguised offers or in relatively private chatrooms. To avoid tracking, traffickers use prepaid phone cards and darknets that hide IP addresses. In addition, cryptocurrencies allow the movement of money without drawing the attention of banking institutions.

2.4- TRANSFORMATIONS THREATS TO HUMAN SECURITY

The threats and challenges that these three impacts of technological transformations on the human trafficking process pose to the three pillars of human security (**freedom from fear, freedom from want, and freedom from indignity**) are discussed below. Annex 1 provides a visual outline. Threats to society on the one hand, and to victims on the other, are considered. Not neglecting the fact that victims are part of society and are affected by the same threats.

a) Freedom from fear

Both the facilitation of recruitment and control of victims and the expansion of the human trafficking market and profits threaten freedom from fear as society not only fears the crime of human trafficking, but also fears that technologies can be used to facilitate and expand other types of crime or abuses. There exists a fear of using technologies because, as they serve different phases of human trafficking and other crimes, they are no longer perceived as safe tools. Given the presence of technologies in our lives, the fear of using them can be an impediment to the full enjoyment of daily life and opportunities, a fear related to freedom from want.

Victims of human trafficking fear for their physical and psychological integrity, for their freedom, for their lives. The use of technologies in their manipulation does not substantially change these fears, it simply facilitates the cause. Technologies add the fear of intrusion into privacy, as victims can be spied on even in the few moments when they are alone, and the fear of loss of reputation and credibility, events that destroy victims emotionally and assault their sense of dignity, which is related to freedom from indignity. In addition, the expansion of the market and the growth of profits may mean for the victims fear of further exploitation, more abuses and of different types.

The low risk of traffickers being detected may lead to increased impunity and criminal activity. The inability of institutions to protect fosters fear of human trafficking and other crimes and abuses, and the fear that in facing threats of different nature, such as economic or resource crises, natural disasters, or wars,

institutions are incapable of addressing them. Victims lose hope of getting out of their situation; fear for their lives escalates.

b) Freedom from want

Freedom from want relates not only to the protection of basic needs but also to the protection of quality of life and human well-being. The manipulation of victims and the expansion of the human trafficking market through technologies deprives society of safe connections and uses of technology, free from threats and with adequate protection measures.

If the authorities are not able to follow and mitigate crime, their legitimacy and credibility diminishes. A need arises in society for compliant, effective institutions that meet their duty to protect society and its rights.

It is known that human trafficking deprives its victims of basic needs such as medicines and health care, sufficient food and income, or full personal development. Technologies specifically facilitate the deprivation of the need for privacy and intimacy.

c) Freedom from indignity

Freedom from indignity refers to the protection of fundamental rights and freedoms, the promotion of a quality of life and human well-being that enable people to make choices and empower themselves. "Dignity is grounded on the universal belief that everyone has equal inherent worth and value, enshrined in Article 1 of the Universal Declaration of Human Rights: ‘All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood’" (UN, 1948, as cited in UNDP, 2022). A society that witnesses how human trafficking expands its business in an easy and undetectable way, violating fundamental rights and preventing a dignified life, sees the shared feeling of human dignity undermined. The threats, fears and needs discussed above constitute a direct attack on fundamental rights and freedoms, quality of life and freedom of empowerment; an attack on human dignity.

Technologies facilitate the violation of rights and freedoms that has criminalized human trafficking throughout history, but specifically allow the violation of the right to non-interference in their private life, nor attacks on their honor or reputation.

The conducted analysis reveals the interlinkages between the three foundations of human security: being afraid prevents or hinders the fulfillment of certain needs and opportunities and the exercise of rights; being in need constitutes a fear that these will never be satisfied or will increase, and directly implies that certain rights are not realized; and ultimately, the inherent dignity of people is the basis for all human rights, which are violated if fears and needs exist.

3- WHAT IS THE EUROPEAN UNION DOING?

The following lines provide a brief summary of the EU's most relevant efforts to address digital transformation and the threats from the misuse of technologies.

The EU is implementing a "Digital Strategy", consisting of a “Digital Compass” and a new approach, to make the digital transformation work for people and businesses. The Digital Compass, established in 2021, is a framework to achieve the digital targets for 2030. It unfolds four cardinal points: digitally skilled citizens and highly skilled digital professionals; secure, performant and sustainable digital infrastructures; digital transformation of businesses; and digitalization of public services. The Commission would develop EU trajectories for each target, with MS, which would in turn propose national roadmaps (European Commission, n.d.-b). The strategy follows an approach based on three pillars to achieve a digital transformation that benefits people while respecting European values: technology that works for people, a fair and competitive digital economy, and an open, democratic and sustainable society (European Commission, n.d.-c).

Conscious that a successful digital transformation requires rights to be exercised online, the Commission proposed in January 2022 a declaration on digital rights and principles. The European Parliament and Council are invited to discuss the draft declaration and endorse it at the highest level by summer 2022 (European Commission, n.d.-a).

Regarding threats specifically, the EU has relied on a Cybersecurity Strategy since 2020, which “aims to ensure a global open Internet with strong safeguards

where there are risks to security and the fundamental rights” (European Commission, 2022). It provides guidelines for regulatory, investment and policy initiatives in three action areas: resilience, technological sovereignty and leadership; operational capacity to prevent and respond; and cooperation.

Of particular note is the European Cybercrime Center and the European Multidisciplinary Platform against Criminal Threats, created within Europol. The first investigates online crime, and the second investigates organized international crime, including online criminal services and human trafficking (European Council, 2022).

Concerning human trafficking, the EU Strategy on Combatting Trafficking in Human Beings 2021-2025 recognizes the urgency of addressing the "new business model" of traffickers, and that it must be addressed with technology, especially with digital evidences that relieve victims of difficult situations. This policy encourages awareness-raising activities on safe use of technologies and cooperation with the private sector to develop technology-based solutions.

It stands out that the EU Digital Strategy aims to empower Europeans and give them control of the digital transformation so that it does not undermine their rights. A project such as the declaration on digital rights and principles provides a clear reference on the kind of digital transformation Europe stands for. The Cybersecurity strategy focuses on risks to security and the fundamental rights of people, although it does not emphasize empowerment. Attention to victims and education place the focus on the well-being and opportunities of the individual. Overall, in the face of new technologies, the EU is developing policies in line with its traditional values, adopting a perspective close to human security: a people-centered, comprehensive, context-specific and prevention-oriented response.

In line manner, it is clear that online crime is high on the EU agenda and that technologies are part of the problem and part of the solution. The development of technologies to combat human trafficking and training on technology and on safe use are of great relevance. This belongs to the purpose of empowering people so that they are able by themselves to exercise their freedoms and opportunities without fear nor risk.

4- CONCLUSIONS AND RECOMMENDATIONS

This section will first present the conclusions of the study, followed by suggestions for future research, and will conclude with recommendations for EU law enforcement agencies to undertake initiatives focused on human security. The central question of this research was: how does the use of new technologies in the human trafficking business threaten human security in the European Union? My proposal has been to focus on the individual given my belief that security is as much about people as it is about states. I am not suggesting that state security is irrelevant to general welfare, but that the human security approach complements the state-centric approach to security.

I have found that the technologies used in human trafficking do not create a new crime, but rather transform it, since they are used to facilitate and hide the processes of recruitment, control, advertising, and exploitation of victims and the movement of criminal proceeds. This has three major impacts: the facilitation of recruitment and control of victims, the expansion of the market and profits, and the reduction of the risk of detection by police forces. All this threatens security in its three pillars freedom from fear, from want and from indignity, resulting in the emergence and intensification of fears and wants, and the infringement of rights and freedoms that prevent people from living in dignity (see annex 1). This analysis proves the linkages between the three foundations of human security: one is not realized without the other two. The findings demonstrate that the concept of human security is very relevant to the case study, because it has been possible and successful to broaden it to include the threats that the use of technologies in human trafficking poses to people's welfare, rights and needs, complementing the national security perspective.

Lastly, it has been observed that digital transformation and the threats that may arise from it are a priority for the EU. To address these areas, the EU is implementing policies and instruments centered on people's rights and empowerment, following an approach close to human security. The presence of a human security perspective in the EU's instruments for combating technological threats should be subject for future studies.

There is sufficient literature on the applicability of the concept of human security to human trafficking threats, and to purely cyber threats and crimes such as cyber-attacks, hacks, hijacking or data theft. There exist, however, very few references to the human security implications of technologies as enablers of established crimes, which evidences the need for further exploration of this dimension.

This lack of references has presented the greatest difficulty in my work. It is complicated to develop indicators to assess human security, as the concept is dynamic, since what people consider “vital” varies according to individuals and societies (UNCHS, 2003). I have employed freedom from fear, from want and from indignity as analysis dimensions due to the well-established consensus that they represent aspirations for human security. It has been challenging but useful to explore how the three pillars relate to beliefs and interact with each other, as UNDP (2022) already states.

To close the study, the following is a list of recommendations for law enforcement agencies of EU MS to adopt initiatives focused on human security when fighting the use of technologies for human trafficking purposes.

1. Clearly understand the problem of technology-facilitated human trafficking and the purpose of technology-based solutions, by providing training on the consequences of the use of technologies in human trafficking for people; training on their functioning, their risks, and what they are capable of achieving; and education in technology ethics, in order to ensure that technology-based solutions are actually a solution and do not add to the problem by undermining individuals' rights and freedoms.
2. Keep abreast of changes in both technology and human trafficking context by providing continuous training; consider the experience of victims to learn about their cases, how technologies were used on them, and how they felt threatened, in order to improve people-centered, comprehensive, context-specific and prevention-oriented responses.
3. Collaborate with EU MS, prosecutors, victim service providers, and NGOs to establish formalized communication channels for training, resources, and information sharing, rather than relying on requesting information on specific cases.

4. Develop partnerships with online platforms, social networks and apps providers to implement solutions to combat and prevent human trafficking on the platforms. For example: raising awareness and instructing safe use on such platforms; introducing or improving tools on the platforms for anonymous reporting of suspected cases of trafficking; offering parental control options.
5. Collect more and more representative statistical data to assess the quantitative impact of the use of technologies for human trafficking in the EU. No representative data are currently available.
6. Provide a hotline, online chat and smartphone app for emergencies and reports related to human trafficking.
7. Enhance capacities for the identification of victims and potential victims of trafficking on the Internet. For example: using visual processing software to detect photos and videos of victims trafficked for online sexual exploitation or detecting hotel rooms where victims may be held.
8. Organize prevention and education campaigns targeting vulnerable sectors and schools. Technologies offer the possibility to livestream workshops on the topic thus reaching a larger audience.
9. Increase the use of digital evidences to prevent victims from and help them in difficult and traumatic experiences of the legal processes. For example: using videos and images together with facial recognition and facial reconstruction AI to support in testifying and describing traffickers and abusers; using applications that allow to interview victims in different languages.
10. Include in the rehabilitation plan for victims initiatives aimed at removing the fear of using technologies and instructing a safe use of them. In this vein, technologies could provide e-learning platforms to educate victims in job skills.

Technologies emerged to facilitate and improve our daily lives. If we do not address the implications for human security, they will end up serving the opposite purpose. This problem does not only concern the EU, but is a global-scale challenge that threatens all regions in the world.

REFERENCES

Antonopoulos G., et al. (2020) *Technology in Human Smuggling and Trafficking. Case Studies from Italy and the United Kingdom*. Springer.

Baldwin, D.(1997). The Concept of Security. *Review of International Studies, vol.23*, 5-26

Brennen, S., & Kreiss, D. (2014). *Digitalization and digitization*. Culture Digitally. http://culturedigitally.org/2014/09/digitalizationand-digitization/ [consulted on 05.03.2022]

Caballero-Anthony, Mely. (2015). *An Introduction to Non-Traditional Security Studies : A Transnational Approach.* SAGE Publications Ltd.

Deutsche Telekom. (2022). *5G speed is data transmission in real time*. https://www.telekom.com/en/company/details/5g-speed-is-data-transmission-in-real-time-544498 [consulted 20.04.2022]

European Commission (2020). Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims. Luxembourg: Publications Office of the European Union. https://ec.europa.eu/anti-trafficking/third-report-progress-made-fight-against-trafficking-human-beings_en

European Commission (2021). EU Strategy on Combatting Trafficking in Human Beings 2021-2025. Luxembourg: Publications Office of the European Union. https://ec.europa.eu/home-affairs/system/files_en?file=2021-04/14042021_eu_strategy_on_combatting_trafficking_in_human_beings_2021-2025_com-2021-171-1_en.pdf

European Commission. (2022*). The Cybersecurity Strategy*. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy [consulted: 10.05.2022]

European Commission. (n.d.-a). *Commission puts forward declaration on digital rights and principles for everyone in the EU.* https://ec.europa.eu/commission/presscorner/detail/en/IP_22_452 [consulted: 10.05.2022]

European Commission. (n.d.-b). *Europe's Digital Decade: digital targets for 2030*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_en [consulted: 10.05.2022]

European Commission. (n.d.-c). *Shaping Europe's digital future*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/shaping-europe-digital-future_en [consulted: 10.05.2022]

European Council (2022). *Cybersecurity: how the EU tackles cyber threats*. https://www.consilium.europa.eu/en/policies/cybersecurity/ [consulted: 10.05.2022]

EUROPOL. (2014). *Trafficking in human beings and the internet.* Intelligence Notification 15/2015. The Hague: SOC Strategic Analysis Team. https://www.europol.europa.eu/publications-events/publications/trafficking-in-human-beings-and-internet

EUROPOL. (2015). *Exploring tomorrow's organized crime.* Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/publications-events/publications/exploring-tomorrow%e2%80%99s-organised-crime

EUROPOL. (2017). *European Union Serious and Organised Crime Threat Assessment (SOCTA). Crime in the age of technology.* . Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/publications-events/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017#:~:text=The%20European%20Union%20(EU)%20Serious,makers%20and%20the%20wider%20public.

EUROPOL. (2018). *Internet Organised Crime Assessment (IOCTA)*. Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/iocta2018.pdf

EUROPOL. (2019). *Do criminals dream of electric sheep? How technology shapes the future of crime and law enforcement.* Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/media-press/newsroom/news/do-criminals-dream-of-electric-sheep-how-technology-shapes-future-of-crime-and-law-enforcement

EUROPOL. (2021). European Union Serious and Organised Crime Threat Assessment (SOCTA). A corrupting influence: the infiltration and undermining of Europe's economy and society by organized crime. . Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/publications-events/main-reports/socta-report

EUROPOL. (2022). *EUROPOL Spotlight. Cryptocurrencies: tracing the evolution of criminal finances.* Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20Spotlight%20-%20Cryptocurrencies%20-%20Tracing%20the%20evolution%20of%20criminal%20finances.pdf

Gillis, S. (2022). *What is the internet of things?* Techtarget. https://www.techtarget.com/iotagenda/definition/Internet-of-Things-IoT [consulted 28.05.2022]

ICAT. (2019) *Human trafficking and technology: trends, challenges and opportunities.* Vienna: UN Publication. https://www.un.org/sexualviolenceinconflict/wp-content/uploads/2019/07/report/human-trafficking-and-technology-trends-challenges-and-opportunities/Human-trafficking-and-technology-trends-challenges-and-opportunities-WEB...-1.pdf

International Labour Office (ILO). (2014). *Poverty: The Economics of Forced Labor.* ILO, 13. Geneva: ILO Publication. https://www.ilo.org/wcmsp5/groups/public/---ed_norm/---declaration/documents/publication/wcms_243391.pdf

Jonsson, Anna. (Ed.). (2008). *Human Trafficking and Human Security* (1st ed.). Routledge. https://doi.org/10.4324/9780203890912

Latonero, M., et al. (2011). Human trafficking online: The role of social networking sites and online classifieds. *Annenberg Centre on Communication Leadership & Policy*, University of Southern California.

Latonero, M., et al. (2012). The rise of mobile and the diffusion of technology-facilitated trafficking. Annenberg Centre on Communication Leadership & Policy, University of Southern California.

Limnéll, J., Majewski, K., & Salminen, M. (2015). *Cyber security for decision makers*. Edited by R. Samani. Jyväskylä: Docendo.

Neack, Laura. (2017). *National, International, and Human Security : A Comparative Introduction.* Vol. Second edition. Rowman & Littlefield Publishers.

Newman, E. (2016). Human security: Reconciling critical aspirations with political "realities". *The British Journal of Criminology, 56*(6), 1165–1183. https://doi.org/10.1093/bjc/azw016

OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings and Tech Against Trafficking (2020). Leveraging innovation to fight trafficking in human beings: A comprehensive analysis of technology tools. Vienna: OSCE publication. https://www.osce.org/files/f/documents/9/6/455206_1.pdf

Paris, R. (2001). Human security: Paradigm shift or hot air? *International Security, 26*(2), 87–102. https://doi.org/10.1162/016228801753191141

Q.C., Felicity. G., & Shaw, P. (2019). Emerging and future technology trends in the links between cybercrime, trafficking in persons and smuggling of migrants. *2019 1st International Conference on Transdisciplinary AI (TransAI)1, 1-9.* https://doi.org/10.1109/TransAI46475.2019.00009

Raets, Sigrid, & Janssens, J. (2021). Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business. *European Journal on Criminal Policy and Research 27, 1-24.* https://doi.org/10.1007/s10610-019-09429-z

Salminen, Mirva, & Hossain, K. (2018). Digitalisation and human security dimensions in cybersecurity: an appraisal for the European High North*. Polar Record, 54*(2), 108-118. https://doi:10.1017/S0032247418000268

Salminen, Mirva, Zojer, G., & Hossain, K. (Eds.) (2020). *Digitalisation and Human Security: A Multi-Disciplinary Approach to Cybersecurity in the European High North*. Palgrave Macmillan. https://doi.org/10.1007/978-3-030-48070-7

Shelley, Louise. (2008). Human security and human trafficking. In Anna Jonsson (Ed.), *Human Trafficking and Human Security.* Routledge, 10-26.

UAM (2022). *¿Tienes clara la diferencia entre DarkWeb, DeepWeb y Darknet?* https://www.uam.es/uam/vida-uam/bibliotecas/noticias/diferencias-darkweb-deepweb-darknet [consulted: 16.04.2022]

UN. (2000). Protocol Against the Smuggling of Migrants by Land, Sea and Air. https://www.unodc.org/documents/middleeastandnorthafrica/smuggling-migrants/SoM_Protocol_English.pdf

UN. (2000). Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime. https://www.unodc.org/res/human-trafficking/2021the-protocol-tip_html/TIP.pdf

UNCHS. (2003). *Human Security Now*. New York: UN Publication. https://reliefweb.int/sites/reliefweb.int/files/resources/91BAEEDBA50C6907C1256D19006A9353-chs-security-may03.pdf

UNDP. (1994). *Human Development Report*. New York: UN Publication. https://hdr.undp.org/sites/default/files/reports/255/hdr_1994_en_complete_nostats.pdf

UNDP. (2022). *New threats to human security in the Anthropocene. Demanding greater solidarity.* New York: UN Publication. https://hdr.undp.org/sites/default/files/srhs2022.pdf

UNGA. (2012). Resolution adopted by the Human Rights Council, No. A/HRC/20/L.3 The promotion, protection and enjoyment of human rights on the Internet. https://ap.ohchr.org/documents/E/HRC/d_res_dec/A_HRC_20_L13.doc

UNHCR. (2022). *Trafficking in persons*. https://www.unhcr.org/human-trafficking.html [consulted on 23.02.2022]

UNODC Conference of the Parties to the United Nations Convention against Transnational Organized Crime (2021b). Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons. Background paper. Vienna. https://www.unodc.org/documents/treaties/WG_TiP_2021/CTOC_COP_WG.4_2021_2/ctoc_cop_wg.4_2021_2_E.pdf

UNODC. (2021). *Global report on trafficking in persons 2020*. New York: UN publication. https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_15jan_web.pdf

UNODC. (2022a). *Human Trafficking*. https://www.unodc.org/unodc/en/human-trafficking/human-trafficking.html [consulted on 15.03.2022]

UNODC. (2022b). *Migrant Smuggling*. https://www.unodc.org/unodc/en/human-trafficking/migrant-smuggling/migrant-smuggling.html [consulted on 23.02.2022]

UNOHCHR. (2014). Human Rights and Human Trafficking. Fact sheet num.36. Geneva: UN Publication https://www.ohchr.org/sites/default/files/Documents/Publications/FS36_en.pdf

Wibben, A. T. (2016). The promise and dangers of human security. In J. Nyman & A. Burke (Eds.), *Ethical security studies.* Routledge, 114-127.

Wylie, G. (2006). Securing States or Securing People? Human Trafficking and Security Dilemmas. *Studies: An Irish Quarterly Review*, *95*(377), 7–17. http://www.jstor.org/stable/30095789

ANNEXES

Annex 1: Threats of the three impacts of technological transformation on the human trafficking process to the three pillars of human security.

		Freedom from FEAR	Freedom from WANT	Freedom from INDIGNITY
Facilitation of recruitment and control of victims	**Society**	- Fear of escalating human trafficking - Fear of the possibility that other crimes or abuses escalate with the use of technologies. - Fear of using technologies.	- Need for a safe use of technology, free from threats and with protection measures. - Need for effective institutions that comply with their duties to protect society and its rights.	Technologies **facilitate** the violation of: - The prohibition of discrimination - The right to life - The right to liberty and security - The right not to be submitted to slavery, servitude, forced or bonded labour - The right not to be subjected to torture and/or cruel, inhuman, degrading treatment or punishment - The right to be free from gendered violence - The right to freedom of association - The right to freedom of movement - The right to the highest attainable standard of physical and mental health - The right to just and favourable conditions of work - The right to an adequate standard of living - The right to social security - The right of children to special protection - The right to non-interference in their private life, nor attacks on their honor or reputation
	Victims	- Fear of intrusion into their privacy. - Fear of loss of reputation and credibility.	- Need for privacy and intimacy	
Expansion of the market and profits	**Society**	- Fear of escalating human trafficking. - Fear of the possibility that other crimes or abuses escalate with the use of technologies. - Fear of using technologies.	- Need for a safe use of technology, free from threats and with protection measures. - Need for effective institutions that comply with their duties to protect society and its rights.	
	Victims	- Fear of further exploitation	- Need for privacy and intimacy	
Reduction of the risk of detection	**Society**	- Fear of escalating human trafficking - Fear of the possibility that other crimes or abuses go unpunished and escalate - Fear that institutions are unable to address threats of different nature	- Need for effective institutions that fulfill their duties to protect society and its rights.	
	Victims	- Fear of not getting their lives back, feeling of unprotection.		

Source: author's own elaboration.