Global Campus Europe

EMA Awarded Theses 2019/2020

Ophélie Stockhem

Improving the International Regulation of Cybersex Trafficking of Women and Children through the Use of Data Science and Artificial Intelligence

EMA, The European Master's Programme in Human Rights and Democratisation

OPHÉLIE STOCKHEM

IMPROVING THE INTERNATIONAL REGULATION OF CYBERSEX TRAFFICKING OF WOMEN AND CHILDREN THROUGH THE USE OF DATA SCIENCE AND ARTIFICIAL INTELLIGENCE

FOREWORD

The European Master's Degree in Human Rights and Democratisation (EMA) is a one-year intensive programme launched in 1997 as a joint initiative of universities in all EU Member States with support from the European Commission. Based on an action- and policy-oriented approach to learning, it combines legal, political, historical, anthropological and philosophical perspectives on the study of human rights and democracy with targeted skills-building activities. The aim from the outset was to prepare young professionals to respond to the requirements and challenges of work in international organisations, field operations, governmental and non-governmental bodies, and academia. As a measure of its success, EMA has served as a model of inspiration for the establishment of six other EU-sponsored regional master's programmes in the area of human rights and democratisation in different parts of the world. Today these programmes cooperate closely in the framework of the Global Campus of Human Rights, which is based in Venice, Italy.

Up to 90 students are admitted to the EMA programme each year. During the first semester in Venice, they have the opportunity to meet and learn from leading academics, experts and representatives of international and non-governmental organisations. During the second semester, they relocate to one of the 42 participating universities to follow additional courses in an area of specialisation of their own choice and to conduct research under the supervision of the resident EMA Director or other academic staff. After successfully passing assessments and completing a master's thesis, students are awarded the European Master's Degree in Human Rights and Democratisation, which is jointly conferred by a group of EMA universities.

Each year the EMA Council of Directors selects five theses, which stand out not only for their formal academic qualities but also for the originality of topic, innovative character of methodology and approach, potential usefulness in raising awareness about neglected issues, and capacity for contributing to the promotion of the values underlying human rights and democracy.

The EMA Awarded Theses of the academic year 2019/2020 are:

• Caruana, Deborah, *Securitising Children Rights: Victims and Heirs of Terrorism. A Critical Analysis of France's Approach to Children of Foreign Terrorist Fighters.* Supervisor: Heidi Riley, University College Dublin, National University of Ireland, Dublin.

• Catalão, Mariana, *Environmental Justice, Climate Change and Human Rights. Different Contributions, Different Consequences and Different Capabilities Should Equal Different Human Rights Obligations.* Supervisor: Jan Klabbers, University of Helsinki.

• Houssais, Olivia, *Democratic Deficit Theory: A Reversed Approach. Why Radical Political Changes in Member States Affect the Quality of Democracy in the EU*. Supervisor: Anna Unger, Eötvös Loránd University, Budapest.

• Monteiro Burkle, Eduardo. *When Forgetting Is Dangerous: Transitional Justice, Collective Remembrance and Brazil's Shift to Far-Right Populism.* Supervisor: Alice Panepinto, Queen's University Belfast.

• Stockhem, Ophélie, *Improving the International Regulation of Cybersex Trafficking of Women and Children through the Use of Data Science and Artificial Intelligence*. Supervisors: Maria López Belloso and Demelsa Beniso Sánchez, University of Deusto, Bilbao.

The selected theses demonstrate the breadth, depth and reach of the EMA programme and the passion and talent of its students. We are particularly proud of EMA's 2019/20 students: as teachers and students across the world can testify, the COVID-19 pandemic brought many different challenges for teaching and learning. It is fair to say that our students researched and wrote their theses in turbulent times. On behalf of the Governing Bodies of EMA and of all participating universities, we applaud and congratulate them.

Prof. Manfred NOWAK
Global Campus Secretary General

Prof. Thérèse MURPHY
EMA Chairperson

Dr Wiebke Lamer
EMA Programme Director

This publication includes the thesis *Improving the International Regulation of Cybersex Trafficking of Women and Children through the Use of Data Science and Artificial Intelligence* written by Ophélie Stockhem and supervised by Maria López Belloso and Demelsa Beniso Sánchez, University of Deusto, Bilbao.

BIOGRAPHY

Ophélie Stockhem wrote her EMA thesis for the University of Deusto in Bilbao, Spain. Graduated in International Law in 2018, she always had a keen interest in women's rights and the social and legal implications of new technologies. After taking part in a summer school in 'IT law' in 2014, she did internships in the private and public sector that extended her knowledge of gender equality, privacy and digital tools.

ABSTRACT

Today, perpetrators of human trafficking for sexual exploitation are using cyberspace to recruit, advertise and exercise control over women and children, who are intrinsically more vulnerable to this crime. The Internet and mobile phone technology have indeed provided an avenue to facilitate considerably the trafficking process. Yet, no regulation is directly addressing the nexus between sexual exploitation and these digital tools. In addition to affirming the necessity to do so, researchers have, although more rarely, investigated the non-legislative path formed by partnerships between governments, civil organizations and private companies aiming to fight cybersex trafficking. This thesis intends to confront the main technologies used in trafficking networks with the legislation in force at the international and regional levels, and to question the opportunities that data analytics and artificial intelligence provide to combat this increasingly sophisticated crime. Through a legal, gender, and technology-focused perspective, it will emphasize the need to carefully examine practical and ethical issues, as well as the privacy and security concerns raised by tools mobilizing these two types of technology. On the one hand, it will confirm that there is a need, alongside the international and regional privacy legislative framework, to regulate the use of data analytics and AI techniques in a way that takes the specificity of cybersex trafficking into account. On the other hand, it will emphasize the compelling necessity to ensure the implementation of a gender-sensitive and interdisciplinary approach in these ICTs-supported anti-trafficking efforts.

ACKNOWLEDGEMENTS

I would like to express my deepest appreciation to my two thesis supervisors, who were present and supportive from the beginning to the end of this thesis writing process: Dr María López Belloso, who organised frequent Google Meetings and provided me with very exhaustive and invaluable feedback, and Dr Demelsa Benito Sánchez, who was of precious help, especially for issues related to the legislative framework of human trafficking. I am deeply indebted to the Global Campus of Human Rights, specifically to Drs Wiebke Lamer and Chiara Altafin, who helped in the early stage of my thesis proposal, as well as the University of Deusto, in particular to Dr Felipe Gómez Isa, who frequently checked with the advancement of my writing. Without the persistent help and guidance of these professors, the goal of this work would not have been realised.

The completion of this Master's thesis would not have been possible either without the 'virtual' support and nurturing of my parents, Anne Defooz and Michel Stockhem, and the unparalleled ears and laugh of my sister, Apolline Stockhem, which allowed me both to escape and refocus during these pandemic times abroad.

I would also like to extend my sincere thanks to Leonam Bernardo, my roommate who 'bore' my instrumental music background and cooked several times delicious Brazilian food, to my friends who supported me from Belgium, and in particular, to Camille Moerenhout, who, by writing her thesis at the same time as mine, participated greatly to my daily productivity and provided some 'complaining' times which are necessary to produce any work.

I am also grateful to Asier García Pérez, who was one of my main Spanish local points of contact in Bilbao and helped me with the language barrier in addition to introducing me to Basque culture, reminding me to have breaks and regularly proposing one of his several 'at-home' plans to escape confinement-provoked boredom.

TABLE OF ABBREVIATIONS

AI	Artificial intelligence
ASEAN	Association of Southeast Asian Nations
AWS	Amazon Web Services
BSR	Business social responsibility
CISPE	Cloud Infrastructure Service Providers in Europe
CoE	Council of Europe
CTDT	Counter-Trafficking Data Collaborative
EU	European Union
GDPR	General Data Protection Regulation
GEN	Global Emancipation Network
IBM	International Business Machines Corporation
ICAT	Inter-Agency Coordination Group against Trafficking in Persons
ICTs	Information communication technologies
IOM	International Organization for Migration
ITU	International Telecommunication Union
NGO	Non-governmental organisation
OECD	Organisation for Economic Cooperation and Development
TAHub	Trafficking Hub (IBM)
THB	Trafficking in human beings
UN	United Nations
UNODC	United Nations Office of Drugs and Crime

LIST OF FIGURES AND TABLES

TABLE OF CONTENTS

INTRODUCTION

Aiming at the exploitation of human beings in its most extreme manifestations, the human trafficking industry generates $150 billion annually and has today ensnared around 40.3 million human beings.[1] Trafficking in human beings (THB) is a complex phenomenon for it is related to several fields and driven by different forces, including but not limited to political instability, violence against women, the international labour market, unequal international economic relationships and the feminisation of poverty. It is therefore, above all, a complex economic problem, as infiltrates the real economy and impacts gross domestic product, all while targeting members of vulnerable domestic populations, especially women and children below and on the poverty line. Unsurprisingly, the recent COVID-19 pandemic crisis has therefore been exposing human beings at greater risk of being trafficked, due to the increase of transnational organised crime such as THB[2].

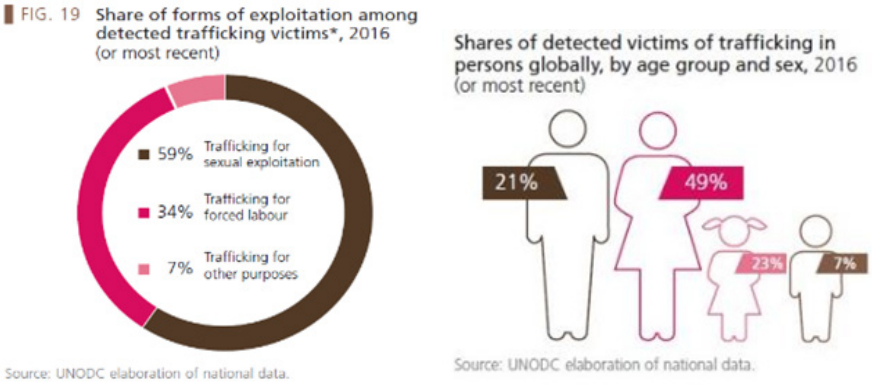
Figure 1. The driving forces of human trafficking.
Source: Trace Project Consortium, 'Tracing Human Trafficking, Handbook for Policymakers, Law Enforcement Agencies and Civil Society Organizations' (Trace 2016) 12.

[1] The statistics and charts provided in the introduction are stemming from the United Nations Office of Drugs and Crime (UNODC), *Global Report on Trafficking in Persons 2018* (United Nations Publications 2018).

[2] UNODC, 'COVID-19 Seen Worsening Overall Trend in Human Trafficking', 2 February 2021, <www.unodc.org/unodc/frontpage/2021/February/share-of-children-among-trafficking-victims-increases--boys-five-times-covid-19-seen-worsening-overall-trend-in-human-trafficking--says-unodc-report.html> accessed 10 April 2021.

Although THB may take other forms such as forced labour, this research will focus on the sexual exploitation of women, because it is by far the most identified type of THB, all while being a gender specific crime, targeting 94% of female individuals among identified victims globally. This can be mainly explained by social and cultural conditions inherent to being a woman: their exclusion from mainstream economic and social systems such as employment and higher education, the fact that they are often hidden victims of war and conflict, displaced persons or refugees, as well as, more generally, their relatively secondary status in the family and society. Finally, rape, domestic violence, harmful traditional practices and lack of or limited access to resources make women particularly vulnerable to trafficking, including to sexual exploitation.

Figures 2. Charts ONUDC.
Sources: United Nations Office of Drugs and Crime (UNODC), Global Report on Trafficking in Persons 2018 (United Nations Publications 2018).



However, due to the importance of child abuse, including child pornography and exploitation, considerations will be made about child trafficking as well, especially in the face of recent important developments in sociotechnical innovations attempting to combat the exploitation of this type of victim. It remains, however, that girls are particularly targeted by the crime, with a high risk of unsafe transportation modes, abuse at the hands of smugglers, forced labour, rape and sexual exploitation. Therefore, the perspective adopted throughout this work will primarily be gendered.

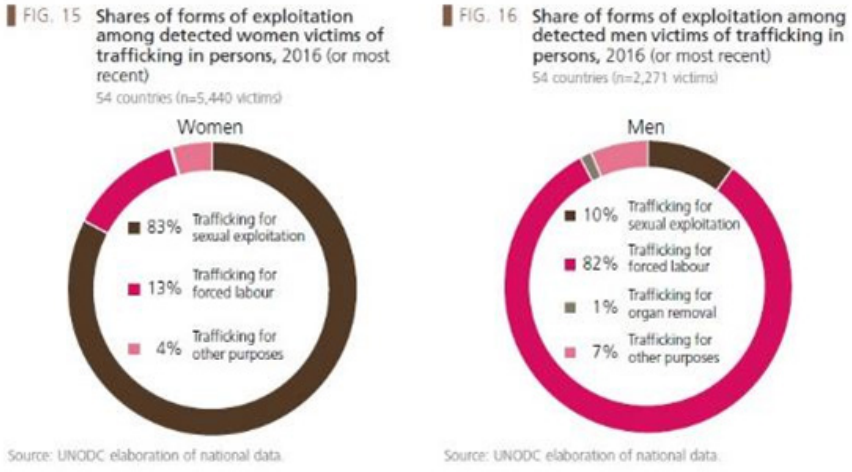
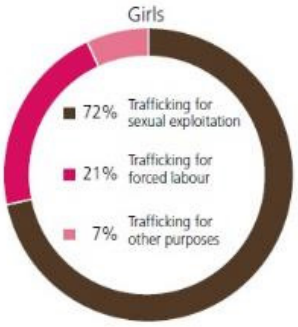
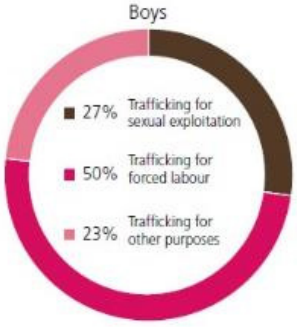


FIG. 17 Share of forms of exploitation among detected girl victims of trafficking in persons, 2016 (or most recent)
54 countries (n=2,350 victims)



Source: UNODC elaboration of national data.

FIG. 18 Share of forms of exploitation among detected boy victims of trafficking in persons, 2016 (or most recent)
54 countries (n=711 victims)



Source: UNODC elaboration of national data.

The personal motivation between this thesis emerged from a long-standing interest for technologies, the unanticipated consequences raised by their use in modern society and their relationship with humanity, coupled with a profound passion, as a lawyer, for questions directly or indirectly addressing the relationship between gender and law, and, in particular, topics that are closely related to violence against women.

These motivations quickly catalysed the idea to focus the research:

1) on the intricate relationship between the issue of forced work and gender-based violence; and

2) on the huge impact technological developments have, in the information age, on the increasingly sophisticated crime of sexual exploitation.

For the purpose of this thesis, reference will therefore be made to 'cybersex trafficking' or 'information communication technologies (ICTs)-facilitated sexual exploitation'. The following paragraphs will, moreover, always refer to 'technology' as understood as ICTs. The latter designates the means used by users to exchange digital information through networks such as the internet, social media and mobile phones.[3] As it will be shown, ICT tools, which are evolving and multiplying at an extremely rapid pace, provide a relatively anonymous forum, facilitate communication, provide particularly efficient and far-reaching advertisement methods, and allow perpetrators to recruit and control victims.

Bearing in mind that other types of digital technologies are currently used, this thesis will try to elucidate on the dynamic of visibility that seems to have emerged through the use of the internet and mobile technology by perpetrators. It will further support the position that sociotechnical innovation can also be used as a disruptive force against cybersex trafficking, through the use of data science and artificial intelligence (AI).

[3] European Commission. Eurostat <https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Information_and_communication_technology_ (ICT)>, accessed 14 April 2021

This research will try to confront the existing digital technologies used in trafficking networks with the legislation in force at the international and regional levels, emphasising the necessity to regulate ICTs to better track perpetrators, trafficking traces and victims through cyberspace. It will also question the opportunities that data analytics and AI can provide for front line law enforcement officers fighting sexual exploitation, all while including considerations about the drawbacks and pitfalls that partnerships around sociotechnical inventions may bring along with a focus on ethics, privacy and security concerns. This will be done through an interdisciplinary approach, combing legal, gender, child-sensitive and technology-focused perspectives.

After drawing up the existing legal framework regulating human trafficking for sexual exploitation of women and children in Chapter I, this work will, in its Chapter II, study the main legislation directly or indirectly involving big data and AI issues. Chapter III will identify the main tools used by traffickers through the internet and mobile technology and provide concrete examples of anti-trafficking initiatives in the area of data science and AI, all while taking account of the ethical challenges that the analysed technologies may raise and their potential conflict with other human rights. Finally, Chapter IV will try to assess how the regulation of ICTs-facilitated sexual exploitation of women and children can be improved in the future.

1.

LEGAL FRAMEWORK REGULATING TRAFFICKING IN HUMAN BEINGS AND SEXUAL EXPLOITATION OF WOMEN AND CHILDREN

The aim of this first chapter will be to analyse the efforts made by the international community as well as regional organisations to regulate human trafficking for sexual exploitation of women anwwd children, through the adoption of 'hard' law (1) and 'soft' law (2) forms. It will also include considerations about the inclusion of the technological aspect in this legal framework. The last section will address the anti-trafficking efforts of a non-legislative nature (3).

1.1 Legally binding instruments

Facilitated by globalisation, an international trend to deregulate the labour market, the occurrence of armed conflicts, migration and, more importantly, by the rise of the internet,[4] the survival of contemporary forms of slavery, in particular through the THB, pushed the international community, towards the end of the 20th century, to increasingly adopt legislation at the global level. Culminating in 2000 with the signature of the Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations (UN) Convention against Transnational Organized Crime (the Palermo Protocol or Trafficking Protocol),[5] this legislative movement gained prominence through the development of human rights norms and the fight against transnational organised crime.[6] Sexual exploitation was no exception to this incrimination trend.

However, when looking at legislation adopted at the international level, the most striking element, knowing that most of the trafficking activities take

[4] Tool 9.15 of the UNODC, *Toolkit to Combat Trafficking of Persons*, *Global Programme against Trafficking in Human Being*s (United Nations Publications 2008) 454.

[5] Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (adopted 15 November 2000, entered in to force 25 December 2003) 2237 UNTS 319.

[6] A-T Gallagher, 'Trafficking in Transnational Criminal Law' in R Piotrowicz, C Rijken and B Heide Uhl (eds), *Routledge Handbook of Human Trafficking* (Routledge International Handbooks 2017) 21.

place today in the cyberspace, making human trafficking a 'cyber-facilitated' crime,[7] is the absence of a universal instrument treating THB as a cybercrime to be prosecuted as such.[8] The following sections will therefore focus on legal instruments adopted to fight human trafficking, including sexual exploitation.

1.1.1 At the international level

Several treaties of international scope have been adopted in order to prevent, combat and prosecute the crime of human trafficking regardless of its technological dimension, including the fight against sexual exploitation. The main one is undoubtedly the Palermo Protocol, adopted by the General Assembly on 12 December 2000. Despite the existence of legislation combating the phenomenon, it is the first universal instrument that addresses all aspects of trafficking in persons and will therefore constitute the main focus of this section.

The Trafficking Protocol defines trafficking as:

> 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.[9]

This definition underlines three elements: the action (recruitment, transportation, transfer, harbouring or receipt of persons), the means (threat or use of force or other forms of coercion, abduction, fraud, deception, abuse of power or abuse of a position of vulnerability, or the giving or receiving of payments or benefits to achieve the consent of a person having control over another person), and the purpose (ultimately, the exploitation of human beings).

In addition to the existence of these three elements and although it does not completely clarify the heated debate about the still very obscure legal definition of trafficking in human beings,[10] the Palermo Protocol defines trafficking in an inclusive way, in particular from a gender perspective. Indeed, it does more than covering exploitation achieved through overt violence or total deception, recognising the unequal power dynamic and the impact of

[7] Europol, *Serious and Organised Threat Assessment, Crime in the age of technology* (Europol 2017) 4.

[8] A-P Sykiotou, 'Cyber Trafficking. Recruiting Victims of Human Trafficking through the Net' in C-D Spinellis, N Theodorakis, B. Emmanouil, and G. Papadimitrakopoulos, *Essays in Honour of Nestor Courakis* (Ant N Sakkoulas Publications LP 2017) 1547-87.

[9] Trafficking Protocol art 3(a).

[10] For a study of the main arguments formulated in this regard, see V Roth, 'Defining Human Trafficking and Identifying Its Victims. A Study on the Impact and Future Challenges of International, European and Finnish Legal Responses to Prostitution-Related Trafficking in Human Beings' (2011) 24(3) International Journal of Refugee Law 657.

the absence of choice or the authority of persons on women's decisions, but also the non-absolute character of consent, for instance when secured through treats, deception, abuse of power or other ways of exercising control.[11] It also explicitly provides in its article 2 a threefold statement of purpose: to prevent and combat trafficking in persons, paying particular attention to the protection of women and children, to protect and assist victims of trafficking, and to promote and facilitate cooperation among states parties to this end.

While it is true that the Palermo Protocol is the only treaty adopted at the UN level to combat THB, providing for the first time a firm ground to the phenomenon, two other treaties also partially address sexual exploitation. The first one is the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, adopted on 25 May 2000,[12] incriminating prostitution and sexual exploitation of children. The other is the Convention for the Elimination of Discrimination of Women,[13] which, through its article 6, provides a ground for the incrimination of the trafficking of women and the exploitation for prostitution.

Due to its specific focus on women and children, the Palermo Protocol undoubtedly provides the most comprehensive and relevant framework to date to combat sexual exploitation. However, it does not address the very important relationship between ICTs and the trafficking of women and children, although the technological aspect is playing a primordial role in modern society, as Chapter III will highlight.

The following section will address the legal instruments that have been adopted at the regional level, through the Council of Europe (CoE), the European Union (EU), as well as the African, Inter-American, Arab and Asian legal systems.

1.1.2 At the regional level

Although several regional instruments directly address the issue of THB for sexual exploitation, the main one is the CoE Convention on Action Against Trafficking in Human Beings.[14] The instrument goes further than the UN Palermo Protocol, which focuses on prosecution and punishment, by putting the emphasis on victims and defining THB as a violation of human rights. The preamble to the convention indeed defines trafficking as 'a violation of human rights and an offence to the dignity and integrity of human beings'.

Although the CoE Convention does not directly adopt a gender perspective

[11] K Maltzahn, 'Digital Dangers. Information and Communication Technologies and Trafficking in Women' (APC Issue Papers 2006) 3.

[12] Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, (adopted 25 May 2000, entered into force 18 January 2002) 2171 UNTS 227.

[13] Convention on the Elimination of All Forms of Discrimination against Women, (adopted 18 December 1979, entered into force 3 September 1979) 1249 UNTS 13 (CEDAW).

[14] Convention on Action against Trafficking in Human Beings, CETS 197.

nor link THB with technological developments, it remains, at this level, the main instrument tackling the issue of sexual exploitation. The Convention on Cybercrime,[15] addressing child pornography can, however, also be considered as an advancement in the prosecution of computer-related crimes, including cyber-trafficking, although it focuses mainly on children[16] and does not directly address the question of THB. Also worth mentioning at the CoE level are the Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse (Lanzarote Convention),[17] and, albeit indirectly, the Istanbul Convention,[18] which has been interpreted as addressing sexual exploitation of women through its constitutive elements in the provisions concerning physical, psychological and sexual violence,[19] since different forms of gender abuse have the potential to form a chain of elements which can eventually amount to a case of trafficking.[20]

At the EU level, the main legally binding instrument is undoubtedly Directive 2011/36/EU.[21] Considering trafficking as a violation of human rights similarly as the Palermo Protocol, it differs from previously adopted EU instruments by focusing on THB prevention and the protection of victims,[22] all while establishing additional measures regarding the investigation and prosecution such as a legal obligation of non-prosecution in addition to the non-imposition of penalties.[23]

Other legal instruments adopted by regional organisations to combat human trafficking would undoubtedly deserve to be mentioned here, but it is beyond the scope of this thesis to provide for a detailed legal framework analysis. These legally binding instruments and their relevant articles will therefore be listed in the following recapitulating table.

[15] Convention on Cybercrime, STE 185

[16] ibid art 9.

[17] Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS 201 (Lanzarote Convention)

[18] Convention on Preventing and Combating Violence against Women and Domestic Violence, CETS 2010 (Istanbul Convention).

[19] In particular art 25, guaranteeing the protection against sexual violence.

[20] European Institute for Gender Equality (EIGE), *Gender-specific measures in anti-trafficking actions: report* (EIGE 2018) 3.

[21] Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims and replacing Council Framework Decision 2002/629/JHA [2011] OJ L 101.

[22] A Pérez Cepeda and D Benito Sánchez, *Trafficking in Human Beings, A Comparative Study of the International Legal Documents* (Europa Law Publishing 2014) 13.

[23] In this regard, see R Piotrowicz and L Sorrentino, 'The Non- Punishment Provision with Regard to Victims of Trafficking. A Human Rights Approach' in R Piotrowicz, C Rijken and B Heide Uhl (eds), *Routledge Handbook of Human Trafficking* (Routledge International Handbooks 2017) 174.

Table 1. Regulation of human trafficking for sexual exploitation and related technologies – binding instruments

Regulation of human trafficking for sexual exploitation and related technologies - binding instruments

International level		Regional level	
United Nations	Organization of American States Inter-American Convention on International Traffic in Minors (adopted 18 March 1994, entered into force 15 August 1997) Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002), 2171 UNTS 227 Convention on the Elimination of All Forms of Discrimination against Women, (adopted 18 December 1979, entered into force 3 September 1979) 1249 UNTS 13 (CEDAW) art 6	**Council of Europe**	Convention on Action against Trafficking in Human Beings, CETS 197 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS 201 (Lanzarote Convention) Convention on Preventing and Combating Violence against Women and Domestic Violence, CETS 2010 (Istanbul Convention), art 25 Convention on Cybercrime, STE 185
		European Union	Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims and replacing Council Framework Decision 2002/629/JHA [2011] OJ L 101 Directive 2011/92/EU of the European Parliament and the Council of 13 December 2011. on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2012] OJ L 26
		Other regional instruments	African Charter on the Rights and Welfare of the Child (adopted 1 July 1990, entered into force 29 November 1999) art 27 Arab Charter on Human Rights (published in May 2004) art 10 Association of South East Asian Nations (ASEAN), Convention Against Trafficking in Persons, Especially Women and Children (Published 22 November 2015) Organization of American States Inter-American Convention on International Traffic in Minors (adopted 18 March 1994, entered into force 15 August 1997)

1.2 Soft law materials

In addition to legally binding instruments, a broad range of soft law instruments relating to trafficking and sexual exploitation have been adopted by international and regional organisations. The importance of these instruments should never be underestimated; in essence, they successfully provide insight into the substantive content of more general legal norms enshrined in treaties,[24] and provide a significant corrective function against the lack of data analysis standards, as Chapter IV will demonstrate.

Finally, it is worth reminding that, while it is true that those instruments do not directly impose obligations on states, the latter have at least the potential to help identifying or confirming a particular legal trend, contribute to the development of customary international law in relation to a particular aspect of trafficking and evolve into legally binding rules.[25]

The following table presents an overview of the ones that are relevant to the topic at stake. Adopted at the international and regional levels, these soft law instruments are addressing THB and sexual exploitation, and sometimes, directly or indirectly, the link between ICTs and sexual exploitation of women and children.

[24] OHCHR, 'Human Rights and Human Trafficking', Fact Sheet No 36 (United Nations 2014) 10.
[25] ibid.

Table 2. Regulation of human trafficking for sexual exploitation and related technologies – soft law instruments

Regulation of human trafficking for sexual exploitation and related technologies - soft law instruments

International level		Regional level	
United Nations		**Council of Europe**	General reports of the Group of Experts on Action against Trafficking in Human Being (GRETA)
Economic and social Council	UN Recommended Principles and Guidelines on Human Rights and Trafficking. Report of the United Nations High Commissioner for Human Rights to the Economic and Social Council (20 May 2002)	**European Union**	EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016
General Assembly	UNGA Res 64/293 (30 July 2010) 'United Nations Global Plan of Action to Combat Trafficking in Persons' UN Doc A/64/293		First report (2016) and second report (2018) from the Commission to the European Parliament and the Council on the progress made in the fight against trafficking in human beings (2016)) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims and replacing Council Framework Decision 2002/629/JHA [2011] OJ L 101
	UNGA 'Report of the Secretary General, Sale and sexual exploitation of children, including child prostitution, child pornography and other child sexual abuse material; and trafficking in persons, especially women and children', UN Doc A/72/164 (2017).		Recommendation of the Commission on measures to effectively tackle illegal content online (1 March 2018)
	UNGA Res 72/195 (19 December 2018) on improving the coordination of efforts against trafficking in persons UN Doc A/2/195		
	UNGA Res 72/195 (19 December 2018) on improving the coordination of efforts against trafficking in persons UN Doc A/2/195		
UNODC	Resolutions of the Commission on Crime Prevention and Criminal Justice (CCPCJ): eg 27.2, 27.3	**OSCE**	Plan of Action to fight Human Trafficking, Decision 557 (24 July 2003)
SDG	Sustainable Development Goals 5: Gender Equality, 8: Decent Work and Economic Growth, and 16: Peace, Justice and Strong Institutions	**League of Arab States**	Model Law on Combating Offences related to Information Technology Systems (2004)
ITU	International Telecommunication Union (ITU), Final Acts of the Plenipotentiary Conference, Dubai (2018)	**ASEAN**	Declaration Against Trafficking in Persons, Particularly Women and Children (29 November 2004)
		UNESCO	World Commission on the Ethics of Scientific Knowledge and Technology (COMEST)

1.3 Beyond the law. Enforcing anti-trafficking legislation

Despite their non-legislative nature, other anti-trafficking tools and initiatives have been adopted by different actors whose importance deserves to be highlighted. To illustrate, confronted with the difficulty of regulating dark web activities and hidden IP addresses, anti-trafficking efforts require, as Chapter III will emphasise, types of actions that cannot be achieved on a legislative level.

Such actions are foremost undertaken by the police, whose role in the fight against sexual exploitation is vital. Indeed, not only are police officials responsible for the identification of victims and the arrest of trafficking offenders as well as their detention, but they also are in charge of the dismantling of trafficking networks to prevent future victimisation.[26] They do, however, encounter several challenges throughout this process, related mainly to the identification of perpetrators and victims, but also due to their often-weak knowledge of legislative frameworks and to training gaps. In addition, they may be confronted with issues related to privacy (see Chapter IV), and even be involved in corruption and complicity. [27]

In order to join police forces against those challenges, Europol is, at the regional level, the main organisation working to implement anti-trafficking legislation. As the EU's law enforcement agency fighting against terrorism, cybercrime and other serious and organised forms of crime,[28] Europol made human trafficking one of its priority crime areas under the 2018-21 EU Policy Cycle.[29] The organisation regularly provides reports and guidelines relevant to the topic at stake,[30] and, as Chapter IV will mention, is part of Traffik Analysis Hub, a partnership between non-governmental organisations (NGOs) and financial institutions aiming at combating THB through the use of AI. It is also at the origin of the creation, on its webpage, of a crowd knowledge sourcing platform aiming at combating child sexual abuse.

At the international level, the mandate of providing technical and operational support to officials is the responsibility of Interpol, also widely mobilised on the issue of THB. By organising working group meetings once a year, the organisation aims to raise investigators' awareness of the latest THB developments. Widely engaged in the fight against sexual exploitation, especially online, it developed an international child sexual exploitation 'image database' successfully helping specialists to analyse and compare child sexual abuse images in order to identify victims.[31] Here again in order to fight child abuse and exploitation, both Europol and Interpol have also joined the global law enforcement partnership Virtual Global Taskforce (VGT) initiative which will be briefly addressed in Chapter IV when addressing the issue of data collection.

[26] A Farrell and B Kane, 'Criminal Justice System Responses to Human Trafficking' in J Winterdyk and J Jones, *The Palgrave International Handbook of Human Trafficking* (Palgrave Macmillan 2020) 5.
[27] ibid.
[28] Europol, 'About Europol' <www.Europol.europa.eu/about-Europol> accessed 8 May 2020.
[29] Europol, 'Trafficking in Human Beings' <www.Europol.europa.eu/crime-areas-and-trends/crime-areas/trafficking-in-human-beings> accessed 8 May 2020.
[30] In particular, see Europol, 'Publications and Documents' <www.Europol.europa.eu/publications-documents?t=human%20trafficking> accessed 2 June 2020.
[31] Interpol, 'International Child Sexual Exploitation database' <www.Interpol.int/How-we-work/Databases/International-Child-Sexual-Exploitation-database> accessed 8 May 2020.

In addition to receiving the support of those organisations and with a more specific focus on the use of ICTs, law enforcement officials are sometimes collaborating with third-party vendors and other third parties, such as 'data handling' technology experts who assist in obtaining and analysing data.[32] In the words of Bowman, the latter provide law enforcement officers with a package of 'predictive analytics, a catch-all phrase for a broad array of statistical analyses, machine learning, and myriad of other algorithmic techniques to enhance law enforcement agencies' predictive policing capacities'.[33] A more exhaustive description of these techniques and the issues they are raising will be provided in Chapter 4.

[32] J-L Mustol and D Boyd, 'The Trafficking-Technology Nexus' (2014) 21(3) Social Politics 461, 473.

[33] B. Pearsall, 'Predictive Policing: The Future of Law Enforcement?, Law Enforcement Explore Ways to Anticipate and Prevent Crime', 266 NJ Journal 16, 17.

2.

EXISTING REGULATION COVERING THE USE OF DIGITAL TOOLS

2.1 Big data and data analytics

Information can be said to be the basis of knowledge, and data, the basis of information.[34] The significant advances in digital technology have made data 'big', because of our enormous ability to collect, store and analyse information encompassing transactions, social media, enterprise content, sensors or even mobile devices.[35] Although there is no single accepted definition of the concept, 'big data' generally refers to 'data that exceeds the typical storage, processing, and computing capacity of conventional databases and data analysis techniques'.[36] Section 2 of this chapter will highlight the importance of the volume of data in modern life and how its analysis is also fuelling AI.

While it is beyond the scope of this thesis to linger too long on data-related concepts, the latter need to be briefly defined since they are going to be used both in this section and the one on AI. 'Data science' involves principles, processes and techniques for understanding phenomena via the analysis of big data, with the ultimate objective of improving decision-making, which is a paramount objective of business in general.[37] Data science also has, as Chapter IV will highlight, the potential to tackle social issues such as human trafficking.

Related concepts arise in the context of data-focused anti-trafficking efforts, such as 'data analytics' and 'data mining'. The first one refers to the method of analysing data with the aim to discover new patterns and relationships which might be invisible, and to provide new insights about the users who created it.[38] The second one designates the actual extraction of knowledge from

[34] F David, *ASEAN and Trafficking in Persons. Using Data as a Tool to Combat Trafficking in Persons* (IOM 2007) 4.

[35] K-C Desouza and K-L Smith, 'Big Data for Social Innovation' [2014] Stanford Social Innovation Review 39, 40.

[36] R Youssra, 'Big Data and Big Data Analytics. Concepts, Types and Technologies' (2018) 5(9) International Journal of Research and Engineering 524.

[37] F Provost and T Fawcett, 'Data Science and its Relationship to Big Data and Data-Driven Decision Making' (13 February 2013) 1(1) Big Data 53.

[38] H and P Gulia, 'Big Data Analytics' (February 2016) 4(2) Research Journal of Computer and Information Technology Sciences 1.

data via technologies that incorporate these principles.[39] Finally, according to the Organisation for Economic Co-operation and Development (OECD) definition, 'datasets' refer to any organised collection of data and is usually used interchangeably with the term 'database'.[40]

With these clarifications in mind, the main issues arising in the context of data analytics initiatives stem, as Chapter IV will emphasise, from privacy and data protection concerns. Although the two concepts are closely related, they are not identical. While the first right has been said to lack conceptual clarity,[41] data protection appears to be regulated with more precision, through the adoption of substantive rules governing data processing, but also on procedural rules on remedies for the data subject.[42] Notwithstanding, on a regional level and following the reasoning of the European Court of Human Rights (ECtHR), the Court of Justice of the European Union (CJEU) seems to encompass both concepts, providing a holistic protection of the fundamental rights of individuals.

All while recognising the importance of other instruments and the necessity, due to the global nature of THB, to pay attention to privacy and data protection concerns in all locations including those where those concepts are less developed, this section will focus on the main instruments adopted by the EU, all while recapitulating the legislation adopted by other instances.

The first one is undoubtedly the General Data Protection Regulation (GDPR),[43] which introduces very important concepts such as 'transparency', 'data minimisation', 'consent', 'data security' or 'rights of erasure', which can now be enforced through economic sanctions and instruments of monitoring and control by EU agencies.[44] It is worth noting, in this regard, that although the instrument emanates from the EU, the GDPR's territorial scope of application is very large due to the existence of two main criteria: article 3(1) refers to the 'establishment' criterion, which has been broadly interpreted by the European Court of Justice, and article 3(2) which refers to the newly introduced 'targeting' criterion. To summarise, those two criteria entail that the GDPR is applicable to data processing even when this processing takes place outside the EU, when the organisation's or subcontractor's activity targets EU residents.[45]

[39] Provost and Fawcett (n 37) 52.

[40] OECD, 'Glossary of Statistical Terms: Data Set' <https://stats.oecd.org/glossary/detail.asp?ID=542> accessed 5 June 2020.

[41] F Gerry, J Muraszkiewicz and N Vavoula, 'The Role of Technology in the Fight Against Human Trafficking. Reflections on Privacy and Data Protection Concerns' (2016) 32 Computer Law & Security Review 205, 207.

[42] ibid.

[43] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119.

[44] P Casanovas and others, 'Regulation of Big Data. Perspectives on strategy, policy, law and privacy' (2017) 7 Health Technol 335, 336.

[45] Freshfields Bruckhaus Deringer, 'The extra-territorial scope of the EU's GDPR' <www.freshfields.com/en-gb/our-thinking/campaigns/digital/data/general-data-protection-regulation/> accessed 15 June 2020.

The second one is the Victims Directive, in particular article 21, which grants victims the right to protection of privacy by asking member states to ensure that they:

> take during the criminal proceedings appropriate measures to protect the privacy, including personal characteristics of the victim taken into account in the individual assessment provided for under Article 22, and images of victims and of their family members, and (…) take all lawful measures to prevent public dissemination of any information that could lead to the identification of a child victim.[46]

In addition to these regional instruments, most countries apply their current rules in the area of privacy and data protection, as developed in their respective jurisdictions to big data processes.[47] Others are summarised in the following table.

It is worth acknowledging that the above-mentioned legislative framework presents the shortcomings of being limited to criminal proceedings and of not addressing specific fundamental rights challenges related to the use of technology in combating human trafficking.[48] However, these legal loopholes are partially compensated by the existence of soft law instruments promoting ethical research and data collection. Their importance having already been underlined in Chapter I (section 2), the second table will recapitulate the main instruments linking data collection, privacy issues and human trafficking.

[46] Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime [2012] OJ L 315/57 art 21.

[47] B Van der Slote and S Van Schendel, 'International and Comparative Legal Study on Big Data' (The Netherlands Scientific Council for Government Policy Working Paper 2016) 34.

[48] Gerry, Muraszkiewicz and Vavoula (n 41) 210.

Table 3. Regulation of data analytics and big data – privacy and data concerns – binding instruments

Regulation of data analytics and big data - privacy and data protection concerns - binding instruments

International level		Regional level	
United Nations	International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) arts 2, 17 and 19 Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (adopted 15 November 2000, entered in to force 25 December 2003) 2237 UNTS 319 (Palermo Protocol) art 6.1	Council of Europe	Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) arts 9 and 10 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as it will be amended by its Protocol CETS No 223 (not in force), STE 108
		European Union	Charter of Fundamental Rights of the European Union arts 7 and 8 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119 Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime (Victim Directive) [2012] OJ L 315/57 art 21 Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims and replacing Council Framework Decision 2002/629/JHA [2011] OJ L 101 art 19 and 20 Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L 350 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281

Table 4. Regulation of data analytics and big data – privacy and data concerns – soft law instruments

2.2 Artificial intelligence

According to the independent high-level expert group on AI set up by the European Commission, AI refers to:

> systems that display intelligent behavior by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals. AI-based systems can be purely software-based, acting in the virtual world (e.g. voice assistants, image analysis software, search engines, speech and face recognition systems) or AI can be embedded in hardware devices (e.g. advanced robots, autonomous cars, drones or Internet of Things applications).[49]

AI is facilitated by 'algorithmics systems' which operate through the detection and reinforcement of patterns in large datasets all while offering 'the potential to rationalize services and deliver enormous efficiency gains in task and systems performance'.[50] Reference is also often made to 'machine learning', which designates a 'category of narrow AI techniques used to train algorithms to operate datasets to recognize and help solve problems'.[51] As mentioned previously, the use of algorithmic systems provides a way to analyse huge volumes of data way more rapidly than what human decision-making previously used to allow.

Bearing in mind those conceptual clarifications, it is necessary to acknowledge the potential interference of individual self-determination, or what can be qualified as 'individual autonomy and agency', with the opacity of AI.[52] While humans are always sovereign in the process of creating and using AI technologies, particularly when deciding the application and use of AI outputs and the degree of human decision-making's complementation or replacement, several rights and freedoms may be harmed with the use of algorithmics systems.[53] This is the case of the rights of privacy, data protection, freedom of expression, meaningful access to remedy and equality and non-discrimination, to name a few.[54] However, because AI systems are formed on the basis of datasets, and, particularly in the case of sexual exploitation, on those that contain personal data, the following sections will focus on the regulation of AI with a focus on the right to privacy and on data protection, which are most likely to be at threat in an anti-trafficking context.

Regarding AI, the most relevant instruments have been adopted at the regional level. Indeed, while the use of machine learning raises freedom of expression

[49] Independent high-level expert group on AI set up by the European Commission, A Definition of AI. Main Capabilities and Disciplines, Definition Developed for the Purpose of the AI HLEG's deliverables (European Commission 2019) 1.

[50] Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, 'Draft Recommendation of the Committee of Ministers to member states on human rights impacts of algorithmics systems' (12 November 2018) 2.

[51] ibid 4.

[52] M Taddeo and L Floridi, 'How AI can be a force for good' (2018) 361(6404) Science 751.

[53] Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, 'Draft Recommendation' (n 50) 4.

[54] Toronto Declaration, Protecting the rights to equality and non-discrimination in machine learning systems (May 2018) art 6 (Toronto Declaration) <www.torontodeclaration.org/> accessed 5 June 2020.

and opinion concerns,[55] no treaty has been adopted to regulate the use of AI specifically and directly at the international level. Initiatives have been undertaken mainly through working groups and panels, and discussions have focused on the Convention on Certain Conventional Weapons adopted in 1980,[56] because of the increasing high-level concern from the UN regarding killer robots.[57] Other discussions have been targeting the UN Guiding Principles for Business and Human Rights,[58] to address the potentially negative impact of AI use on human rights in a corporation setting. It is therefore at the level of the CoE, the EU and the OECD that the most important legal instruments have been adopted, mostly under the form of soft law.

The CoE is responsible for the adoption of Protocol CETS No 223[59] amending the 1981 Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data,[60] which will be in force if all the parties ratify it, or on 11 October 2023 if it obtains 38 ratifications. This amendment introduces, in article 9(1)(a), the right not to be subject to a decision affecting significantly an individual taken solely on the basis of automatic processing of data without his/her point of view being taken into account. More recently, under a softer legal form, the CoE also adopted the European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems and Their Environment in 2018,[61] focusing on five main principles regarding the use of AI in a judicial context.[62]

As for the EU, the regional organisation has adopted a more protective regulatory framework through the ratification of the GDPR. Indeed, in its article 22(1), Regulation 2016/679 introduces the very important right to have a decision based solely on automated processing (algorithm) be made or reviewed by a natural person instead of a computer.[63] As for Protocol CETS No 223, it includes exceptions to these rights if the proper safeguards are provided. The EU has also adopted several soft law instruments, such as the Ethics Guidelines for Trustworthy AI, adopted by the High-Level Expert Group on Artificial Intelligence set up by

[55] Rights which are enshrined, at the UN level, in arts 2(1) and 19(1) of the International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR).

[56] Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Discriminated Effects (adopted 10 October 1980, entered into force 2 December 1983), 1342 UNTS, 137.

[57] Campaign to Stop Killer Robots, 'High-level concerns on killer robots at UN', 30 October 2019, <www.stopkillerrobots.org/2019/10/unga74/?lang=es> accessed 5 June 2020.

[58] Guiding Principles for Business and Human Rights, Implementing the United Nations 'Protect, Respect and Remedy' Framework (2011).

[59] Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 223,

[60] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as it will be amended by its Protocol CETS No 223 (not in force), STE 108.

[61] European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (adopted at the 31st plenary meeting of the CEPEJ, Strasbourg, 3-4 December 2018).

[62] For more information, see Council of Europe, 'CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment' <www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> accessed 5 June 2020.

[63] The Library of Congress, 'Regulation of Artificial Intelligence: Europe and Central Asia' <www.loc.gov/law/help/artificial-intelligence/europe-asia.php> accessed 24 April 2020.

the Commission[64] which enshrines four ethical principles, seven key requirements and an assessment list to ensure the adequate use of AI, or the Declaration of Cooperation on Artificial Intelligence, signed by 25 European countries on 10 April 2018.[65]

Other soft law instruments have been adopted by regional organisations. This is the case of the OECD Principles on Artificial Intelligence,[66] which provide five complementary values-based principles for the responsible stewardship of trustworthy AI, namely inclusive growth, sustainable development and well-being, human-centred values and fairness, transparency, explainability robustness, security and safety as well as accountability.[67] The instrument also includes five recommendations to policymakers, namely to invest in AI research and development, to foster a digital ecosystem for AI, to shape an enabling policy environment for AI, to build human capacity and prepare for labour market transformation, and to develop international cooperation for trustworthy AI.

Adopted in 2018, the Toronto Declaration[68] also constitutes a relevant instrument, asking governments and companies to urgently protect human rights in the age of machine learning, AI and advanced computing, with a focus on the right to equality and non-discrimination.[69] Although it is 'only' a statement made by Amnesty International and the digital rights groups Access Now, it has already been widely accepted by the human rights community.

Finally, some initiatives that are not of legal nature per se are worth mentioning. This is the case of the European AI Alliance, which aims to interact on AI issues with experts of the High-Level Expert Group on Artificial Intelligence set up by the European Commission, but also the Coordinated Plan on AI,[70] established following the adoption of the European Strategy[71] in 2018. More recently, the EU also adopted a White Paper on Artificial Intelligence in order to promote the uptake and address the risks associated with certain uses of AI.[72]

Other initiatives that do not have a legal value but are closely related to the regulation of AI are summarised for the most part in the following table.

[64] High-Level Expert Group on Artificial Intelligence set up by the European Commission, 'Ethics Guidelines for Trustworthy AI' (Brussels, 8 April 2019).

[65] Declaration on Artificial Intelligence (10 April 2018).

[66] OECD Principles on Artificial Intelligence, Recommendation of the Council on Artificial Intelligence (22 May 2019).

[67] OECD Recommendation of the Council on Artificial Intelligence OECD/LEGAL/0449 (adopted 22 May 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 29 April 2020.

[68] Toronto Declaration (n 54).

[69] ibid.

[70] European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Coordinated Plan on Artificial Intelligence' (7 December 2018) COM(2018) 795 final <https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence> accessed 2 July 2020.

[71] European Commission, Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, *Artificial Intelligence for Europe* {swd(2018) 137 final}.

[72] European Commission, 'White Paper on Artificial Intelligence. A European Approach to Excellence and Trust' (19 February 2020) COM (2020) 65 final.

Table 5. Regulation of artificial intelligence – privacy and data concerns – binding and soft law instruments

Regulation of artificial intelligence - privacy and data protection concerns - binding and soft law instruments

	International level	Regional level
Binding instruments	International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR) arts 2 and 19 Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Discriminated Effects (adopted 10 October 1980, entered into force 2 December 1983), 1342 UNTS 137	**Binding instruments** Council of Europe: Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) arts 7 and 10 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as it will be amended by its Protocol CETS No 223 (not in force), STE 108 European Union: Charter of Fundamental Rights of the European Union arts 7 and 8
Soft law instruments	UNGA 'Report of the United Nations High Commissioner for Human Rights on the promotion, protection, and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective', UN Doc HCR/35/9 (2017) UNGA Res 71/199 (19 December 2017) on the right to privacy in the digital age, UN Doc A/71/199 UNGA 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' UN Doc A/73/348 (2018) UNGA 'Report on privacy and technology from a gender perspective', UN Doc A/HRC/40/63 (2019) Committee on the Right of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment (2 March 2021)	European Union: European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (adopted at the 31st plenary meeting of the CEPEJ, Strasbourg, 3-4 December 2018) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119 **Soft law instruments** Council of Europe: Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, Draft Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes (16 November 2018) Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, 'Draft Recommendation of the Committee of Ministers to member states on human rights impacts of algorithmics systems' (12 November 2018) Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, 'Study of the implications of advanced digital technologies (including AI) for the concept of responsibility within a human rights framework' (9 November 2018) European Union: Independant High Level Expert Group on AI set up by the European Commission, Ethics guidelines for thrustworthy AI (8 April 2019) European Parliament's Resolution on Civil Law Rules on Robotics (16 February 2017) EU Declaration of Cooperation on Artificial Intelligence, Digital Day (10 April 2018)
Other	IBM, 'Principles for Trust and Transparency', (adopted 30 May 2018) ITU focus groups on AI and machine learning UNICRI Centre for Artificial Intelligence and Robotics	Other: OECD Principles on Artificial Intelligence, Recommendation of the Council on Artificial Intelligence (22 May 2019) Toronto Declaration, Protecting the right to equality and non-discrimination in machine learning systems (May 2018) EU Data Protection Code of Conduct for Cloud Infrastructure Service Providers in Europe (27 January 2017) (CISPE) Asia-Pacific Cooperation Cross-Border Privacy Framework, 2015 (APEC)

Keeping the above-mentioned legislative framework in mind, the following chapter will analyse the link between digital technologies and the crime of sexual exploitation of women and children, through the internet on the one hand (1) and through mobile technology on the other (2).

3.

THE ICTS AND SEXUAL EXPLOITATION NEXUS. TECHNOLOGIES (MIS)USED BY TRAFFICKERS

Both practical and normative reasons justify the need to research the role of the technologies used by perpetrators in cybersex trafficking. In addition to addressing the need to adopt adequate prevention measures and responses to the digital threats, research may also shed light on the social cost of bringing this crime to more public and mainstream space through these technologies.[73] Indeed, if it makes little doubt that the impact of THB on individuals and society is very destructive, from the physical abuse and torture of victims to the psychological and emotional trauma, on the one hand, and to the economic and political implications of unabated crime on the other,[74] digital tools, although they may help as a disruptive force against these consequences, may also have a (high) cost.

ICTs have enabled people to connect and transfer their activity, whether criminal or not, from a private space into a public one. As Interpol highlights, 'technology is allowing offenders to develop networks with like-minded people that are more complex and on a larger scale than ever before. As a network, as opposed to an isolated individual, they are more innovative, collectively intelligent, pervasive and robust'.[75] On the other hand, digital tools are also responsible for hiding activities that were previously recognised and identified.[76] It is therefore crucial, in order to restore the visibility of those large scale and connected activities and networks, that the whole set of anti-trafficking actors has a proficient knowledge of these tools.

Besides the issue of their (in)visibility, it is worth acknowledging that ICTs tend to be used in ways that 'replicate or perpetuate gender stereotypes and biases and can have unintended negative impacts'. To a broader extent, they may even constitute a nexus of victimisation for women and children.[77] This phenomenon can be illustrated by the issue of 'virtual' trafficking, which is raised when a video

[73] M Leary, 'Fighting Fire with Fire. Technology in Child Sex Trafficking' (2014) 21 Duke Journal of Gender Law and Policy 289, 294.

[74] UNODC and UN.GIFT (UN Global Initiative to Fight Human Trafficking), 'An Introduction to Human Trafficking. Vulnerability, Impact and Action' (Background paper 2008) 14.

[75] WePROTECT Global Alliance, 'Working together to end the sexual exploitation of children online' (UN.GIFT Global Threat Assessment 2018) 9.

[76] Leary (n 73) 291.

[77] S Milivojevic and M Segrave, 'Tracing the emergence of ICT-enabled human trafficking for ransom' [2017] Gender, Technology and Violence (Routledge Studies in Crime and Society) 28.

or a picture itself is trafficked and sold worldwide. In this context, questions arise as to when pornography ends and when trafficking in images of sexual exploitation begins.

For C Dettmeijer-Vermeulen, the circulation of images of sexual acts with victims on the internet has created particularly intricate challenges and is adding a new dimension to victimhood.[78] D-M Hughes, who has been studying the link between ICTs and THB for more than 20 years, goes even further by emphasising the tendency that human beings have to pretend that what is real is in fact virtual. According to her, digital technologies have provided a new way of denying real harm and have established a forum to reject women's experience or to state that the latter are imagined.[79]

This consideration has to be kept in mind while reading this chapter, which will draw up an inventory of the main technologies used by perpetrators in their attempt to advertise sex services, recruit into trafficking and exercise control over the victims, namely the internet through the surface and dark web (1), as well as mobile technology tools (2).

3.1 Through the internet

Since human beings entered the information age in the 1990s, our relationship to communication has been radically transformed. While the internet is undoubtedly the most broadly used technology today, it is worth reminding that its democratisation brought major changes in our lives, specifically by changing the ways in which information is flowing and by making us constantly connected with others. As Verham summarises, '[n]either the Internet or sex trafficking would look like it does today without its counterpart'.[80] Indeed, since the beginning of this era, perpetrators of sexual exploitation have mobilised characteristics such as the relative anonymity and the modest cost that the web is offering to commit the crime. Therefore, many new challenges emerge in the context of this relationship, such as the difficulty to prosecute traffickers and to establish the burden of proof for criminal offences,[81] and even sometimes, if activities are done on the darknet, the impossibility to do so.

There is currently little information about how digital tools are used to sexually exploit adult women. Much more is known about the ones used to share and disseminate child pornography and other types of child abuse, including sexual exploitation.[82] However, the gender dimension appears again to be an important

[78] C Dettmeijer-Vermeulen, 'Trafficking in Human Beings. Ten Years of Independent Monitoring by the Dutch Rapporteur on Trafficking in Human Beings' (2012) 18 European Journal on Criminal Policy and Research 283, 301.

[79] D-M Hughes, 'The Impact of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation', Misuse of the Internet for the Recruitment of Victims of Trafficking in Human Beings, Council of Europe Campaign to combat trafficking in human beings (Seminar proceedings**,** Strasbourg, 7-8 June 2007) 54.

[80] Z Verham, 'The Invisibility of Digital Sex Trafficking in Public Media' (2015), 8 Intersect 3, 4.

[81] Myria, 'Tightening the Links. 2015 Annual Report of Trafficking and Smuggling of Human Beings' (Myria 2016) 69-71.

[82] K Maltzahn*,* 'Digital Dangers. Information and Communication Technologies and Trafficking in Women' (APC Issue Papers 2006) 5.

component in the equation. The Counter-Trafficking Data Collaborative (CTDC), a data analysis initiative which will be analysed in Chapter IV, has in this regard highlighted the omnipresence of psychological, physical and sexual abuse as means of control in trafficking in human beings. Those can give hints about the prevalence of abusive means mobilised to recruit women into sexual exploitation.

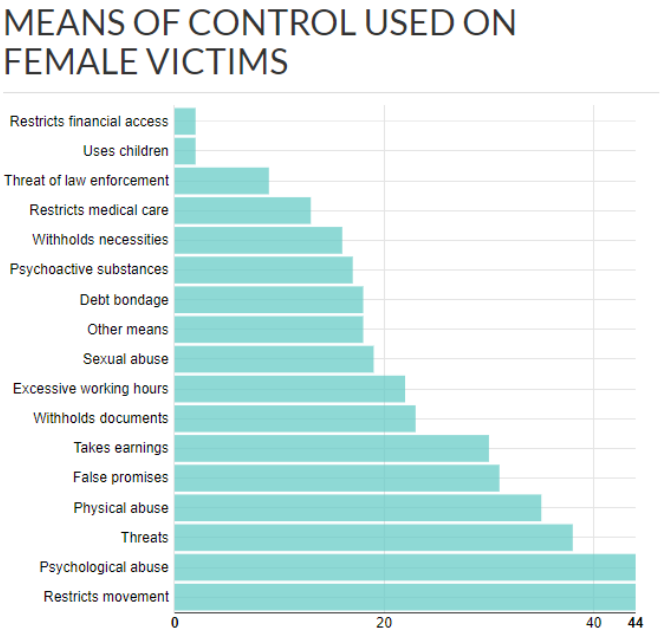


Figure 3. Means of control used on victims
Source: CTDC, 'Human Trafficking and Gender: Differences, Similarities and Trends' <www.ctdatacollaborative.org/story/human-trafficking-and-gender-differences-similarities-and-trends> accessed 29 July 2020

While they remain rare, reports and contemporary literature have been aiming to identify the most important digital tools used to recruit women through the internet. The following section will focus on these, all while including considerations about the abuse and trafficking of children. In any case, the emphasis will be on recruiting tools, but also on the ones used to advertise and keep control on victims, whether they emanate from the surface web (3.1.1) or the dark web (3.1.2).

3.1.1 Using the surface web

The surface web, which is the portion of internet visible by all users, serves as a platform advertising and selling services, identifying and recruiting victims, exercising control over them, and communicating with other trafficking actors. As the next chapter will highlight, it is also through this visible part of the 'net-iceberg' that anti-trafficking agents can trace and analyse perpetrators' 'digital footprint', which designates the information about trafficking actions that can be found on the internet as a result of their online activity.[83]

Offering undeniable qualities, social networking and messaging sites are, to this day, undoubtedly used by almost everyone. Facebook, Instagram, Snapchat, Tumblr, Viber, Skype and Facetime, among others, are networks which target

[83] Lexico, 'digital footprint' <www.lexico.com/definition/digital_footprint> accessed 4 April 2020.

audience, connect people and develop relationships, all for free. However, their unlimited potential is also exploited by human traffickers. Indeed, the latter use social media at the recruitment stage but also once their victims are identified and part of their network, to put pressure on them, often through deceptive or coercive messages. Taking advantage of the possibility to post messages and exchange information in relative anonymity,[84] they use these types of communication both for practical and cultural reasons, mainly to outline where to find victims, and this undoubtedly reinforces and normalises negative gender attitudes due to the large proportion of women and girls who are looked for.[85]

At the recruitment stage, one of the perpetrator's main strategies is to secure trust and cooperation of vulnerable individuals, particularly young girls,[86] by answering, for instance through fake Facebook accounts, posts that include expressions of fear, emptiness and disappointment. In this regard, the law enforcement literature has been widely using the concept of 'online grooming' to refer to 'the process of establishing/building a relationship either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person'.[87]

Social media can also be used by traffickers to blackmail victims, by taking a compromising screenshot during a video conversation or voluntarily supplied photographs.[88] In addition, perpetrators also broadly use online dating sites and applications such as Elmaz, Twoo, Gepime,[89] Tinder, Grindr or Okcupid, particularly for international trafficking.[90] Regardless of whether social networks or dating sites are used, human traffickers generally communicate with victims through private chats, and then through applications such as Skype or Viber, or directly through mobile phones.[91] The fact that most social network messaging services are moving towards 'end-to-end encryption' as the default setting raises further issues which will be discussed in the last chapter.

In recent years, the so-called phenomenon of 'loverboys' has become, at least throughout Europe, the most common *modus operandi* for the recruitment of women and children through the social networking channel. Through this tactic, pimps, usually young men, attempt to seduce young women, often minors, to force them into prostitution or other illegal activities by establishing a romantic (abusive) relationship with their victims. Starting with the sharing of presupposed

[84] Myria, 'Trafficking and Smuggling of Human Beings Online, 2017 Annual Report' (Myria 2018) 27.

[85] Hughes, 'The Impact of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation' (n 79) 11.

[86] University of Toledo, 'Study Details Link Between Social Media and Sex Trafficking' (phys.org, 8 October 2018) <https://phys.org/news/2018-10-link-social-media-sex-trafficking.html> accessed 5 April 2020.

[87] See for eg International Centre for Missing & Exploited Children (ICMEC), 'Online Grooming of Children for Sexual Purposes. Model Legislation and Global Review' (1st edn, ICMEC 2017) <www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-ofChildren_FINAL_9-18-17.pdf> accessed 6 May 2020.

[88] Myria, 'Trafficking and Smuggling of Human Beings Online, 2017 Annual Report' (n 84) 27.

[89] Surf and Sound, *Improving and sharing knowledge on the Internet role in the processes of human trafficking and smuggling*, (UK National Report 2017) 23.

[90] Myria, 'Trafficking and Smuggling of Human Beings Online, 2017 Annual Report' (n 84) 29.

[91] Surf and Sound (n 89) 24.

common hobbies, victims end up in a state of 'complete emotional, psychological and financial dependency' and are 'ready to do anything to keep the loverboy's affection'.[92] Again, it is worth noting that the use of digital tools does not stop at the stage of recruiting: social networks are particularly effective to keep control on the victims, for instance through blackmailing with the threat of online exposure.[93]

Internet chat websites such as Chatroulette, particularly popular among teens, especially girls,[94] are also often used to 'befriend potential victims to fall into the traffickers' net'.[95] Other online forums such as applications and computer games are also frequently used to 'groom' young children via chat functions in multiplayer video games.[96] To that also has to be added the cultural impact of inherently violent video games freely accessible to minors that tends to banalise, *inter alia*: assaults on women, murder, rape, slavery, torture, forced prostitution, child abuse and other violations of human rights.[97]

If not recruited through social networks, victims are mainly identified and contacted by traffickers through advertisements. This can be done through spurious ads for employment, travel or dating and marriage agencies.[98] Victims are most of the time replying to a job offer, including vacancies for dancers, waitresses, hostesses, housekeepers, cleaning ladies, childminders or household help, and are subsequently forced into prostitution.[99]

According to D-M Hughes, these types of advertisements rely heavily on the inequality between men and women all while targeting particularly vulnerable populations.[100] As a recent illustration, a fake modelling agency was used to recruit young girls, including minors, who were reacting to advertisements offering work in their countries of origin, ultimately forcing them into prostitution in Belgium.[101] The agency recruiting in the country of origin turned out to be part of an important international prostitution network exploiting its victims in Western

[92] Payoke, 'Loverboys' <www.payoke.be/fr/loverboys/> accessed 8 May 2020.

[93] D Boyd and others, 'Human Trafficking and Technology. A Framework for Understanding the Role of Technology in the Commercial Sexual Exploitation of Children in the U.S.' (Microsoft Research Connection 2011) 4.

[94] D-M Hughes, 'The Impact of the Use of New Communications and Information Technologies on Trafficking in Human Beings for Sexual Exploitation', Report for the Committee for the Equality between Women and Men (Council of Europe 2001) 20.

[95] Hughes, 'The Impact of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation' (n 79) 7.

[96] Thorn, 'Meet the new anti-grooming tool from Microsoft, Thorn, and our partners' (*Thorn*, 11 February 2020) <www.thorn.org/blog/what-is-project-artemis-thorn-microsoft-grooming/> accessed 22 April 2020.

[97] Amnesty International Espana, 'Discriminación y violencia contra las mujeres en los videojuegos más populares de estas navidades' (*Amnistía Internacional*, 29 December 2014) <www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/discriminacion-y-violencia-contra-las-mujeres-en-los-videojuegos-mas-populares-de-estas-navidades/> accessed 7 May 2020.

[98] Europol, 'Trafficking in Human Beings and the Internet' Intelligence Notification 15/2014 (4 November 2014) <www.Europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet> accessed 7 May 2020.

[99] Myria, 'Trafficking and Smuggling of Human Beings Online, 2017 Annual Report' (n 84) 27.

[100] D-M Hughes, 'Role of Marriage Agencies in Trafficking in Women and Trafficking in Images of Sexual Exploitation', The Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation (EG-S-NT) (Committee for Equality between Women and Men (CDEG), Council of Europe 2001) 3.

[101] Myria, 'Combating social fraud to prevent trafficking in human beings, 2010 Annual Report on Human Trafficking and Smuggling' (Myria 2011) 128.

European countries.[102] Recruiting with advertisements can also often take place through what is commonly referred as the 'bribe trade', namely the involvement of marriage agencies in trafficking for sexual exploitation. Here again, the gender dimension appears striking, and raises the issue of demand for trafficked women from abroad in countries such as China and India, where the phenomenon of 'missing women'[103] is commonplace.[104]

Recruiting through advertisements can also directly take place through sex services offers. As way of illustration, Craigslist's adult section and Backpage, which were, until recently, the main websites advertising for sex services in the United States, were closed due to the finding of sexually exploited women and children. Although this may be perceived a major achievement in the combat against THB, the blurred distinction between advertisements of trafficking victims and of sex workers not falling within the legal definitions of trafficking[105] continues to raise many issues, including from a gender perspective. Knowing the important decrease in street prostitution in the recent years due to web-based prostitution pages,[106] it has been contended that the seizure of those websites has caused the loss of jobs or the pushing of independent sex workers to the streets, the latter becoming constrained to work again for pimps.[107] On the other hand, an important number of alternatives to those websites are already flourishing since demand is not disappearing.

Alongside advertisement pages, other adult entertainment websites such as webcam sex services are mobilised by perpetrators. Those pages provide buyers sex acts performances in live-streamed sessions in exchange for their payment. Again, although those kinds of websites have been said to offer greater autonomy and opportunity on the part of consensual sex workers to work from a distance in relative safety, the fact remains that the webcam sex tourism industry is filled with victims of sexual exploitation, and particularly of underage victims.[108] The best-known example is the Philippine-based sex trafficking network allegedly forcing children to perform sexual acts in front of webcams and offering the possibility

[102] Myria, 'Trafficking and Smuggling of Human Beings Online, 2017 Annual Report' (n 84) 27.

[103] According to economist Amartya Sen, this concept designates the women who are 'demographically' missing across the developing world, because they died prematurely due to gender discrimination (eg from forced abortions to femicides); see Amartya Sen, 'More Than 100 Million Women Are Missing' (20 December 1990) 37(20) New York Review of Books <https://web.archive.org/web/20130504072819/http://ucatlas.ucsc.edu/gender/Sen100M.html> accessed 25 July 2020.

[104] H Barr, 'Bride Trafficking to China Spreads Across Asia' (*Human Rights Watch*, 3 November 2019) <www.hrw.org/news/2019/11/03/bride-trafficking-china-spreads-across-asia> accessed 25 July 2020.

[105] M Latonero, 'The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking', Research Series on Technology and Human Trafficking (Center on Communication Leadership and Policy, University of Southern California 2012) 18.

[106] European Parliament, Directorate General for Internal Policies, Policy Department C, Citizens' Rights and Constitutional Affairs, 'Sexual Exploitation and Prostitution and its Impact on Gender Equality' (2014) 53.

[107] M Castillo, 'Sex workers may be hurt by Backpage ad crackdown' (*The Lily,* 10 April 2018) <www.thelily.com/sex-workers-may-be-hurt-by-backpage-ad-crackdown/> accessed 5 May 2020.

[108] C Allen, 'The Role of the Internet on Sex Trafficking' (*International Observatory Human Rights*, 7 March 2019) <https://observatoryihr.org/blog/the-role-of-the-internet-on-sex-trafficking/> accessed 4 April 2020.

to consumers to provide directions.[109] Finally, it is worth noting that pornographic spams, and in particular unsolicited commercial e-mail, make up about half of all e-mail sent worldwide.[110] Most of them are deceptive and cost businesses billions of dollars each year.[111] Although they are not systematically linked to human trafficking, knowing their ubiquitous presence and unsolicited nature, they deserve to be acknowledged.

With all this in mind, it seems impossible to avoid addressing the inescapable link between pornography and human trafficking. In addition to often normalising aggression, violence and therefore exploitation, pornography may be used to 'groom' and blackmail sex-trafficking victims.[112] Indeed, coerced participation to the pornographic industry, including of underage victims being advertised as adults,[113] is far from rare. In addition, as already highlighted in the beginning of this chapter when addressing the issue of trafficking in images of sexual exploitation, acts of prostitution are frequently filmed without the consent of the victim and later distributed.[114] Overall, it has been repeatedly contended that the above-mentioned industry increases demand for THB due to the fact that users can become increasingly absorbed in acting out what they view on the screen.[115]

When not operating through social media, advertisement pages and the porn industry, cybersex traffickers mobilise other channels, such as online discussion forums involving participants that are favourably disposed towards sexually graphic communications.[116] Flourishing on the internet, these forums may simply be filled by exchanges made between clients of prostitution. However, as they tend to reinforce and normalise negative attitudes towards women,[117] they sometimes contain clues of trafficking.[118] Additionally, such forums may be a space in which child pornography or videos of brutal sexual assault is shared.[119]

Finally, perpetrators do not hesitate to use peer-to-peer networks such as Gnutella, eDonkey or eMule, to share child pornography and images of sexually exploited women and children.[120] Through these networks, digital documents and computer files are 'distributed and shared directly between Internet-connected devices using a specialized software program that searches for other connected computers on a network and locates the desired

[109] N Frei, 'On "Cyber Trafficking" and the Protection of its Victims' (*Völkerrechtsblog*, 26 July 2017) <https://voelkerrechtsblog.org/on-cyber-trafficking-and-the-protection-of-its-victims/, accessed 19 June 2020.

[110] M Chawki and M Wahab, 'Technology Is a Double-Edged Sword. Illegal Human Trafficking in the Information Age' [2004] Droit-TIC 22.

[111] A Schwartz, *Stopping Spam* (O'Reilly 1998) 17.

[112] Office for Democratic Institutions and Human Rights and Organization for Security and Co-operation in Europe, 'Cross Linkages of Human Trafficking and Pornography. Myth or Reality' Conference (4 May 2020).

[113] Europol, 'Criminal Networks Involved in the Trafficking and Exploitation of Underage Victims in the EU' (European Union Agency for Law Enforcement Cooperation 2018) 7 <www.Europol.europa.eu/publications-documents/criminal-networks-involved-in-trafficking-and-exploitation-of-underage-victims-in-eu/> accessed 11 May 2020.

[114] Hughes, 'The Impact of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation' (n 79) 76.

[115] Dressember, 'The Link Between Pornography and Human Trafficking' (*Dressember*, 3 April 2018) <www.dressember.org/blog/thepornographylink> accessed 10 June 2020.

[116] J Savirimuthu, *Online Child Safety. Law, Technology and Governance* (Palgrave Macmillan 2012) 43.

[117] Maltzahn (n 82) 6.

[118] Myria, 'Le rôle des réseaux sociaux et d'internet dans la traite des êtres humains. Apercu du phénomène' (Myria 2017) <www.myria.be/files/RATEH-2017-fiches-r%C3%A9sum%C3%A9s_(1).pdf> accessed 6 May 2020.

[119] UNODC, 'Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children' (UN Publications 2015) 19.

[120] ECPAT International, 'Emerging Global Threats Related to the Online Sexual Exploitation of Children' Briefing paper (2018) 2.

resource'.[121] Mislabelling violent child sexual abuse material, including sexual exploitation, users often attempt to trick children into opening, downloading and viewing those files.[122]

In any case, knowing the risks that the use of the whole panel of those online forums implies, it has become crucial to create wider information campaigns in order to address the responsible use of technology among parents and teachers when it comes to child exploitation, but also, more generally, among internet service providers (ISPs)[123] in cybersex trafficking cases. ISPs, along with other stakeholders, carry a responsibility for often facilitating the trafficking process through the internet. This is the case, inter alia, of financial institutions who are receiving payments by credit cards for sex-trafficking services, but also of the media and press who host deceptive advertisements.[124]

Bearing in mind those 'visible' means, the next section will address the less detectable tools that the dark web is offering to perpetrators of sexual exploitation.

3.1.2 Using the dark web

As part of the deep web, namely the non-searchable parts of the web, the dark web is formed by communication protocols, such as the network Tor, designed to exchange information sent through a vast number of relays around the world.[125] The fact that those protocols prevent the tracing of an activity back to its origin makes the policing of this space particularly challenging.

Figure 4. Visible Web, Deep Web, Dark Net. Source: F Ruiz, 'Trends in the Area of Child Sexual Exploitation', (European Cybercrime Centre, Europol 2016.

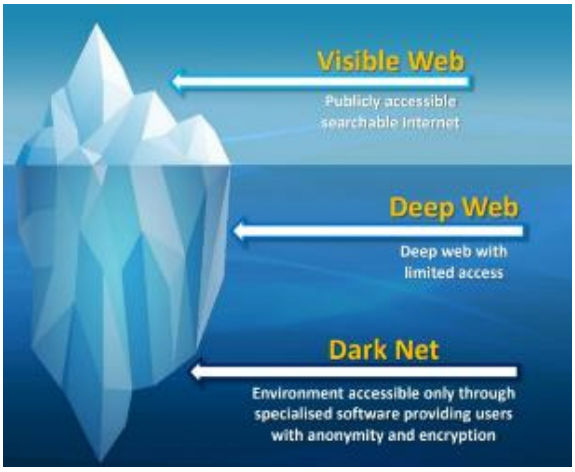


Figure 5. Tor. Source : Tor, <www.torproject.org/> accessed 13 April 2021

[121] UNODC, 'Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children' (n 119) 60.

[122] ibid 17.

[123] Plan International, 'Children sex trade at the digital age. A Study on the Commercial Sexual Exploitation of Children in Metro Manila' (The Girls Advocacy Alliance 2017) 6.

[124] A-P Sykiotou, 'Cyber Trafficking. Recruiting Victims of Human Trafficking through the Net' in C-D Spinellis, N Theodorakis, B. Emmanouil, and G. Papadimitrakopoulos, *Essays in Honour of Nestor Courakis* (Ant N Sakkoulas Publications LP 2017) 1547-87. 1566.

[125] Stop the Traffik, 'Human Trafficking and the Darknet. Insights on Supply and Demand' (Centre for Intelligence Led Prevention 2018) 1.

Figure 6. Surface Web, Deep Web, Dark Web. Source: C Sheils, 'Enter the Deep and Dark Web If You Dare (And Get Ready for a Surprise). Inside the Onion. Here's What You Need to Know About the Deep Web', <https://digital.com/online-privacy/deep-dark-web/>, accessed 5 March 2020.

	THE SURFACE WEB	THE DEEP WEB	THE DARK WEB
How to Access	Traditional search engine	Requires password, encryption, or specialty software	Requires Tor Project or similar to view
Includes	All indexed web pages	All unindexed webpages	Subset of unindexed webpages inside the deep web
Size	Approximately 4.47 billion pages	Massive, likely 4-5x larger than the Surface web	A subset of the Deep Web, but unmeasurable in size
Uses	Email, social media, video, legitimate business websites, etc.	Usually used for legit purposes that require anonymity	Sometimes used for illegal activities
Who uses it?	Anyone with an internet connection	Whistleblowers, journalists, etc.	Hackers, sellers & buyers of illegal merchandise
Can be browsed anonymously?	No, nearly all activity can be seen by your ISP.	Usually, especially if you use a VPN to access.	With precautions, yes.

Even though, due to this difficult regulation, the darknet has always unsurprisingly been associated with crime, it is important to emphasise that not all activities occurring on this part of the web are malicious. For instance, the anonymity it offers can be useful for education and research, or within oppressive regimes of mass surveillance.[126] Nevertheless, it remains a forum allowing, inter alia, the spread of illegal selling of drugs and arms, the production of false documents, blackmail and extortion, terrorist recruitment and planning, and, more importantly, of sex trafficking and child pornography.[127] As an illustration, Stop the Traffik, a British NGO focusing on intelligence prevention for fighting human trafficking, published a study in 2018 on the basis of data collected from DeepPaste, a website allowing the posting of anonymous messages, requests and offers.[128] The study brought to light paste titles such as 'girls for rent and sale', 'sale or rent' and 'child escorts'. Another study made in 2016 established that four out of five searches in the dark web involved paedophile activity and child sexual abuse material (CSAM).[129]

[126] Stop the Traffik (n 125).
[127] FindLaw, 'Dark Web Crimes' (15 May 2019) <https://criminal.findlaw.com/criminal-charges/dark-web-crimes.html> accessed 11 May 2020.
[128] Stop the Traffik (n 125) 1.
[129] A Greenberg, 'Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds' (*Wired*, 30 December 2014) <www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/> accessed 22 April 2020.

Figure 7. Paste titles and comments Sources: Stop the Traffik. 'Human Trafficking and the Darknet. Insights on Supply and Demand' (Centre for Intelligence Led Prevention 2018) 3.

Figure 1. Paste titles

Figure 2. Paste comments

DarkScandals provides another striking example of how the dark web may be used for trafficking ends. The website used to advertise itself as featuring over 2,000 videos and images of 'real blackmail, rape and forced videos of girls all around the world', in particular paedophile material.[130] Following an operation led by authorities and Europol, the page was seized, and its administrator arrested in March 2020. The scope of anti-trafficking activities taking place on the dark web can therefore not be denied, especially knowing the difficulty to track them. In this regard, it is worth adding that dark web users make all their payments with a cryptocurrency (usually Bitcoin) which allows laundering transactions from operations to be carried out quickly and almost anonymously.[131] Law enforcement agents are therefore confronted with the specific difficulty of tracing these transactions.

Although this section demonstrated that the internet undoubtedly constitutes the most used digital tool to advertise, recruit and exercise control over victims of sexual exploitation, it is worth acknowledging that mobile and wireless technology also have completely changed the trafficking landscape today. The following section will therefore address this development.

3.2 Through mobile and wireless technology

According to the World Bank, almost fourth-fifth of the world's population owns a mobile phone, with the poorest households more likely to have access to mobile technology than to toilets or clean water.[132] Just as the internet completely reshaped the ways we are exchanging information, mobile technology, which has been adopted more quickly and broadly than any communication technology

[130] Europol, 'Dark Web Child Abuse: Administrator of DarkScandals arrested in the Netherlands' (Europol press release 12 March 2020) <www.europol.europa.eu/newsroom/news/dark-web-child-abuse-administrator-of-darkscandals-arrested-in-netherlands> accessed 9 July 2020.

[131] Ambassade de France en Bulgarie, 'De l'utilisation frauduleuse d'Internet pour favoriser l'exploitation des personnes… quelles réponses apportées par le secteur public et le secteur privé?' (2018) <https://bg.ambafrance.org/De-l-utilisation-frauduleuse-d-Internet-pour-favoriser-l-exploitation-des> accessed 5 May 2020.

[132] World Bank Group, *World Development Report 2016. Digital Dividends* (International Bank for Reconstruction and Development / The World Bank 2016) 2.

in history,[133] has, without any doubt, revolutionised our way of communicating. By providing real-time coordination from anywhere in the world, new ways of advertising and of conducting transactions, cellular phones have also proven to be particularly profitable for business activities.

The globalisation of ICT services has led to the adoption of global standards and harmonised regulations aligning mobile operators and equipment producers.[134] This brought about the development of a whole range of text messaging websites and applications: Yahoo messenger, Facebook, WhatsApp, Viber and Skype for example. Those services can be accessed by anyone, almost everywhere. Although this 'explosive growth of the mass mobile market at a global scale'[135] may generally be regarded as a common good, it also raised new significant challenges, knowing they have provided a more fluid environment to criminal enterprises, and therefore, to traffickers.[136]

Due to the characteristics offered by mobile and wireless technologies, it is unsurprising that the latter are relying on them to a broader extent than other hardware such as video technologies, desktops, laptops, tablets and printers, scanners, telephones or televisions. In recent years, internet searches have started to be made predominately through mobile phones, with volumes of mobile data surpassing volumes of voice calling services.[137] This trend, combined with the availability and use of mobile money platforms and the percentage of smartphones operational on mobile networks may be considered not only as the 'mobile revolution',[138] but also as the 'tipping point' of ICT-facilitated trafficking.[139]

Sex traffickers typically use mobile technology, in particular applications,[140] to photograph victims and post their pictures through advertisements that can be easily modified when the latter are transported to new cities.[141] Mobile phones also allow them to communicate with partners, clients or victims, through text messaging or phone calls, whether within the country or abroad,[142] in particular through VoIP numbers[143] and prepaid and disposable phones.[144] The latter

[133] M Castells and others, *Mobile Communication and Society. A Global Perspective* (Cambridge MIT Press 2007) 27.

[134] M van Reisen and others, 'Tracing the emergence of ICT-enabled human trafficking for ransom' in R Piotrowicz, C Rijken and B Heide Uhl (eds), *Handbook of Human Trafficking* (Routledge 2018) 146.

[135] ibid.

[136] D-M Hughes, *Trafficking in Human Beings in the European Union. Gender, Sexual Exploitation, and Digital Communication Technologies* (Sage Open 2014) 5.

[137] A Ram, 'Modern Slavery Campaigners Turn to Online Exploitation' (*FT*, 28 August 2018) <https://next.ft.com/content/c6d6edce-3792-11df-88c6-00144feabdc0> accessed 6 May 2020.

[138] Hughes, *Trafficking in Human Beings in the European Union* (n 136) 4.

[139] van Reisen and others (n 134) 151.

[140] Thorn in collaboration with V Bouché, 'A Report on the Use of Technology to Recruit, Groom and Sell Domestic Minor Sex Trafficking Victims' (Thorn 2015) 20.

[141] V Greiman and C Bain, 'The Emergence of Cyber Activity as a Gateway to Human Trafficking', (2013), 12(2) International Journal of Cyber Warfare and Terrorism 5, 8.

[142] Surf and Sound (n 89) 34.

[143] Voice over Internet Protocol (VoIP), is a technology allowing to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line; see <www.fcc.gov/general/voice-over-internet-protocol-voip> accessed 13 April 2021.

[144] N Ungerleider, 'How Mobile Phones And The Internet Fight (And Help) Human Trafficking' (*Fast Company*, 1 August 2013) <www.fastcompany.com/1681155/how-mobile-phones-and-the-internet-fight-and-help-human-trafficking> accessed 10 July 2020.

have the particularity not to require any contract with network operators nor monthly costs for service, making them one of the last remaining anonymous communication tools.[145] In essence, while these prepaid phones may be efficiently used by marginalised groups such as political dissidents and migrant workers, they also create a 'potential tool for criminal activity'.[146]

Finally, it is worth noting that perpetrators are most of the time conducting transactions over cellular phones. Therefore, thanks to the hybrid nature of smartphones, recruiting, advertising and payments can be made on the go, and cyber-trafficking activities have become much easier and more effective due to the accessibility, availability, affordability and facility of mobile devices to operate.[147] Not to mention that offenders also use these devices to monitor information on law enforcement authorities' plans.[148]

On the other hand, just as the digital footprint found on the internet can provide, for law enforcement authorities, the ability to trace trafficking activities, mobile devices can also support anti-trafficking actions by furnishing evidence. This extensive use has made cell phones and text messages so important for enforcement officers that they sometimes describe them as 'golden evidence'.[149] However, the fact that the latter are using surveillance techniques and looking for individuals that are presumed to be potentially linked to human trafficking networks raises many issues in terms of privacy, as addressed in the following chapter. Therefore, the necessity to educate anti-trafficking agents about the creation and use of technology appears to be primordial. While those are beyond this thesis's scope, some initiatives which have been developed to educate consumers via mobile phone applications are worth mentioning, such as the Human Trafficking Toolkit, Redlight Traffic or ALOVE Cut It Out, among others.[150]

As this chapter tried to demonstrate, ICTs constitutes effective tools to recruit victims, to 'remotely control and influence their emotions, attitudes, and behaviors',[151] but also to ensure anonymised transactions and communication, and to stay updated about law enforcement actions.

Keeping these roles in mind, the next section will, after highlighting some issues related to ethics, privacy and security (section 1), address how data analytics (section 2) and AI (section 3) may also constitute a way to trap traffickers who have been using technology in the first place.

[145] M Latonero, 'Human Trafficking Online. The Role of Social Networking Sites and Online Classifieds' (Center on Communication Leadership and Policy, University of Southern California 2011) 33.
[146] ibid.
[147] van Reisen and others (n 134) 151.
[148] Surf and Sound (n 89) 34
[149] J-L Mustol and D Boyd, 'The Trafficking-Technology Nexus' (2014) 21(3) Social Politics 461, 472.
[150] For other examples, see C Apisa, 'Anti-trafficking Apps of Interest' (*End Slavery Now*, 29 June 2015) <www.endslaverynow.org/blog/articles/anti-trafficking-apps-of-interest> accessed 10 June 2020.
[151] van Reisen and others (n 134) 151.

4.

THE POTENTIAL OF ICTS TO PREVENT, INVESTIGATE AND PROSECUTE THE CYBERSEX TRAFFICKING OF WOMEN AND CHILDREN

4.1 Preliminary remarks regarding ethical, privacy and security concerns

Technological advancements provide unprecedented opportunities for law enforcement and the private sector to monitor illicit activity, analyse data to prosecute traffickers, and locate and rescue victims.[152] More specifically, data collection and AI have the potential to provide significant help to identify, track and prosecute traffickers through the information trail provided through digital tools.[153] Therefore, there is an obvious necessity to harness this useful potential, both through legal and non-legal means, as well as through stronger and coordinated legal, policy and technological solutions,[154] as the last chapter of this thesis will demonstrate.

In J Carey's views, 'electronics is neither the arrival of apocalypse nor the dispensation of grace. Technology is technology; it is a means for communication and transportation over space, and nothing more'.[155] Nuancing this technological neutrality perspective, J Kranzberg was writing as early as in 1986:

> Technology's interaction with the social ecology is such that technical developments frequently have environmental, social, and human consequences that go far beyond the immediate purposes of the technical devices and practices themselves, and technology can have quite different results when introduced into different contexts or under different circumstances.[156]

[152] R Sadwick, '7 Ways Technology is Fighting Human Trafficking' (*Forbes*, 11 January 2016) <www.forbes.com/sites/rebeccasadwick/2016/01/11/tech-fighting-human-trafficking/#65ad3a686cacn> accessed 15 May 2020.

[153] K Fedorschak and others, 'Data Collection and Human Trafficking' in M Chiarini Tremblay and others (eds), *Advancing the Impact of Design Science. Moving from Theory to Practice* (Springer 2014) 71.

[154] Equality Now, 'Technology and Trafficking. The Need for a Stronger, Gendered and Cooperative Approach' (Equality Now 2019) 1 <www.equalitynow.org/technology_and_trafficking_the_need_for_a_stronger_gendered_and_cooperative_response> accessed 11 July 2020.

[155] J Carey, 'Communication as Culture' in *Essays on Media and Society* (Routledge 2008) 139.

[156] M Kranzberg, 'Technology and History. "Kranzberg's Laws"' (July 1986) 27(3) Technology and Culture 544, 545.

In addition to these unexpected repercussions, ICT tools often have been said to be 'infused with the assumptions and biases of [their] creators'.[157] Therefore, in the same vein, claims have been arising in the context of the fight against sexual exploitation that sociotechnical inventions were designing a caricatured painting of the phenomenon.[158] In any case, and this is the underlying idea behind this work, these inventions may undoubtedly be used for good and bad purposes.

The dangers of the double nature of technology must be combined with other fears, such as the ones arising when looking at the rationale behind the adoption of legislation combating sexual exploitation. Indeed, the latter sometimes reveal other dubious objectives, such as racially rooted fears.[159] This warning must be borne in mind by bringing awareness to the fact that technologies are not sufficient on their own and do not constitute the 'miracle cure' to combat cybersex trafficking. Even more, one must stay aware of the potentially damaging impact of anti-trafficking identification efforts through sociotechnical inventions due to their often underlying gendered, racial, and cultural expectations.[160]

As an illustration, it has long been demonstrated that people of colour, including pimps, clients and sex workers, have been overwhelmingly subjected to 'heightened state surveillance and carceral punishment under the auspices of fighting trafficking'.[161]

Along with the possible biases, gender concerns are often raised in anti-trafficking efforts. In this regard, it makes little doubt that gender inequality and the lack of education are pillars of the sex trafficking industry. According to R Tidwell, these root causes are pushing individuals to routinely disregard the equal humanity of females and to accept their inferior treatment, abuse and, ultimately, trafficking.[162] Even more, as the previous chapter underlined, ICT tools themselves can be considered as a nexus of victimisation of female individuals. As emphasised by D-M Hughes, 'when some factors, particularly gender, sexual exploitation, and digital technologies, converge to create enhanced victimization, special attention is needed to look at the nexus of the problem and not just the separate elements'.[163] Therefore, it appears that a specific attention must be given to this nexus when developing digital tools, even if they appear at first glance to be aimed at supporting social justice causes and combating a gendered crime.

[157] D Boyd, 'When It Comes to Sex Trafficking, Tech Is Far From Neutral' (*Wired*, 6 July 2013) <www.wired.com/2013/06/bias-as-disruption-how-tech-disrupts-sex-trafficking/> accessed 25 May 2020.

[158] ibid.

[159] H Lieberman, 'Why Laws to Fight Sex Trafficking Often Backfire' (*The Washington Post*, 4 March 2019) <www.washingtonpost.com/outlook/2019/03/04/why-laws-fight-sex-trafficking-often-backfire/> accessed 25 May 2020.

[160] J Hua and H Nigorizawa, 'US Sex Trafficking, Women's Human Rights and the Politics of Representation' International Feminist Journal of Politics 412.

[161] E Bernstein, 'Militarized Humanitarianism Meets Carceral Feminism. The Politics of Sex, Rights, and Freedom in Contemporary Anti-trafficking Campaigns' (2010) 36 Signs 45.

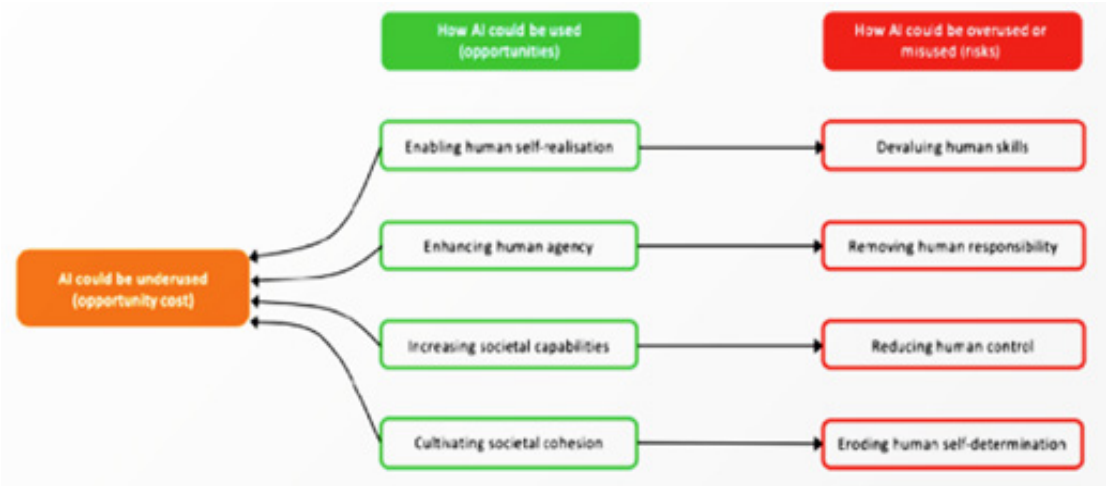
[162] R Tidwell, 'Caught in the Web. The Importance of Ethical Computing Illustrated via an Exploration of the Online Recruitment of Women and Girls into Sex Trafficking' (Western Oregon University, Honors Senior Theses/Projects 2016) 14.

[163] D-M Hughes, *Trafficking in Human Beings in the European Union. Gender, Sexual Exploitation, and Digital Communication Technologies* (Sage Open 2014) 5.

In addition to those concerns, attention must be drawn to the competition arising from the different anti-trafficking partnerships around technological innovations. Indeed, knowing that initiatives emanating from the private sector provide good business and corporate philanthropic sense, it is no wonder, as the following section will highlight, that tech giants such as Google, Microsoft and Palantir have joined the anti-trafficking combat.[164] Consequently, it comes as no surprise either that market-based values of competition are fastening the field. According to A Gallagher, this anti-trafficking environment can 'foster innovation and excellence, but it can also lead to duplication of experience and effort, contradictory standards, and closed circles of knowledge'.[165] In this sense, it is very important to study the impact that such an underlying ethos of competition has on law enforcement efforts. This is even more true knowing the existence of bias behind innovations and the possible oversight of important considerations such as gender concerns.

Finally, regarding AI techniques, it is important to emphasise that the latter present important opportunities, but also many challenges, particularly in counter-trafficking actions. Since the next paragraphs will be devoted to privacy and human control issues, the following graph summarises the main others.

Figure 8. AI ethical framework. Source: L. Floridi and others, 'The AI4People's Ethical Framework for a Good AI Society' (2018), 28 Minds and Machine, 689,691



Along with these ethical issues are the ones raised by privacy and data protection. According to R Finn, D Wright and M Friedewalds, privacy is 'a key lens though which many new technologies, and most especially new surveillance technologies, are critiqued'.[166] The previous chapter highlighted an array of legislation of binding nature emanating from the global and regional levels regulating this

[164] Mustol and Boyd (N 149) 467.

[165] A Gallagher, 'Human Rights and Human Trafficking. A Reflection on the Influence and Evolution of the U.S. Trafficking in Persons Reports' in A Brysk and A Choi-Fitzpatrick (eds), *From Human Trafficking to Human Rights: Reframing Contemporary Slavery* (University of Pennsylvania Press 2011) 192.

[166] R Finn, D Wright, and M Friedewald, 'Seven Types of Privacy' in S Gutwirth, R Leenes, and P De Hert, *European Data Protection. Coming of Age* (Springer 2013) 4.

right and protecting data. International soft law instruments do also provide relevant guidelines to promote ethical research and data collection, as long as they target research methods specific to trafficking, and a more active sharing of information.[167] In any case, the existence of those instruments emphasises that, while big data and machine learning have the potential to be very useful for anti-trafficking purposes, they should never compromise safety and privacy concerns.

Yet, research has demonstrated that staff combating human trafficking and working in victim protection often know very little about data protection laws.[168] This is problematic, given that enforcement officials, often along with third party vendors working in the field of predictive analytics,[169] are increasingly employing surveillance strategies to gather evidence and gain access to digital and mobile phone of both suspected traffickers and victims. Through tactics such as the monitoring of online classified ad sites, the creation of fake social networks accounts and online identities, and even the use of search incidents to arrest suspected victims in order to identify traffickers,[170] the concept of consent, which is at the heart of the right to privacy,[171] tends to be underpinned. This appears particularly striking in carcerally-orchestrated anti-trafficking efforts.[172]

Regarding data collection and knowing the high risk of intimidation and retaliation that trafficked women and children are facing,[173] the need to ensure an enhanced protection of their privacy and security cannot be emphasised enough. To that end, it is paramount that actors involved in data collection receive appropriate training, especially given that their awareness knowledge and training about privacy and data protection issues is often significatively limited.

Some recommendations have been made in order to ensure a better protection of victims in a data analytics context: ensuring secure storage of data, especially information that identifies a person; establish gender and age-sensitive consent protocols; assessing risks related to law enforcement release of information; ensuring that data collected from victims is used to assist them and to end exploitative practices, not for business purposes; ensuring the compliance with national and international legal frameworks, taking into account privacy and confidentiality standards; and addressing potential conflicts between the protection of anonymity and confidentiality, and providing support to victims of trafficking in accessing services or rehabilitation.[174] While those may not be exhaustive, they seem to constitute a necessary starting point to ensure that anti-trafficking data collection initiatives are made in line with the right to privacy and data protection.

[167] K Aromaa, 'Trafficking in Human Beings. Uniform Definitions for Better Measuring and for Effective Countermeasures' in E Savona and S Stefanizzi, *Measuring Human Trafficking. Complexities and Pitfalls* (ISPAC, Springer 2007) 43.

[168] M Wijers, 'Where Do All the Data Go? European Data Protection Law and the Protection of Personal Data of Trafficked persons', DatACT. Conference on data protection and trafficking, Berlin (25 September) <www.datact-project.org/fileadmin/user_upload/pdf/Marjan_Wijers.pdf> accessed 27 May 2020.

[169] Mustol and Boyd (N 149) 473.

[170] ibid 472.

[171] P Casanovas and others, 'Regulation of Big Data. Perspectives on strategy, policy, law and privacy' (2017) 7 Health Technol 335, 339.

[172] ibid.

[173] OHCHR, 'Recommended Principles and Guidelines on Human Rights and Human Trafficking. Commentary' (United Nations 2010) 146.

[174] ibid 196-202.

Finally, attention has to be drawn toward the tendency of social media messaging services to move towards 'end-to-end encryption', which implies the impossibility to access to the content of messages by third parties, including law enforcement and social media such as Facebook itself. If this trend has been appraised from the perspective of privacy defenders and is said to better protect users from hackers, it is also expected to raise many issues, including the growth of child sex abuse material, and of human trafficking in general. As Facebook founder M Zuckerberg stated in a 2019 blog, 'Encryption is a powerful tool for privacy, but that includes the privacy of people doing bad things'.[175] Precisely, this trend puts in jeopardy the whole process of 'decryption', namely the removal of this protection, which is exactly what anti-trafficking actors are targeting in their effort to address those 'bad things'.

The above-mentioned considerations are also applicable to the use of AI tools. Indeed, decision-making systems driven by AI also depend on the collection and exploitation of data, including personal and sensitive information.[176] Nevertheless, due to the 'complex ecosystem of technologies, platforms and private and public actors that facilitate access to and dissemination of information through digital means',[177] specific issues related to algorithmic systems are arising. In particular, recent developments of AI have allowed the proactive request for data without any human intervention. Due to the manipulative capabilities of algorithmic systems and the unpredictability of results provided by automated systems for the data subject,[178] it has become more challenging to control the impact of data collection processes.

In any case, attention must be drawn to the fact that privacy itself can be considered as a double-edged sword for women.[179] The internet and digital tools have offered, on the one hand, a space for their development and their emancipation from familial and social control all while being protected from criticism and censure.[180] On the other hand, these very same tools have created a forum which most of the time prioritises men's privacy, even when confronted to situations of violence.[181] Very often, 'civil liberties' grounds are invoked in an attempt to reject measures aiming at combating violence, for instance in the context of pornographic material use.

This is particularly true of the intricate issues raised by trafficking in images of sexual exploitation which often enters in conflict with privacy and freedom of expression. In this regards, D-M Hughes affirms that:

[175] The New York Times, 'Read Mark Zuckerberg's Blog Post on His "Privacy-Focused Vision" for Facebook' (*The New York Times*, 6 March 2019) <www.nytimes.com/2019/03/06/technology/facebook-privacy-blog.html> accessed 10 June 2020.

[176] Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, 'A study of the implications of advanced digital technologies (including AI systems) for the concept of responsibility within a human rights framework' (9 November 2018) 14.

[177] ibid 6.

[178] ibid 25.

[179] See D-M Hughes, 'Prostitution Online' (2003) 2(3) Journal of Trauma Practice 115.

[180] K Maltzahn, 'Digital Dangers. Information and Communication Technologies and Trafficking in Women' (APC Issue Papers 2006) 9.

[181] ibid.

> most people see the reduction or elimination of prosecution of adult pornography as being a victory for the individual rights of people and an end to suppressive government enforcement of morality-based laws. They assume all women in pornography are consenting, even when the women are visibly injured. If a woman protests after a photograph has been taken or a video made, people assume she consented at the time, but now is embarrassed by other people seeing it. Or they blame the victim and say she shouldn't have been so silly as to allow such photographs to be taken in the first place.[182]

While the importance of protecting pornography viewers' privacy and freedom should not be underestimated, several women's human rights, from their right to freedom and dignity to the prohibition of torture or inhuman treatment, tend, more often than not, to bend and erode behind these rights, although their consent had never been given in the first place.[183]

Whatever the digital tool at stake, it appears obvious that the whole set of anti-trafficking players has the duty to collaborate together, inside and outside governments, to ensure that data is used in a way that is protective of human rights. Above and before that, technologists carry an immense responsibility and a real ethical obligation to carefully consider the various potential impacts of any anti-trafficking technological development.[184]

The next sections will therefore address the main challenges this set of actors has to face while developing data analytics (section 2.A) and AI tools (section 3.A), all while providing illustrations of contemporary initiatives aimed at combating sexual exploitation in each of these fields (sections 2.B and 3.B). In order to have a more simplified overview of the whole set of anti-trafficking initiatives, the reader can at all times refer to the table which recapitulates the main anti-trafficking projects addressed in the following paragraph (end of section 3).

4.2 Data analytics

4.2.1 Practical challenges to data collection in the sex-trafficking arena

Data-driven intelligence is very common in the scientific field or the business community, and the private sector is routinely collecting data on consumer behaviours for targeted marketing strategies. Yet, although the need to obtain better data on both the perpetrators and the trafficked persons' side has been

[182] D-M Hughes, 'Role of Marriage Agencies in Trafficking in Women and Trafficking in Images of Sexual Exploitation', The Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation (EG-S-NT) (Committee for Equality between Women and Men (CDEG), Council of Europe 2001, 48.

[183] F Gerry, J Muraszkiewicz and N Vavoula, 'The Role of Technology in the Fight Against Human Trafficking. Reflections on Privacy and Data Protection Concerns' (2016) 32 Computer Law & Security Review 205, 207.

[184] Tidwell (n 162) 33.

repeatedly highlighted,[185] efforts to harness data and technological tools to address social problems seem to be lagging.[186] While they can still constitute a fruitful arena for data collection and AI if the most common challenges are faced, it makes little doubt that social issues such as human trafficking are more dynamic and complex than their technical counterparts.[187]

The main challenges encountered by anti-trafficking actors in the context of data collection firstly stem from the clandestine nature of sexual exploitation, and of human trafficking in general. Indeed, this essence causes perpetrators to conceal their identities and to operate in covert networks. This does not provide a fertile ground for data analysis. The results are therefore directly linked to secrecy: trafficking data is often highly unstructured, limited to numbers, and sometimes, not available at all.[188] In addition to this clandestine aspect, the absence of a clear definition of THB, emphasised in the first chapter, is pushing the different actors involved in data collection such as the police, courts and service providers, to apply international definitions that have been transposed differently in their national order, as well as different criteria in order to establish if a victim is trafficked or not. This lack of standardisation is responsible for provoking huge data recording discrepancies.

Therefore, unsurprisingly and despite the success of big data projects, very few initiatives have been launched in the human trafficking arena.[189] Indeed, for an industry that is expected to 'surpass drug and arms trafficking in its incidence, cost to human wellbeing and profitability to criminals within the next decade',[190] very few policies to gather data do actually exist, especially for sexual exploitation which is by itself is the most detected form of human trafficking.[191] The choice to make data collection a priority seems to vary with political will, and even, as surveys tend to demonstrate, are completely forgotten by the majority of law enforcement entities, the latter often abstaining from collecting human trafficking related data.[192]

Of course, without sufficient and reliable data, policymakers' decisions cannot be completely effective,[193] and knowledge must urgently be improved to increase the prospects of fighting this crime. In addition, collecting data is undoubtedly resource intensive, humanly, technically and financially, all while having to be done at the levels of prevention, investigation and prosecution.[194] But statistics do not

[185] Gerry, Muraszkiewicz and Vavoula (n 183) 212.
[186] M Latonero, 'The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking', Research Series on Technology and Human Trafficking (Center on Communication Leadership and Policy, University of Southern California 2012) 9.
[187] K-C Desouza and K-L Smith, 'Big Data for Social Innovation' [2014] Stanford Social Innovation Review 39, 40.
[188] B Peace, 'Using Data and Analytics to Combat Human Trafficking' (*IBM*, 18 October 2018) <www.ibm.com/blogs/think/2018/10/using-data-and-analytics-to-combat-human-trafficking/> accessed 10 July 2020.
[189] Desouza and Smith (N 187) 41.
[190] E Wheaton, E Schauer and T Galli, 'Economics of human trafficking' (2010) 48(4) International Migration 114.
[191] UNODC, *Global Report on Trafficking in Persons 2018* (United Nations Publications 2018). 10.
[192] Fedorschak and others (n 153) 72.
[193] ibid 70.
[194] B Hancilova and C Massey, 'Legislation and the Situation Concerning Trafficking in Human Beings for the Purpose of Sexual Exploitation in EU Member States' (International Centre for Migration Policy Development 2009) 24.

need to be 100% accurate to take immediate action,[195] and the digital footprint, in particular from internet and mobile sources data, has the potential to greatly help law enforcement officials to track suspects, corroborating relationships between them and the suspected exploited victims.[196]

Nevertheless, other challenges are emerging in data collection-targeted anti-trafficking strategies. Regarding the identification of victims, issues stem from the fact that they are often hidden or in transit,[197] all while being widely reluctant to speak out and, therefore, to self-identify.[198] As already emphasised, cybersex trafficking mainly targets women and children whose inherent vulnerability increases with the severe violence and abuse traffickers are inflicting most of the time. Coercion, collusion and contrition, or even Stockholm syndrome, if they are held captive,[199] are common phenomenon pushing victims to remain silent, and therefore depriving data of its existence in the first place. Even when data is available, other issues are emerging, as data abundance does not automatically imply representative or reliable data, for it can be easily manipulated.[200] It is therefore important to ensure its accurateness and robustness, all while placing the needs of the individuals anti-trafficking aims to serve at the centre of collecting efforts.[201] According to J Brunner, 'The answer for the anti-trafficking movement is not simply more data; it is better, more responsible data that goes far beyond annual donor reports or global statistics'.[202] For the same author, it implies that data should be valid, accurate, relevant, reliable, impartial, accessible, timely, responsible and empowering.[203] Of course, fulfilling all these criteria is an intricate task, but acknowledging the importance of such guidelines should be at the centre of data science initiatives.

Finally, although they are at the origin of the most important number of data collection initiatives, civil society organisations are encountering an additional number of challenges, such as the unreliability of indicators to measure anti-trafficking programmes and policy success, the lack of collaboration with governments, the focus on organisational needs and not global ones, the reluctance of some organisations to share data in raw form because of data privacy and security issues, and even the competition between agencies for scarce resources.[204] Nevertheless, they do provide valuable insights into various facets of sexual exploitation, as the following section will illustrate.

[195] Gerry, Muraszkiewicz and Vavoula (n 183).
[196] Mustol and Boyd (N 149) 469.
[197] M Leary, 'Fighting Fire with Fire. Technology in Child Sex Trafficking' (2014) 21 Duke Journal of Gender Law and Policy 289, 291.
[198] C Friesendorf, 'Strategies Against Human Trafficking. The Role of the Security Sector', Study Group Information (National Defence Academy and Austrian Ministry of Defence and Sports 2009) 24.
[199] Fedorschak and others (n 153) 72.
[200] Desouza and Smith (N 187) 41.
[201] J Brunner, 'Getting to Good Human Trafficking Data. Everyday Guidelines for Frontline Practitioners in Southeast Asia' (WSD Handa Center for Human Rights and International Justice of Stanford University, East-West Center and Human Rights Resource Centre 2018) 10.
[202] ibid 8.
[203] ibid 11-12.
[204] Fedorschak and others (n 153) 73.

As previously demonstrated, the predominantly under-reported nature of trafficking, coupled with the unreliability of data, the inadequacy of law enforcement efforts, and the lack of collaboration and data sharing initiatives constitute the main reasons explaining the lack of data, insight and understanding of human trafficking networks.[205] However, and this will be the object of the following section, so long as those challenges are addressed, some initiatives deserve to be appraised.

4.2.2 Contemporary trends and data analytics initiatives

By providing law enforcement, the private and non-governmental sectors as well as academia with new tools to identify traffickers' digital footprints[206] which have been analysed in Chapter III, initiatives emanating from partnerships around 'data analytics' are offering ways to improve strategies to uncover trafficking rings and prevent sexual exploitation. The following section will focus on the main projects mobilising big data, all while trying to consider, for each one, the principal issues and challenges that have been addressed in the previous sections. As already mentioned above, to have a more general picture of the initiatives analysed, the reader can at all time refer to the recapitulating table below.

For the purpose of succinctness and to preserve the focus on interdisciplinarity and on the technological aspect, the choice was made to narrow down this section to data initiatives emanating from private organisations. However, it is worth noting that governments are also increasingly using technological traces to identify traffickers. On the one hand, efforts have been made at the international level to regulate and standardise data collection instruments. This is the case of the UN Office of Drugs and Crime (UNODC), which has been calling for states, intergovernmental and nongovernmental organisations to collaborate on this issue.[207] Several EU member states have also been establishing a national rapporteur or equivalent mechanisms to address 'gaps' and centralise data collection in the human trafficking context.[208] On the other hand, international partnerships between law enforcement agencies have been created to mobilise data with the perspective of fighting sexual exploitation, such as the already mentioned VGT which aims to fight child abuse and exploitation.[209] At the level of the EU, the Europol Analytical Work File, through the operational project 'AP Phoenix',[210] and at the national level, initiatives such as the Belgian eCops system[211] are also worth mentioning.

In addition to these legitimate governmental tools, it is worth emphasising that *prima facie* 'illegal' means can also sometimes lead to successfully uncovering human traffickers. Although the technique is beyond the scope of this work and entails

[205] Fedorschak and others (n 153) 71.
[206] Latonero, 'The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking' (n 186) 27.
[207] See, in particular, Tool 9.15 of the UNODC, *Toolkit to Combat Trafficking of Persons*, *Global Programme against Trafficking in Human Beings* (United Nations Publications 2008) 470-477.
[208] Hancilova and Massey (n 194) 25.
[209] The law enforcement partnership is made out of 14 organisations, including Europol and Interpol.
[210] See Europol, 'Europol Analysis Projects' <www.Europol.europa.eu/crime-areas-trends/Europol-analysis-projects> accessed 9 June 2020.
[211] See eCops, 'Child pornography reporting platform' <www.ecops.be/request.php?Lang=EN> accessed 9 June 2020.

several dangers such as the risk of disturbing ongoing investigations or tainting evidence, 'hacktivism', which refers to 'the activity of getting into computer systems without permission in order to achieve political aims',[212] can play an important role in combating sexual abuse and trafficking. As illustration, Anonymous, the famous decentralised collective known for cyberattacks, successfully managed, through its 'Operation Darknet', to shut down several websites trading in images of child sexual abuse, including 'Lolita City', which included more than 1,500 users and 100 gigabytes of child porn.[213]

At the level of private organisations, it is not a surprise, given the importance of the use of social networks by cybersex traffickers, that initiatives around 'data analytics' are mainly focusing on 'data mining' from social media sources.[214] Penetrating social networking platforms, big data experts are able, by targeting the recruitment stage of trafficking activities, to better understand the scope of the phenomenon and identify perpetrators of sexual exploitation.[215] The issue of encryption and decryption, addressed in the previous section, has, however, to be kept in mind here, for it considerably challenges the work of these experts and raises heated debate among privacy defenders. Less problematically, anti-trafficking organisations are also routinely analysing advertisements, trying to locate linked phone numbers, and to search through datasets in order to identify information.

In addition to social network and website sources, collecting financial data is also of extreme value for law enforcement and victim advocates.[216] The investigation of payment systems may reveal certain patterns that are very useful to uncover networks. However, given that, as any crime organisation, trafficking rings frequently use money laundering all while mixing with profits from legitimate business, the disentanglement of the web of financial transactions inside the organisation is rendered difficult.[217] Here again, the role of companies which are performing 'data mining' or forensic accounting to identify suspicious transactions cannot be emphasised enough.[218] As illustration, researchers have been focusing on the possibility to link Backpage advertisements to Bitcoin transactions at the investigation phase.[219] As already mentioned, the website closed following a law enforcement action in 2014.

[212] Cambridge Dictionary, 'hacktivism' <https://dictionary.cambridge.org/dictionary/english/hacktivism> accessed 9 June 2020.

[213] J Hourdeaux, 'Un vaste réseau de sites pédophiles piraté' (*L'Obs*, 25 October 2011) <www.nouvelobs.com/les-internets/20111025.OBS3200/un-vaste-reseau-de-sites-pedophiles-pirate.html> accessed 10 June 2020.

[214] Fedorschak and others (n 153) 82.

[215] A Lucanus, 'Can Big Data Help Us Stop Human Trafficking?' (*DataFloq*, 3 February 2020) <https://datafloq.com/read/can-big-data-help-us-stop-human-trafficking/7611> accessed 10 June 2020.

[216] T Sneed, 'How Big Data Battles Human Trafficking' (*US News*, 14 January 2015) <www.usnews.com/news/articles/2015/01/14/how-big-data-is-being-used-in-the-fight-against-human-trafficking> accessed 26 May 2020.

[217] J Wu, "AI Is Helping Us Combat The Economic Problem Of Human Trafficking" (*Forbes*, 14 April 2020) <www.forbes.com/sites/cognitiveworld/2020/04/14/ai-is-helping-us-combat-the-economic-problem-of-human-trafficking/#546e08a0752c> accessed 19 June 2020.

[218] M Latonero, 'Human Trafficking Online. The Role of Social Networking Sites and Online Classifieds' (Center on Communication Leadership and Policy, University of Southern California 2011) 26.

[219] R Portnoff and others, 'Backpage and Bitcoin. Uncovering Human Traffickers' 23rd ACM SIGKDD International Conference (2017) 1-10.

After having highlighted the main techniques used by law enforcement and data analytics experts, the following paragraphs will be devoted to providing illustrations. In the field of 'data mining', the main initiative worth acknowledging is undoubtedly the Global Human Trafficking Hotline Network, created through the cooperation between three global data enterprises in 2013: Palantir, Google and Salesforce, along with the collaboration of the NGO sector: the US-based anti-trafficking organisation Polaris, the European NGO network La Strada International and the Hong-Kong-based NGO Liberty Shared. This alliance, which originally aimed to transform data from existing anti-trafficking hotlines into a global database, displaying both trafficking routes and supporting infrastructure for victims in a real-time mapping,[220] led to the creation of the CTDC,[221] a database founded by Polaris and the International Organization for Migration (IOM), and supported by Liberty Shared.

Since 2007, Polaris has operated the US National Human Trafficking Hotline, providing 24/7 support for survivors of human trafficking.[222] Acting as an inspiration for other countries such as Vietnam and Canada, it has also been administering global consulting practice through the offering of a range of services for governments and NGOs seeking tools and practices.[223] Finally, the organisation is contributing to the Global Modern Slavery Directory, a 'publicly searchable database of over 2,900 organizations and hotlines working on human trafficking and forced labor around the world'.[224]

The CTDC is the most relevant project for this research since it has housed the first-ever global data hub on human trafficking aiming at breaking down the information-sharing barriers that have been addressed in the previous sections. Launched in 2017 and focusing on providing up to date and reliable data on THB by leveraging modern technology, the collaborative is said to have provided access to CTDC data to users from over 150 countries and territories.[225] The initiative is based on case management data gathered from identified cases recorded in a case management system and stemming from assistance activities of the contributing organisations, including from case management services and from counter-trafficking hotline logs.[226]

[220] B Heide Uhl, 'Assumptions Built into Code. Datafication, Human Trafficking, and Human Rights. A Troubled Relationship?' in R Piotrowicz, C Rijken and B Heide Uhl (eds), *Routledge Handbook of Human Trafficking* (Routledge International Handbooks 2017) 410.

[221] The Counter Trafficking Data Collaborative (CTDC), 'Global Data Hub on Human Trafficking' <www.ctdatacollaborative.org/> accessed 10 June 2020.

[222] Polaris, 'Responding to Human Trafficking' <https://polarisproject.org/responding-to-human-trafficking/> accessed 11 June 2020.

[223] ibid.

[224] Global Modern Slavery Directory <www.globalmodernslavery.org/> accessed 11 June 2020.

[225] CTDC, 'Telling Their Stories Through Open Data' <www.ctdatacollaborative.org/about-us> accessed 11 June 2020.

[226] ibid.

Figure 9. Global datahub on human trafficking. Source: CTDC, 'Global Data Hub on Human Trafficking' <www.ctdatacollaborative.org/> accessed 10 June 2020.

While the collaborative seems very appealing, allegations of the publication of misleading data arose in 2011.[227] However, this was before Polaris partnered with data analysis firm Palantir Technologies, which is said to have improved the organisation of data and the accuracy of statistics released to the public. In addition, the CTDC seems to have due regard to the protection of rights, emphasising the necessity to guarantee privacy and data protection on its website.[228] In particular, the company states that it ensures that all explicit identifiers are removed from the global victim dataset. It also affirms to ensure the transformation of data, for instance through the ranking of age into age ranges, ensuring that no personally identifying information is transferred to or hosted by the partnership. Finally, it ensures that anonymisation is made by all the contributing organisations.

Therefore, although it is very difficult – and beyond the scope of this thesis – to verify the adequacy of the data provided by the alliance, especially in the context of the inherent difficulty to collect data as already discussed in the beginning of this section, it seems that the CTDC has been considering the main privacy and data protection concerns and appears at first sight to have taken the legislative framework analysed in Chapter II into account.

A similar partnership has been established by the Global Emancipation Network (GEN), composed by experts in technologies and big data analysts such as Microsoft, Recorded Future, Splunk, Accenture, Owl Cybersecurity, Deep Vision, GitHub, Maltego, Chainanalysis and Neustar. This alliance has built **Minerva**, a data analytics platform enabling 'secure, individualized data sharing and the easy application of intelligent analytics in the field of human trafficking'.[229]

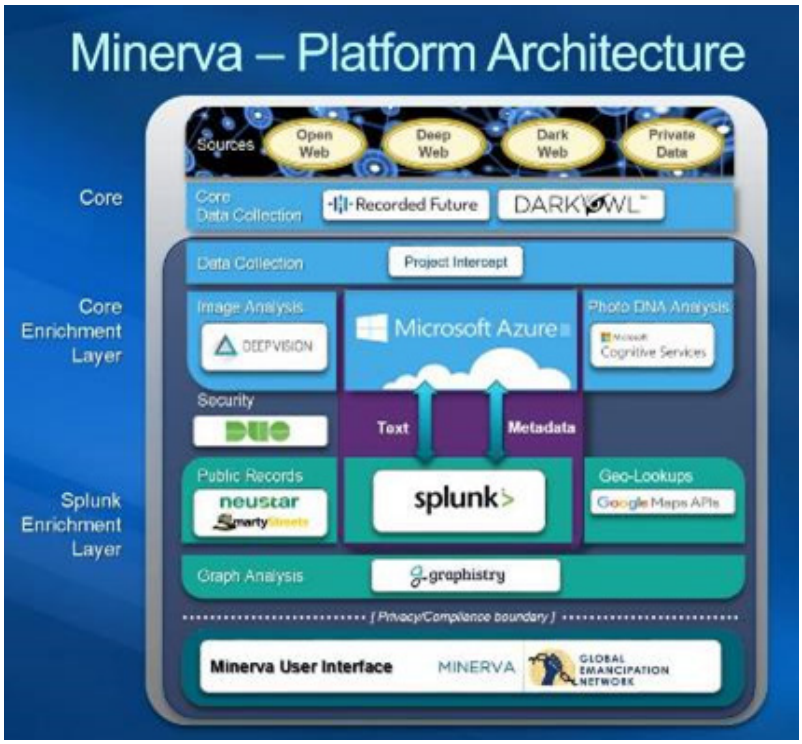
[227] NC Harm Reduction Coalition, 'Why are Sex Worker and Public Health Advocates Annoyed with Google?' (*Daily Kos*, 21 December 2011) <www.dailykos.com/stories/2011/12/21/1047597/-Why-are-Sex-Worker-and-Public-Health-Advocates-Annoyed-with-Google> accessed 11 June 2020.

[228] CTDC, 'FAQ' <www.ctdatacollaborative.org/faqs> accessed 11 June 2020.

[229] K Schreiner, 'Data for Social Good Case Study: Global Emancipation Network' (*SIX*, 2 July 2018) <https://socialinnovationexchange.org/insights/data-social-good-case-study-global-emancipation-network> accessed 11 June 2020.

The GEN collects data on THB, from both the surface and deep web to gain insight into trafficking through advertisement analysis, text analysis tools and natural language processing, using public records, open web searches and image processing tools such as Microsoft's PhotoDNA[230] (see section 2). But what makes the initiative stands out from a data analytics point of view is that Minerva's data is made available free of charge to law enforcement, government agencies, researchers, academia and anti-trafficking non-profit organisations so they can combine this data with their own specialised datasets.[231]

Figure 10. Minerva platform architecture. Source: Global Emancipation Network, 'Products' <www.globalemancipation.ngo/products/> accessed 11 June 2020.



While, again, the partnership seems particularly appealing, specifically for its availability, what appears to be striking is the lack of information about data protection and privacy concerns on the website of the GEN. However, the website of Splunk,[232] the data analysis technology company powering this project, provides such information. Therefore, it can be contended by deduction that considerations regarding privacy and data protection are also considered in the context of the initiative. In this regard, in addition to security agreements, Splunk is certified to the EU-US and Swiss-US Privacy Shield Frameworks,[233] aiming to enable the transfer of personal data from the European Economic Area, the United Kingdom

[230] Global Emancipation Network, 'Products' <www.globalemancipation.ngo/products/> accessed 11 June 2020.
[231] ibid.
[232] Splunk, 'Guiding Principles' <www.splunk.com/en_us/legal/splunk-data-security-and-privacy.html> accessed 31 July 2020.
[233] Both frameworks can be found on <www.privacyshield.gov/eu-us-framework>, accessed 13 April 2021.

and Switzerland to the United States.[234] The company also employs a dedicated data protection officer who oversees the collection and use of data.

Some initiatives focusing on prevention are also worth mentioning. In addition to working with AI tools, as the next section will address, the NGO Stop the Traffik has been mobilising crowdsourced and open-sourced data to combat human trafficking[235] together with its Traffik Analysis Hub (TAHub) platform (see section 3). As a process largely mobilised in data analytics, 'crowd knowledge sourcing' refers to the 'utilization of the knowledge possessed by Web users for the collection and/or analysis of mass data'.[236] The oldest example of this type of source is undoubtedly Wikipedia, but open-source software allowing for the contribution of anyone is also flourishing on the internet. Coming back to the anti-trafficking context, with the idea that 'the most innocent clues can sometimes help crack a case', Europol developed the **TraceanObject** tool on its website to ensure the contribution of everyone, through posting pictures of children's belongings, to the fight against their sexual abuse.[237]

Figure 11. Europol Stop Child Abuse. Source: Europol, 'Stop Child Abuse – Trace an Object' <www.Europol.europa.eu/stopchildabuse> accessed 9 June 2020.

[234] <www.splunk.com/en_us/legal/splunk-data-security-and-privacy.html#tabs/tab_parsys_tabs_CustomerDataPrivacy_1> accessed 17 June 2020.

[235] B Grove and A Bedi, 'It's time we harnessed Big Data for good' (*World Economic Forum*, 17 October 2019) <www.weforum.org/agenda/2019/10/data-big-harness-good-human-trafficking-stop-the-traffic/> accessed 28 April 2020.

[236] J Howe, 'The rise of crowdsourcing' (*Wired*, 6 January 2006) <www.wired.com/2006/06/crowds/> accessed 3 June 2020.

[237] See Europol, 'Stop Child Abuse – Trace an Object' <www.Europol.europa.eu/stopchildabuse> accessed 9 June 2020.

Keeping that in mind, Stop the Traffik is also behind the creation of the phone application '**STOP APP**' which allows anyone to submit suspicious activity by sending text-based messages and uploading photos and videos.[238] As the next section will highlight, the initiative also combines data analytics with AI techniques. Still from the perspective of preventing trafficking, the Australian Company Quantium is behind the **Operation Red Alert** which aims to identify the villages in India that are at most risk of committing sexual exploitation of women and children. Finally, at the individual and on a more anecdotical level, Eric Shles, a New York-based data scientist has created TraffickingGrab,[239] a tool to analyse websites for evidence of sexual exploitation, using Selenium and Tor to investigate hardly accessible deep web trafficking traces.

After briefly highlighting the main issues brought by anti-trafficking tools using machine learning techniques, the following section will address the partnerships made around sociotechnical inventions aiming to use AI to combat cybersex trafficking.

4.3 Artificial intelligence

4.3.1 Machine learning and the fight of THB for sexual exploitation

As already highlighted in the previous section, AI has a considerable influence on data collection. Through machine learning, the potential and impact of big data in anti-trafficking efforts significantly increase in comparison with traditional data collection tactics. AI is said to improve data by creating new methods to analyse it, making analytics less labour-intensive, while, at least in theory, keeping human decision at the centre of intelligence.[240] Recent advances in matrix completion, a type of machine learning, even have the potential to 'help clean up falsified information or make predictions about missing data',[241] which seems particularly relevant given the challenges raised by the lack of data in human trafficking.

Today, textual and image cues such as third person voices, obfuscated faces in images or certain keywords that could indicate a trafficking situation are routinely looked for by law enforcement within escort advertisements.[242] Those efforts, which can be partially automated by machine-learning methodologies through classifier models trained to identify instances of trafficking, have the capacity, for instance, to monitor escort advertisements and compute their likelihood to potentially involve trafficking.[243]

[238] Stop the Traffik, 'The Stop App' <www.stopthetraffik.org/stopapp/> accessed 11 June 2020.
[239] GitHub, 'Bornlex/traffickingGrab' <https://github.com/Bornlex/traffickingGrab> accessed 11 June 2020.
[240] K Casey, 'How Big Data and AI Work Together' (*The Enterprisers Project*, 14 October 2019) <https://enterprisersproject.com/article/2019/10/how-big-data-and-ai-work-together> accessed 15 June 2020.
[241] R Konrad and AC Trapp, 'Data Science Can Help us Fight Human Trafficking' (*The Conservation*, 28 July 2017) <https://theconversation.com/data-science-can-help-us-fight-human-trafficking-81647> accessed 11 June 2020.
[242] A Dubrawski and others, 'Leveraging Data to Discern Human Trafficking Pattern' [2015] Journal of Human Trafficking 65, 70.
[243] ibid.

However, as already highlighted above, since these approaches are relatively new, they introduce the possibility of false positives as well as potential privacy and civil liberties breaches. While it appears primordial to ensure that human beings are always on the loop, applying common sense and judgement to the inputs and outputs of AI,[244] the process of pattern identification remains highly complex, and algorithmic systems are far from impartial: their 'shape and design are being constrained by the assumptions and "procedural logic" held by the sociotechnical actors who create them'.[245]

Keeping those considerations in mind, the following section will summarise the most relevant and promising AI initiatives that have been recently developed to support the fight against sexual exploitation. Here again, to have a general overview of the AI partnerships, the reader can refer to the summarising table below.

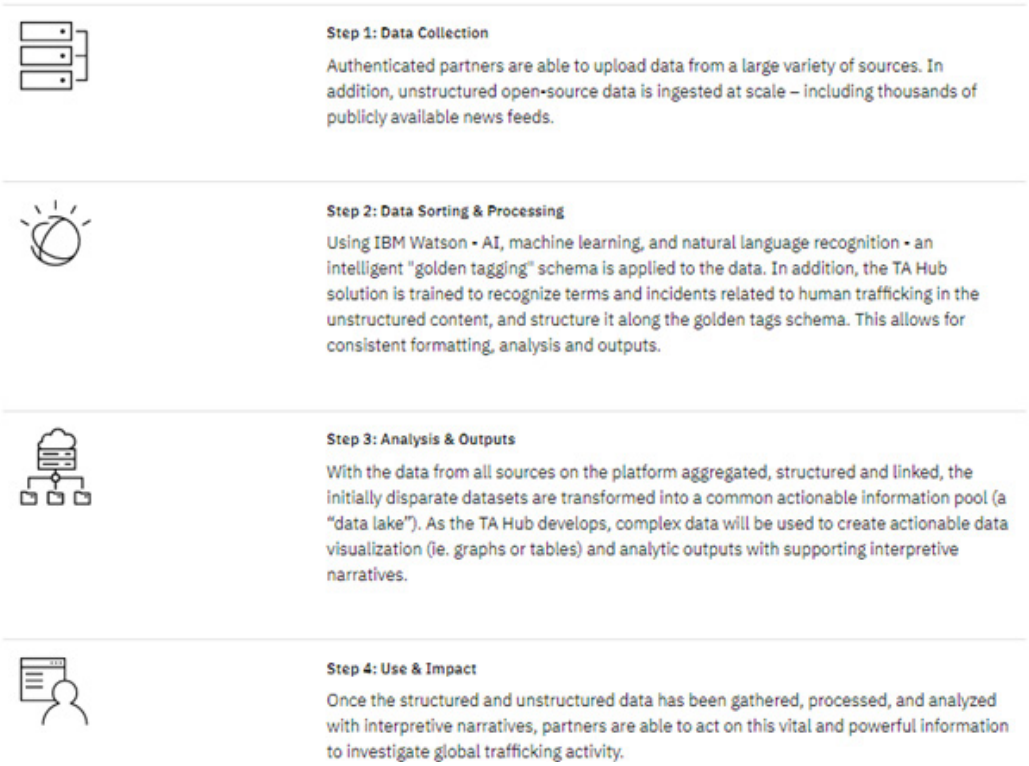
4.3.2 Trends and contemporary AI initiatives

The largest scaled initiative is undoubtedly the **TAHub**.[246] TAHub was launched in 2019 through a partnership between the largest computer company IBM, the international law firm Clifford Chance and the NGO Stop the Traffik. Supported by other NGOs such as Allies and the International Center for Missing and Exploited Children, it is also assisted by the financial institutions Red Compass, Western Union, Barclays and Lloyd's Banking Group, as well as the law enforcement agency Europol and University College London. The initiative is mobilising IBM's data hub's intelligence,[247] which is consolidated through a visualisation platform to provide insights about illicit trafficking operations, such as the market supply and demand, trafficking routes and financial flows.[248]

As briefly mentioned in the previous section, the initiative is focusing on prevention, overlapping the multiple datasets with public and open-source data. This creates 'a virtual community of intelligence on where trafficked victims come from, how they get where they are, and in which regions and industries they are most likely to end up working'.[249] Information obtained through this process can therefore be used by financial organisations, for example, to identify where people are financially benefiting from trafficking, and then establish processes that make it riskier for them to do so.[250]

[244] Mustol and Boyd (n 149) 473.
[245] ibid.
[246] Traffik Analysis Hub <www.traffikanalysis.org/> accessed 15 June 2020.
[247] IBM Big Data Hub <www.ibmbigdatahub.com/> accessed 15 June 2020.
[248] Traffik Analysis Hub, 'Our Mission' <www.traffikanalysis.org/our-mission> accessed 15 June 2020.
[249] Stop the Traffik, 'Traffik Analysis Hub' <www.stopthetraffik.org/what-we-do/traffik-analysis-hub/> accessed 15 June 2020.
[250] ibid.

Figure 12. Traffik analysis hub. Source: Traffik Analysis Hub, 'How It Works' <www.traffikanalysis.org/how-it-works/> accessed 29 July 2020.



After carefully examining the websites of the TAHub and Stop the Traffik, it appears again that no consideration is given about privacy and data protection concerns. However, IBM has, very early on, developed principles and guidelines to ensure that their inventions are ethical and respectful of legislation. These are the IBM Principles for Trust and Transparency,[251] which require to ensure that AI's objective is to augment human intelligence, that data and insight belong to their creator, and that new technology, including AI systems, are transparent and explainable.

IBM also affirms on its website that it ensures that all its technologies comply with data privacy laws everywhere in which the company operates. From a practical point of view, the company could even be said to be a leader in the protection of privacy, being the first to develop and adopt soft law instruments such as the EU Data Protection Code of Conduct for Cloud Infrastructure Service Providers in Europe (CISPE)[252] and the Asia-Pacific Economic Cooperation Cross-Border Privacy Framework.[253] Likewise, it has established a comprehensive compliance framework to ensure GDPR compliance for all IBM products and services. Finally, the company has developed SPbD@IBM, a 'streamlined and agile set of focused security and privacy practices ensuring the embedding of security and privacy into

[251] IBM, 'Principles for Trust and Transparency' <www.ibm.com/ibm/responsibility/2017/assets/downloads/IBM-2017-CRR-Principles.pdf> accessed 15 June 2020.

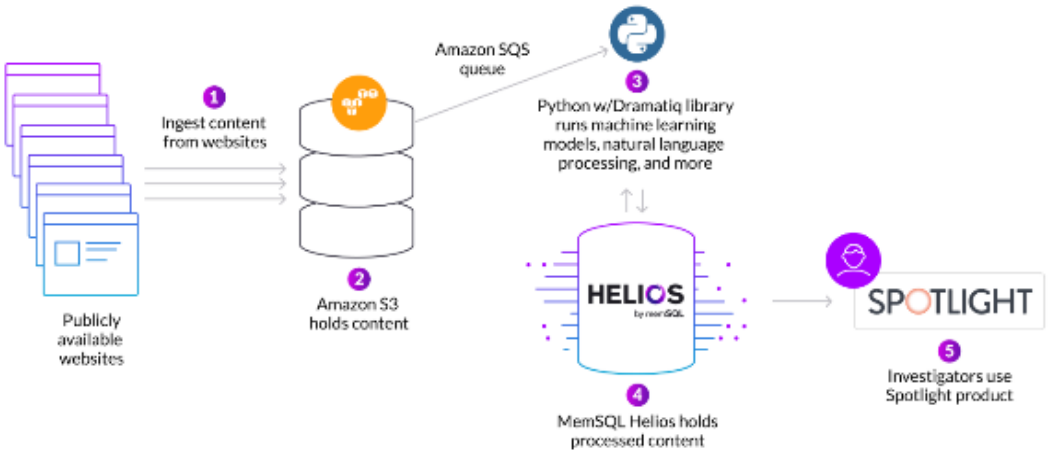
[252] EU Data Protection Code of Conduct for Cloud Infrastructure Service Providers in Europe, 27 January 2017, (CISPE)

[253] Asia-Pacific Cooperation Cross-Border Privacy Framework, 2015 (APEC).

the design of the company's products, offerings, and services'.[254] Therefore, given that IBM is behind the data hub, it seems that the initiative carefully considered the risks and threats that the use of AI is posing to the right to privacy and data protection laws.

On a smaller scale, the **Spotlight** initiative is also worth acknowledging. Developed through a partnership between the US-based AI company Digital Reasoning and the international organisation Thorn whose mandate is to fight against the sexual exploitation of children, it has been established as a web-based tool aiming to help with the identification and assistance of those victims. Powered by Digital Reasoning's cognitive computing platform Synthesys, it provides law enforcement with intelligence about suspected human trafficking networks and individuals. According to the computing platform, the initiative has, to date, been assisting more than 8,300 US investigations conducted by 780 law enforcement agencies and has contributed to the identification of 6,625 victims and 2,255 pimps, all while reducing investigation times by 44%.[255] Today, Thorn mobilises several data analytics and machine learning processes, summarised in the following chart:

Figure 13. Thorn. Source: F Smith, 'Case Study. Thorn Frees up Resources with MemSQL Helios to Identify Trafficked Children Faster' (SingleStore, 5 December 2019) <www.memsql.com/blog/case-study-thorn-frees-up-resources-with-memsql-helios-to-identify-trafficked-children-faster/> accessed 29 July 2020.



However, it is worth emphasising that the websites of Thorn and Digital Reasoning do not seem to leave room for privacy and data protection considerations. Concerns have also been raised by technology writer V Blue; focusing on the war on sex-trafficking and the non-consensual tracing of sex workers, she went as far as describing Spotlight as 'terrifying and practically purpose-made for abuse'.[256] While this argument should be carefully examined, it remains that any

[254] IBM, 'IBM Security and Privacy by Design / SPbD@IBM' <www.ibm.com/trust/security-spbd> accessed 15 June 2020.
[255] Digital Reasoning, 'We Found a Way…' <https://digitalreasoning.com/resources/thorn-case-study/> accessed 23 April 2020.
[256] V Blue, 'Sex, Lies, and Surveillance. Something's Wrong with the War on Sex Trafficking' (*Engadget*, 31 May 2019) <www.engadget.com/2019/05/31/sex-lies-and-surveillance-fosta-privacy> accessed 11 July 2020.

company working so closely with data, especially about victims, should include considerations about privacy laws in addition to the privacy policy related to how information or cookies are collected from the website viewer's activity,[257] in addition to specifically integrating information on how AI tools are respecting the above-mentioned framework.

T Estes, Digital Reasoning's founder and president, questions, on the website of the company, the so-called dash for data tendencies which appear to focus on demanding a large quantity of data in order to train AI machines. In his opinion, the qualities that most influence understanding and intelligence are not based on data volumes, but on better algorithmics systems.[258] This seems like an interesting argument, knowing the inherent issues raised by anti-trafficking efforts, especially the unreliability and lack of data. However, this emphasis on AI quality does not mean that the Spotlight initiative should escape from its legal obligations, especially knowing that the company still routinely uses a massive amount of data, in particular about women and child victims of THB.

In addition to initiatives trying to improve data analytics, AI tools also support the fight against sexual exploitation by focusing on face recognition. Although both techniques are supported by AI, it is necessary, in this regard, to differentiate facial recognition from photo recognition: while the first allows the mapping of facial features from an image and then comparing this information with a database to find a match,[259] the second aims to identify copies of a particular photo among the 'sea of images on the Internet'.[260]

Some initiatives have been focusing on facial recognition. This is the case of **TrafficJam,** operated by MarinusAnalytics, a woman-owned company founded in 2014 out of Carnegie Mellon Robotics. Working in collaboration with the US-based NGO National Center for Missing and Exploited Children, the initiative has been named this year as one of ten global semi-finalists for the prestigious IBM Watson AI XPRIZE, a competition aiming to promote AI innovations to tackle global challenges.[261] The partnership has the goal to investigate 'how AI can turn big data online into actionable intelligence',[262] using a suite of analytics tools, including the Amazon Rekognition AI service. This does so by identifying people, objects, scenes, text and activities in images and videos, and detecting any inappropriate content, as well as 'highly accurate facial analysis and facial search capabilities that can be used to detect, analyze, and compare faces for a wide variety of user verification, people counting, and public safety use cases'.[263] In addition to this service, TrafficJam also uses the SimSearch feature which aims, in

[257] Digital Reasoning, 'Privacy' <https://digitalreasoning.com/privacy/> accessed 11 July 2020.
[258] Digital Reasoning, 'What Offers More Hope – More Data or Better Algorithms?' <https://digitalreasoning.com/resources/offers-hope-data-better-algorithms/> accessed 15 June 2020.
[259] Addepto, 'Using Artificial Intelligence (AI) for Image Recognition' (15 July 2019) <https://addepto.com/using-artificial-intelligence-ai-for-image-recognition/> accessed 17 June 2020.
[260] Latonero, 'Human Trafficking Online. The Role of Social Networking Sites and Online Classifieds' (n 218) 31.
[261] XPrize, 'AI to Solve Global Issues' <www.xprize.org/prizes/artificial-intelligence> accessed 18 June 2020.
[262] XPrize, 'Marinus Analytics' <https://ai.xprize.org/prizes/artificial-intelligence/teams/marinus_analytics> accessed 18 June 2020.
[263] AWS, 'Amazon Rekognition', <https://aws.amazon.com/rekognition/?nc1=hls&blog-cards.sort-by=item.additionalFields.createdDate&blog-cards.sort-order=desc> accessed 18 June 2020.

cases where a facial profile is not visible, to look for similar images, find the same person in different photos and even identify new victims.[264]

Since no consideration is made about data protection and privacy on the website of MarinusAnalytics, the latter must be looked for on the Amazon Rekognition website, the main tool used by the company. From a data protection perspective, Amazon Web Services (AWS) guarantees that its recognition service complies fully with the GDPR and provides customers with several resources to ensure that they comply, through their operations, with the EU regulation.[265] This is done through AWS' adherence to the CISPE,[266] granular data access controls, monitoring and logging tools, encryption, key management, audit capability, adherence to IT security standards and AWS' C5 attestations.[267]

From the point of view of privacy, the company is mobilising several encryption and deletion tools all while monitoring the processing of personal data through CloudTrail, a service providing a record of actions taken by a user, role or an AWS service in Amazon Rekognition.[268] However, it remains to be seen if other ICT tools do provide the same guarantees. Moreover, some researchers have been contending that photo recognition services such as Amazon Rekognition do suffer severe racial and gender bias,[269] confirming once again the urgency of carefully examining algorithmic error rates and their underlying causes.

With regard to photo recognition, in the same vein as Amazon through its facial recognition programme, the technological multinational company Microsoft, in partnership with Dartmouth College, developed **PhotoDNA** in 2009. The tool consists of a 'hashing technology', which develops a 'signature' for online photos of exploited children. Through the creation of a digital fingerprint which converts the image into a grayscale format, a grid is created, and a number is assigned to each square of the format. This number is the 'hash' of the image, its 'PhotoDNA signature'. This hash can then be used to locate the photo on the internet, even if it has been altered.[270] Since 2018, the tool has been developed to work on videos as well.[271]

[264] Marinus Analytics, '27th Annual Crimes Against Children Conferences' (28 August 2015) <www.marinusanalytics.com/articles/2015/8/28/27th-annual-crimes-against-children-conference> accessed 18 June 2020.

[265] AWS, 'Using AWS in the Context of Common Privacy & Data Protection Considerations' (May 2018) 10 <https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf> accessed 18 June 2020.

[266] CISPE Cloud, 'Data Protection. Code of Conduct for Cloud Infrastructure Service Providers' (27 January 2017) <https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf> accessed 18 June 2020.

[267] AWS, 'Using AWS in the Context of Common Privacy & Data Protection Considerations' (n 265) 10.

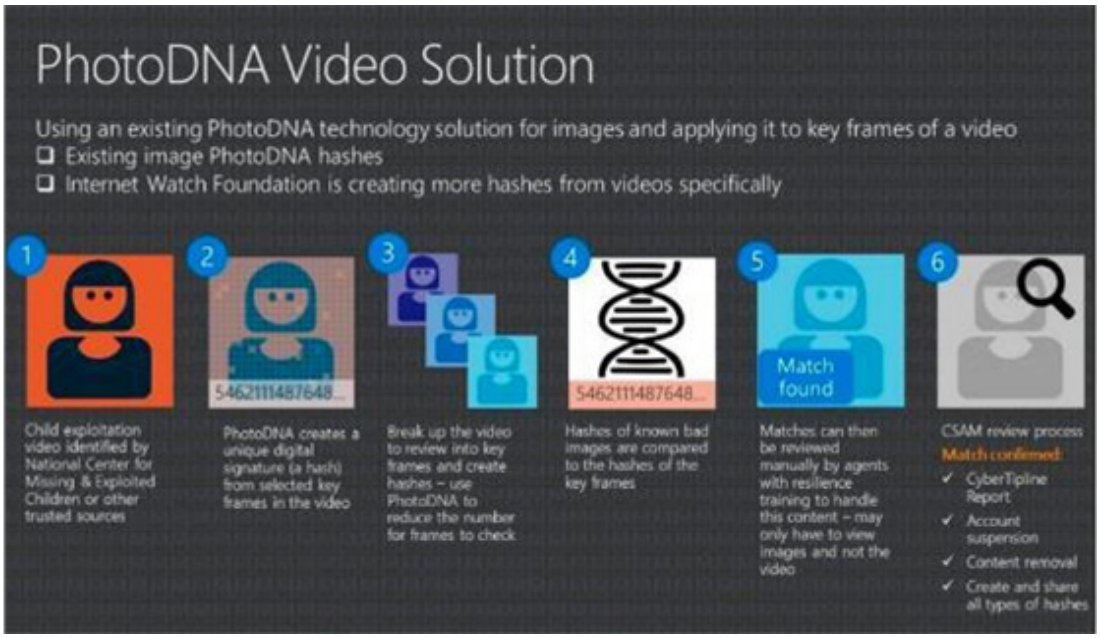
[268] AWS, 'AWS Service Capabilities for Privacy Considerations' <https://aws.amazon.com/compliance/data-privacy/service-capabilities/> accessed 18 June 2020.

[269] J Buolamwini, 'Response. Racial and Gender bias in Amazon Rekognition. Commercial AI System for Analyzing Faces' (*Medium*, 25 January 2019) <https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analysing-faces-a289222eeced> accessed 29 July 2020.

[270] Thorn, 'Microsoft's PhotoDNA: Leading the Fight Against Child Sexual Abuse Imagery' (*Thorn*, 25 April 2016) <www.thorn.org/blog/photodna-leads-fight-against-child-sex-abuse-imagery/> accessed 23 April 2020.

[271] J Langston, 'How PhotoDNA for Video is being used to fight online child exploitation' (*Microsoft*, 12 September 2018) <https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/> accessed 14 July 2020.

Figure 14. Photo DNA video solution. Source: J Langston, 'How PhotoDNA for Video is being used to fight online child exploitation' (Microsoft, 12 September 2018) <https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/> accessed 14 July 2020.



Regarding data privacy, because PhotoDNA instantly converts pictures and videos to secure hashes and the latter are never retained by Microsoft, the emergence of data privacy conflicts seems very unlikely. However, would it be the case, Microsoft appears to have a strong privacy policy which is applicable to all the products that the company is offering.[272]

PhotoDNA is used by the organisation Thorn to combat child sex abuse and trafficking. In addition to using the service, the NGO is currently developing an AI-led Child Finder Service and an 'anti-grooming technique' which will be able, with the help of machine learning, to scan text-based chats potentially responsible for grooming children, with the aim of allowing individual companies to monitor and report these activities to law enforcement.[273] However, the same concerns as the ones raised above apply and need to be further investigated, given the lack of information provided on the respective websites of the NGO and of technology companies regarding the protection of data.

Finally, it is worth highlighting that initiatives focusing on the use of AI to combat trafficking are also emerging from the research field. This is the case of the **Technology and Human Trafficking Initiative**. Launched by the USC Annenberg Center on Communication Leadership and Policy, the project has been working on the development of a 'prototype software' designed to detect possible cases of online sex trafficking activity, particularly cases involving underage victims.[274] On

[272] Microsoft, 'Privacy: It's All About You' <www.microsoft.com/en-us/trust-center/privacy> accessed 12 July 2020.

[273] C Canton Ferrer, 'Machine Learning Can Help Find Kids Faster' (*Thorn*, 18 May 2017) <www.thorn.org/blog/machine-learning-find-kids-faster/> accessed 18 June 2020.

[274] University of Southern California, 'Technology & Human Trafficking' <https://communicationleadership.usc.edu/projects/list/trafficking/> accessed 18 June 2020.

the other hand, the non-profit organisation Business Social Responsibility (BSR) established the collaboration **Tech Against Trafficking** which gathers technology companies such as Microsoft, Amazon, AT&T, and BT Group, along with global experts. Through biannual 'in person' meetings per year as well as bimonthly calls, the coalition aims to help eradicating THB by focusing on knowledge-sharing, research and technology solutions, including AI.[275]

The above-mentioned initiatives demonstrated the potential that big data and AI may have to combat human trafficking for sexual exploitation of women and children. Although they raise issues relating to the absence or quality of data, ethics, data privacy and security, they constitute helpful tools which need to be investigated further, as long as governments, technological actors, companies, lawyers and law enforcement officials work together and take into consideration these inherent challenges.

The following chapter will try to give hints on how this could be done.

[275] BSR, 'Tech Against Trafficking' <www.bsr.org/en/collaboration/groups/tech-against-trafficking> accessed 18 June 2020.

Table 6. Contemporary data analytics and AI initiatives fighting trafficking of human beings for sexual exploitation

Contemporary data analytics and AI initiatives fighting trafficking of human beings for sexual exploitation

Data analytics		Artificial intelligence	
Counter Trafficking Data Collaborative (CTBC)	Global datahub on human trafficking managed by ICT companies and NGOs (Polaris, IOM, Liberty Shared, Palantir Technologies), initially launched by the Global human trafficking hotline, an alliance between global data enterprises Palantir, Google, Salesforce, Polaris and NGOs La Strada International and Liberty Shared. The Network is also at the origin of : • An antitrafficking hotline • The Global Modern Slavery Directory	**Traffik analysis Hub (TaHub)**	Datahub visualisation platform managed by IBM machine learning , supported by other tech companies, NGOs, companies from the banking sector, law enforcement agencies and the academia, which provides insights about illicit trafficking operations
Minerva	Antitrafficking data analytics platform launched by the Global Emancipation Network, an alliance composed by experts in technologies and big data analytists (Microsoft, Recorded Future, Splunk, Accenture, Owl Cybersecurity, DeepVision, GitHub, Maltego, Chainanalysis and Neustar). The platform is using advertisement analysis, natural language processing, public records, open Web searches and image processing tools to uncover trafficking nets, free of charge for its users (law enforcement, NGOs, Academia...)	**Spotlight**	Web-based tool aiming to fight sexual exploitation of children powered by company Digital Reasoning machine learning and used by the NGO Thorn
Traceanobject	Opensource tool developped on Europol website to find children victims of sexual abuse and trafficking	**TrafficJam**	Initiative operated by the AI Company Marinus Analytics, mobilising analytical tools such as the software Amazon Recognition to identify trafficking traces online
StopApp	Mobile phone application designed by NGO Stopthetraffik, allowing anyone to declare a suspected trafficking case	**Microsoft Photo and Video DNA**	Hashing technology mobilising machine learning to recognize pictures of individuals from the Internet. The NGO Thorns uses it to track human trafficking offenders and children victims of sexual exploitation
		Techagainst Trafficking	Technology and global experts gathering to eradicate trafficking through knowledge sharing, research and technology through knowledge sharing, research and technology solutions such as AI

5.

IMPROVING THE REGULATION OF ICTS-FACILITATED SEXUAL EXPLOITATION

When examining the legal framework regulating human trafficking for sexual exploitation (Chapter I), it appears obvious that very few considerations have been made about the enormous impact that digital technologies, in particular the internet and mobile technologies, have on this crime (Chapter III). Regarding the internet in particular, the Inter-Agency Coordination Group Against Trafficking in Persons (ICAT) rightly summarised the issue at stake by stating that the legal framework 'does not provide the tools necessary to enable successful investigations and prosecutions to counter impunity online or use the entire array of tools to efficiently fight trafficking in persons in the online world'.[276] In addition to this gap in the general framework, it seems that the regulation does not associate AI and big data use to anti-trafficking efforts, focusing for the most part on data protection and privacy concerns and leaving those practices to law enforcement guidelines or other soft law materials (see Chapters I and II).

Yet, in order to address the transnational and ever-evolving nature of technology, it has become vital to identify and address these legal gaps and focus on the elimination of legal standards discrepancies.[277] In the opinion of the NGO Equality Now, one solution could be to elaborate an international framework and common standards to address online sexual exploitation in the form of a 'Global Compact'[278] or through an addition to the Palermo Protocol, signed by both governments and technological companies.[279] While these suggestions need to be carefully analysed from a legal perspective, they offer the advantage of highlighting the joint responsibility of the international community, technological companies and civil society to come up with a common regulation enshrining the responsibility and accountability of all actors involved in the combat against trafficking.

[276] Inter-Agency Coordination Group Against Trafficking in Persons (ICAT), 'Human Trafficking and Technology. Trends, Challenges and Opportunities' Issue Brief 7 (ICAT 2019) 2.

[277] Equality Now, 'Technology and Trafficking. The Need for a Stronger, Gendered and Cooperative Approach' (Equality Now 14 August 2019) <www.equalitynow.org/technology_and_trafficking_the_need_for_a_stronger_gendered_and _cooperative_response> accessed 18 June 2020.

[278] It has been done at the UN level through the development of principles and good practices applicable to companies in order to ensure that their business is conducted in a responsible and sustainable way; see United Nations Global Compact, 'Business as a Force for Good' <www.unglobalcompact.org/what-is-gc/mission> accessed 18 June 2020.

[279] Equality Now (n 277).

Another solution, proposed by author L-M Rhodes, would be to consider and regulate human trafficking, and therefore sexual exploitation, as a cybercrime.[280] This would, *inter alia*, accelerate the identification of perpetrators and preserve evidence.[281] Although there is no consensus on the notion of 'cybertrafficking', it cannot be denied that each of the cumulative elements of trafficking (action, means and purpose)[282] are so largely facilitated by computer networks that pure 'offline trafficking' has become the exception.[283] This state of fact also led authors V Greiman and C Bain to offer a definition of 'cybertrafficking' which combines notions enshrined in both the UN Palermo Protocol and the CoE Convention on Cybercrime, designating it as the 'transport of persons, by means of a computer system, Internet service, mobile device, local bulletin board service, or any device capable of electronic data storage or transmission to coerce, deceive, or consent for the purpose of exploitation'.[284]

However, given that the protection afforded to victims of human trafficking is more extensive than the one that the regulation on cybercrime is offering,[285] it might be better to consider drafting a new legal instrument taking account of the set of specificities of the two conventions all while ensuring a high level of victim protection, especially knowing the intrinsic vulnerability of women and children who have to endure this crime.

In addition, while the law undoubtedly needs to 'catch up' to problems caused by current technology,[286] it remains to be seen whether enforceable regulation of AI and big data is the right solution. According to the CoE experts on human rights dimensions of automated data processing and different forms of AI:

> this approach (…) may be ill-suited to such an innovative field and may compensate for lack of detail with overly restrictive or overly permissive provisions. Sectoral regulation may be preferable although, arguably, existing law and regulation, for example in the field of data protection, could be flexible and available without the need to legislate further.[287]

Therefore, knowing that the traditional legislative approach might be unfit, a careful balance should be made by the legislator when approaching the challenges raised by the regulation of technologies. This is where soft law instruments prove to have precious value. Indeed, although they are inherently 'imperfect' due to their unenforceable nature, private standards, guidelines, best practices, principles, code of conducts and certification programs may be more suited to 'cope with the rapid pace, diverse applications, heterogeneous risks and concerns, and inherent uncertainties of emerging technologies'.[288] What is more, they

[280] L-M Rhodes, 'Trafficking as Cybercrime' (2017) 1 AGORA International Journal of Administration Sciences 23.

[281] A-P Sykiotou, 'Cyber Trafficking. Recruiting Victims of Human Trafficking through the Net' in C-D Spinellis, N Theodorakis, B. Emmanouil, and G. Papadimitrakopoulos, *Essays in Honour of Nestor Courakis* (Ant N Sakkoulas Publications LP 2017) 1547.

[282] In the meaning of the Palermo Protocol's definition enshrined in art 3; see ch I.

[283] N Frei, 'On "Cyber Trafficking" and the Protection of its Victims' (*Völkerrechtsblog*, 26 July 2017) <https://voelkerrechtsblog.org/on-cyber-trafficking-and-the-protection-of-its-victims/, accessed 19 June 2020.

[284] V Greiman and C Bain, 'The Emergence of Cyber Activity as a Gateway to Human Trafficking', (2013), 12(2) International Journal of Cyber Warfare and Terrorism 5, 10.

[285] See, for instance, art 6 of the Palermo Protocol which offers a wide range of means to protect and assist victims of trafficking, including on privacy matters, as mentioned in ch IV.

[286] C Campbell, 'Web of Lives. How Regulating the Dark Web Can Combat Online Human Trafficking' 38 J Nat'l Ass'n Admin L Judiciary 136, 181.

[287] Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, 'Draft Recommendation of the Committee of Ministers to member states on human rights impacts of algorithmics systems' (12 November 2018)) 16.

[288] G Marchant, '"Soft Law" Governance of Artificial Intelligence' (*AI Pulse*, 25 January 2019) <https://aipulse.org/soft-law-governance-of-artificial-intelligence/> accessed 12 July 2020.

can be adopted and revised quickly, without having to go through the whole governmental legislative process, all while sometimes creating a more cooperative relationship between stakeholders.[289]

While this is true, it remains important to highlight the insufficient character of mobilising the legislative path alone whether brought through 'hard' or 'soft' instruments. Indeed, although the previous chapter referred to some initiatives launched by actors joining forces to combat sexual exploitation, issues relating to weak cooperation between the different anti-trafficking players are still numerous. The importance of law enforcement cooperation through partnerships between the public and the private sector must be emphasised and should probably be addressed in the legislation itself. Technology companies do indeed seem to be uniquely positioned in this fight. It has even been contended that the cultivation of sociotechnical solutions is one of the most efficient ways to respond to the trafficking cause.[290] In this regard, the priority must be to ensure the firm rooting of technological inventions within front line responders' daily practices, rather than 'making them an additional step that law enforcement officials must take in their already busy work schedules'.[291]

The previous chapters have emphasised the huge part played by social networks in trafficking rings. They have also demonstrated that the latter can in turn be used by law enforcement officials, by tracking traffickers and victims' digital footprint in cyberspace. To this end, it has become urgent to obtain up-to-date knowledge and to train officials on how to use social media sites as a form of intelligence in the fight against THB, in order to increase their capacity to monitor and track the role of these sites in sexual exploitation.[292] Due to the fast pace of ICTs evolution, the lack of capacity, awareness and expertise of these actors, along with prosecutors and the judiciary, remains a central issue which should urgently be addressed in regulation, practices and policies.[293]

It is worth noting in this regard that 'hackathons' gathering big tech companies and engineers from all over the world involved in societal issues, including the trafficking cause, are frequently organised, as they seem to constitute a good way to spread awareness all while emphasising the necessity to strengthen cooperation in the field. As way of illustration, Google, Microsoft, Amazon, Twitter, Pinterest, Intel and Facebook, among others, gather every year during the Child Safety Hackathon, a 48-hour collaborative event organised to propose solutions to sexual exploitation and child abuse.[294]

While the organisation of such events highlights their important potential, sociotechnical tools have, as for each technological innovation, to be approached

[289] Marchant (n 288).

[290] Slavery Footprint, 'Made in a Free World. How many slaves work for you?' <http://slaveryfootprint.org> accessed 24 April 2020.

[291] H Thinyane, 'How Can Human Trafficking Frontline Responders Use Technology?' (*Thomson Reuters Foundation News*, 30 May 2017) <https://news.trust.org/item/20170530133713-c7ik0/> accessed 23 April 2020.

[292] J-L Mustol and D Boyd, 'The Trafficking-Technology Nexus' (2014) 21(3) Social Politics 461, 471.

[293] ICAT (N 276) 2.

[294] Thorn, 'Child Safety Hackathon Brings Silicon Valley Together' (*Thorn*, 12 May 2016) <www.thorn.org/blog/child-safety-hackathon/> accessed 20 June 2020.

with scrutiny. In addition to the underlying market-based values running in their background, partnerships between public and private actors can be said to be built around an 'injunction to cooperation', forcing actors with very diverging objectives depending on the professional belonging to collaborate on the issue of trafficking.[295] Therefore, ethical obstacles and human rights challenges are unavoidable, and the impact and effects of these initiatives should be carefully studied.

A specific area of concern in this regard is undoubtedly the one related to the issue of the availability, reliability and safety of data. It is not a surprise, due to the fact that quantitative and qualitative information on trafficking in persons is scarce, unreliable and non-comparable, that the emphasis has currently been put on controlling the crime by 'reducing the legal and illegal opportunities for criminal activities'.[296] So long as data is unavailable or unreliable, counterstrategies, whether oriented regionally or internationally, will remain a strenuous task.

Moreover, even if information is available, additional challenges are brought by privacy and data protection concerns. As the previous sections demonstrated, initiatives stemming from the private sector are widely mobilising data, regardless of when simple data analytics or AI technologies are used. Companies tend to adopt regulations that allow them to comply with the legislative framework governing data, such as the GDPR at the EU level. However, this is not systematic, and it is sometimes necessary to go beyond the initiative's website and access the page of the tech partners responsible for the creation of the specific technology to look for this information. Therefore, while it is very difficult to verify the exactitude of data or even if companies fulfil their legal obligations *de facto*, these considerations should be at the centre of regulation and law enforcement debates.

Alongside with data-related issues, the other main area of concern is the necessity to integrate a gender perspective in all anti-trafficking actions. As demonstrated above, trafficking and sexual exploitation are 'highly gendered systems that result from structural inequality between men and women and children on a world scale'.[297] In addition, women and girls have always been trafficked and treated by the criminal justice system in ways that are very gender specific. Alongside with this treatment, digital technologies themselves, and particularly the internet, are often said to both empower and objectify women. Specifically, as they constitute forums for influencing culture, they have brought along a significant extension of the acceptance of violence all while normalising practices that were previously said to be unacceptable.[298] As highlighted above, the internet and mobile technology are providing a more fluid environment and can be said to constitute, 'disruptive enablers of the commoditization of human beings'.[299] On the other

[295] B Lavaud-Legendre, 'Approche Globale et Traite des Etres Humains, de l' "Injonction à la Coopération" au Travail Ensemble ' Rapport de recherche (CNRS 2018) 7.

[296] K Aromaa, 'Trafficking in Human Beings. Uniform Definitions for Better Measuring and for Effective Countermeasures' in E Savona and S Stefanizzi, *Measuring Human Trafficking. Complexities and Pitfalls* (ISPAC, Springer 2007) 24.

[297] D-M Hughes, *Trafficking in Human Beings in the European Union. Gender, Sexual Exploitation, and Digital Communication Technologies* (Sage Open 2014) 20.

[298] K Maltzahn, 'Digital Dangers. Information and Communication Technologies and Trafficking in Women' (APC Issue Papers 2006) 7.

[299] M van Reisen and others, 'Tracing the emergence of ICT-enabled human trafficking for ransom' in R Piotrowicz, C Rijken and B Heide Uhl (eds), *Handbook of Human Trafficking* (Routledge 2018) 151.

hand, technological tools used to combat THB often do discriminate; algorithms, for instance, because they are written by humans, are inherently biased. In any case, knowing the capacity of technology in general to normalise human rights violations, special attention should be drawn on the cultural dimension of the ICT tools mobilised for anti-trafficking actions.

CONCLUSION

Human trafficking and digital technologies, in particular the internet and mobile technologies, have in fact been fairly newly regulated by the law at the regional and international levels. This thesis foremost highlighted the lack of a legislative framework covering the two dimensions altogether despite their strong link. Alongside this ICTs-sexual exploitation nexus, it emphasised the absence of regulations covering the use of data science and AI techniques outside of the framework of privacy and data protection.

Above all, this work pointed out the benefits derived from the use of digital tools by both trafficking networks and law enforcement officials. On the one hand, it summarised the broad range of technological tools that the surface web, the deep web and mobile technologies provide to perpetrators of sexual exploitation to recruit, advertise and exercise control over victims. In the same vein, it highlighted the importance of the underlying gender dimension of cybersex-trafficking and ICT tools, as well as the role of social media, advertisements, the pornographic industry, dark web forums and mobile phones in the perpetuation and normalisation of negative gender attitudes, digital tools being often considered a nexus of victimisation of women and children.

On the other side of the trafficking net, this research tried to demonstrate that the technological visibility of cybersex-trafficking can in turn be mobilised by antitrafficking agents through data analytics and AI methods established by partnerships between the public and private sector. While it emphasised the importance for further study of the potential of these initiatives, it also highlighted a certain number of practical, ethical and security hurdles, mostly stemming from the competitive context in which these socio-technological tools are created and deployed.

In particular, it acknowledged the fact that data science and AI techniques are morphing and redefining the surveillance context in which they evolve, and therefore underlined the ensuing necessity to operate a balance between data privacy concerns and the human rights violations that many women and children are facing in this context. Finally, it raised the concern that anti-trafficking actors mobilising these techniques, who sometimes have very different and even conflicting interests, also have to confront to the biases emerging from the underlying cultural dimension of digital tools and the highly gendered dimension of sexual exploitation.

Although this thesis proposed some food for thought to support the quest of regulating cybersex trafficking and the use of data science and AI tools, it established that fighting sexual exploitation cannot be done solely on a legal or technical basis. In essence, it insisted on the necessity of providing interdisciplinary solutions aiming to fight the sexual exploitation of women and children, on the one hand, and on the importance to focus on the intersection of governmental cooperation, social engineering and technology all while including a gender and children sensitive approach, on the other.

Nevertheless, beyond the potential of the analysed ICT tools and should the said interdisciplinarity and gender-sensitive approaches be ensured, it is worth a reminder that human beings remain involved in the cybersex trafficking industry for one reason: the profitability of sexual exploitation. By contrast, implementation and resources remain the most important weakness in anti-trafficking efforts. Therefore, in the words of J-L Mustol, 'as technologies grow more sophisticated so too will the possibilities for staging innovative sociotechnical interventions. Yet, capitalizing on this knowledge requires far more low-tech solutions; specifically, political will and agitation for redistributive justice, the hardest assets to find'.[300]

One may in this sense wonder, beyond law enforcement tactics mobilising cutting edge technology and should the above-mentioned challenges be overcome at the level of prosecution, if addressing the demand side of sexual exploitation should not be, in our globalised and 'technologised' modern society, the first priority.

[300] J-L Mustol and D Boyd, 'The Trafficking-Technology Nexus' (2014) 21(3) Social Politics 461, 477.

BIBLIOGRAPHY

Books and articles

Alexiadis P and Cole M, 'The Application of the Concept of Technology Neutrality Under the New ECNS Regulatory Framework' (2004) ECTA Review

Aronowitz A and Koning A, 'Understanding Human Trafficking as a Market System. Addressing the Demand Side of Trafficking for Sexual Exploitation' [2014] 85(3) Revue internationale de droit penal 669

Aromaa K, 'Trafficking in Human Beings. Uniform Definitions for Better Measuring and for Effective Countermeasures' in Savona E and Stefanizzi S, *Measuring Human Trafficking. Complexities and Pitfalls* (ISPAC, Springer 2007)

Bernstein E, 'Militarized Humanitarianism Meets Carceral Feminism. The Politics of Sex, Rights, and Freedom in Contemporary Anti-trafficking Campaigns (2010) 36 Signs 45

Boyd D and others, 'Human Trafficking and Technology. A Framework for Understanding the Role of Technology in the Commercial Sexual Exploitation of Children in the U.S.' (Microsoft Research Connection 2011)

Burri T, 'International Law and Artificial Intelligence' [2017] German Yearbook of International Law 91

Brunner J, 'Getting to Good Human Trafficking Data. Everyday Guidelines for Frontline Practitioners in Southeast Asia' (WSD Handa Center for Human Rights and International Justice of Stanford University, East-West Center and Human Rights Resource Centre 2018)

Campbell C, 'Web of Lives. How Regulating the Dark Web Can Combat Online Human Trafficking' 38 J Nat'l Ass'n Admin L Judiciary 136

Carey J, 'Communication as Culture' in *Essays on Media and Society* (Routledge 2008)

Casanovas P and others, 'Regulation of Big Data. Perspectives on strategy, policy, law and privacy' (2017) 7 Health Technol 335

Castells M and others, *Mobile Communication and Society. A Global Perspective* (Cambridge MIT Press 2009)

Chawki M and Wahab M, 'Technology Is a Double-Edged Sword: Illegal Human Trafficking in the Information Age' [2004] Droit-TIC 22

Cook A, 'A Non-Traditional Security Threat in Asia. Cyberspace and Human Trafficking?' in Rueppel P and Hofmeister W, *Trafficking in Human Beings Learning from Asian and European Experiences* (East Asian Institute, European Policy Centre and European Union Centre in Singapore, Konrad-Adenauer Stiftung, 2014) 97

Dettmeijer-Vermeulen C, 'Trafficking in Human Beings. Ten Years of Independent Monitoring by the Dutch Rapporteur on Trafficking in Human Beings' (2012) 18 European Journal on Criminal Policy and Research 283

Desouza K and Smith K, 'Big Data for Social Innovation' [2014] Stanford Social Innovation Review 39

Dubrawski A and others, 'Leveraging Data to Discern Human Trafficking Pattern' [2015] Journal of Human Trafficking 65
Farrell A and Kane B, 'Criminal Justice System Responses to Human Trafficking in Winterdyk J and Jones J, *The Palgrave International Handbook of Human Trafficking*, (Palgrave MacMillan 2020) 1
Finn R, Wright D and Friedewald M, 'Seven Types of Privacy' in Gutwirth S, Leenes R and De Hert P (eds), *European Data Protection. Coming of Age* (Springer 2013)
L. Floridi, J. Cowls, M. Beltrametti, R. Chatila, P.Chazerand, V. Dignum, C. Luetge, R. Madelin, U. Pagallo,· F. Rossi, B. Schafer, P. Valcke, and E. Vayena, 'The AI4People's Ethical Framework for a Good AI Society' (2018), 28 Minds and Machine, 689
Friesendorf C, 'Strategies Against Human Trafficking. The Role of the Security Sector', Study Group Information (National Defence Academy and Austrian Ministry of Defence and Sports 2009)
Gallagher A, 'Human Rights and Human Trafficking. A Reflection on the Influence and Evolution of the U.S. Trafficking in Persons Reports' in Brysk A and Choi-Fitzpatrick A (eds), *From Human Trafficking to Human Rights. Reframing Contemporary Slavery* (University of Pennsylvania Press 2011)
— and Holmes P, 'Developing an Effective Criminal Justice Response to Human Trafficking. Lessons from the Front Line' (2008) 18(3) International Criminal Justice Review, 318
Gallagher A-T, 'Trafficking in Transnational Criminal Law' in Piotrowicz R, Rijken C and Heide Uhl B (eds), *Routledge Handbook of Human Trafficking* (Routledge International Handbooks 2017)
Gerry F, Muraszkiewicz J and Vavoula N, 'The Role of Technology in the Fight Against Human Trafficking. Reflections on Privacy and Data Protection Concerns' (2016) 32 Computer Law & Security Review 205
Greiman V and Bain C, 'The Emergence of Cyber Activity as a Gateway to Human Trafficking' 12(2) International Journal of Cyber Warfare and Terrorism 41
Gulia H and P, 'Big Data Analytics' (February 2016) 4(2) Research Journal of Computer and Information Technology Sciences 1
Hancilova B and Massey C, 'Legislation and the Situation Concerning Trafficking in Human Beings for the Purpose of Sexual Exploitation in EU Member States' (International Centre for Migration Policy Development 2009)
Heide Uhl B, 'Assumptions Built into Code. Datafication, Human Trafficking, and Human Rights. A Troubled Relationship?' in Piotrowicz R, Rijken C and Heide Uhl B (eds), *Routledge Handbook of Human Trafficking* (Routledge International Handbooks 2017)
Herbert B and Dixon J, 'Human Trafficking and the Internet (and Other Technologies, Too)' (2013) 52(1) The Judges' Journal, 46
Hughes D-M, 'The Impact of the Use of New Communications and Information Technologies on Trafficking in Human Beings for Sexual Exploitation', Report for the Committee for the Equality between Women and Men (Council of Europe 2001)
— 'Role of Marriage Agencies in Trafficking in Women and Trafficking in Images of Sexual Exploitation', The Group of Specialists on the Impact of the Use of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation (EG-S-NT) (Committee for Equality between Women and Men (CDEG), Council of Europe 2001)
— 'Prostitution Online' (2003) 2(3) Journal of Trauma Practice 115
— 'The Impact of New Information Technologies on Trafficking in Human Beings for the Purpose of Sexual Exploitation', Misuse of the Internet for the Recruitment of Victims of Trafficking in Human Beings, Council of Europe campaign to combat trafficking in human beings (Seminar proceedings, Strasbourg, 7-8 June 2007)
— *Trafficking in Human Beings in the European Union. Gender, Sexual Exploitation, and Digital Communication Technologies* (Sage Open 2014)

Fedorschak K and others, 'Data Collection and Human Trafficking' in Chiarini Tremblay M and others (eds), *Advancing the Impact of Design Science. Moving from Theory to Practice* (Springer 2014)
Hua J and Nigorizawa H, 'US Sex Trafficking, Women's Human Rights and the Politics of Representation' International Feminist Journal of Politics 412
Kinsella N and Rankin G, 'Human Trafficking - The Importance of Knowledge Information Exchange' in Akhgar B and Yates S, *Intelligence Management* (Springer 2011)
Kranzberg M, 'Technology and History. "Kranzberg's Laws"' (July 1986) 27(3) Technology and Culture 544
Latonero M, 'Human Trafficking Online. The Role of Social Networking Sites and Online Classifieds' (University of Southern California, Center on Communication Leadership and Policy, 2011)
— 'The Rise of Mobile and the Diffusion of Technology-Facilitated Trafficking', Research Series on Technology and Human Trafficking (Center on Communication Leadership and Policy, University of Southern California 2012)
Lavaud-Legendre B, 'Approche Globale et Traite des Etres Humains, de l'"Injonction à la Coopération"au Travail Ensemble' Rapport de recherche (CNRS 2018)
Leary M, 'Fighting Fire with Fire. Technology in Child Sex Trafficking' (2014) 21 Duke Journal of Gender Law and Policy 289
Maltzahn K, 'Digital Dangers. Information and Communication Technologies and Trafficking in Women' (APC Issue Papers 2006)
Manheim K and Kaplan L, 'Artificial Intelligence. Risks to Privacy and Democracy' (2019) 21 The Yale Journal of Law & Technology 106
Milivojevic S and Segrave M, 'Tracing the emergence of ICT-enabled human trafficking for ransom' [2017] Gender, Technology and Violence (Routledge Studies in Crime and Society) 28
Muraszkiewicz J, 'Alternative ways to address Human Trafficking: Technology and Human Trafficking' in Carrera S and Guild E (eds), *Irregular Migration, Trafficking and Smuggling of Human Beings Policy Dilemmas in the EU* (Centre for European Policy Studies 2016) 74
— 'Crowd Knowledge Sourcing. A Potential Methodology to Uncover Victims of Human Trafficking' in G Leventakis and MR Haberfeld (eds), *Societal Implications of Community-Oriented Policing and Technology* (Springer 2018) 23
Mustol J-L and Boyd D, 'The Trafficking-Technology Nexus (2014) 21(3) Social Politics 461
Pearsall B, 'Predictive Policing: The Future of Law Enforcement ?, Law Enforcement Explore Ways to Anticipe and Prevent Crime', 266 NJ Journal 16
Pérez Cepeda A and Benito Sánchez D, *Trafficking in Human Beings, A Comparative Study of the International Legal Documents* (Europa Law Publishing 2014)
Piotrowicz R, Rijken C and Heide Uhl B (eds), *Routledge Handbook of Human Trafficking* (Routledge International Handbooks 2017)
Piotrowicz R and Sorrentino L, 'The Non- Punishment Provision with Regard to Victims of Trafficking. A Human Rights Approach' in Piotrowicz R, Rijken C and Heide Uhl B (eds), *Routledge Handbook of Human Trafficking* (Routledge International Handbooks 2017) 174
Portnoff R and others, 'Backpage and Bitcoin. Uncovering Human Traffickers' 23rd ACM SIGKDD International Conference (2017)
Provost F and Fawcett T, 'Data Science and its Relationship to Big Data and Data-Driven Decision Making' (13 February 2013) 1(1) Big Data 51
van Reisen M and others, 'Tracing the emergence of ICT-enabled human trafficking for ransom' in *Handbook of Human Trafficking* (Routledge 2018)
Rhodes L-M, 'Trafficking as Cybercrime' (2017) 1 AGORA International Journal of Administration Sciences 23

Roth V, 'Defining Human Trafficking and Identifying Its Victims: A Study on the Impact and Future Challenges of International, European and Finnish Legal Responses to Prostitution-Related Trafficking in Human Beings' (2011) 24(3) International Journal of Refugee Law 657-660
Ruchti L-C, 'Fear, Fraud and Frank Complexities, The Influence of Gender on Human Trafficking' in Burke M-C, *Human Trafficking: Interdisciplinary Perspectives* (Routledge, Taylor and Francis 2013) 88
Ruiz F, 'Trends in the Area of Child Sexual Exploitation' (European Cybercrime Centre, Europol 2016)
Sabo T, 'An Artificial Intelligence Framework on SAS® Viya® to Counter International Human Trafficking' (Paper 3071, SAS Institute Inc 2019)
Savona E and Stefanizzi S, *Measuring Human Trafficking. Complexities and Pitfalls* (ISPAC, Springer 2007)
Savirimuthu J, *Online Child Safety. Law, Technology and Governance* (Palgrave MacMillan 2019)
Sen A, 'More Than 100 Million Women Are Missing' (20 December 1990) 37(20) New York Review of Books
Sykiotou A-P, 'Cyber Trafficking. Recruiting Victims of Human Trafficking Through the Net', in Spinellis C-D, Theodorakis N, Emmanouil,B and Papadimitrakopoulos G, *Essays in Honour of Nestor Courakis* (Ant N Sakkoulas Publications LP 2017) 1547-1587
Schwartz A, *Stopping Spam* (O'Reilly 1998)
Taddeo M and Floridi L, 'How AI can be a force for good' (2018) 361(6404) Science 751
Tidwell R, 'Caught in the Web: The Importance of Ethical Computing Illustrated via an Exploration of the Online Recruitment of Women and Girls into Sex Trafficking' (Western Oregon University, Honors Senior Theses/Projects 2016)
Van der Slote B and Van Schendel S, 'International and Comparative Legal Study on Big Data' (The Netherlands Scientific Council for Government Policy Working Paper 2016)
Vaz Cabral G, *La Traite des Êtres Humains. Réalités de l'Esclavage Contemporain* (La Découverte 2006)
Verham Z, 'The Invisibility of Digital Sex Trafficking in Public Media' (2015), 8(3) Intersect 3, 4.
Wheaton E, Schauer E and Galli T, 'Economics of human trafficking' (2010) 48(4) International Migration 114.
Winterdyk J and Jones J, *The Palgrave International Handbook of Human Trafficking* (Palgrave MacMillan 2020)
Youssra R, 'Big Data and Big Data Analytics. Concepts, Types and Technologies' (2018) 5(9) International Journal of Research and Engineering 524

Official documents

A. Legislation

1. UN

Convention on Prohibitions or Restrictions on the Use of Certain Conventional Weapons which may be Deemed to be Excessively Injurious or to have Discriminated Effects (adopted 10 October 1980, entered into force 2 December 1983), 1342 UNTS 137.
Convention on the Elimination of All Forms of Discrimination against Women, (adopted 18 December 1979, entered into force 3 September 1979) 1249 UNTS 13 (CEDAW)
International Covenant on Civil and Political Rights (adopted 16 December 1966, entered into force 23 March 1976) 999 UNTS 171 (ICCPR), arts 2, 3, 6, 7, 8, 9, 17 and 19

Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography (adopted 25 May 2000, entered into force 18 January 2002), 2171 UNTS 227
Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (adopted 15 November 2000, entered in to force 25 December 2003) 2237 UNTS 319 (Palermo Protocol)

2. Council of Europe

Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, as it will be amended by its Protocol CETS No 223 (not in force), STE 108
Convention on Action against Trafficking in Human Beings, CETS 197
Convention on Cybercrime, STE 185
Convention on Preventing and Combating Violence against Women and Domestic Violence, CETS 2010 (Istanbul Convention), art 25
Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, CETS 201 (Lanzarote Convention)
Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR) arts 2, 3, 4, 5, 8, 9, 10 and 14
Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS 223

3. European Union

Charter of Fundamental Rights of the European Union arts 7 and 8
Council Framework Decision 2008/977/JHA of 27 November 2008 on the Protection of Personal Data processed in the framework of police and judicial cooperation in criminal matters [2008] OJ L 350
Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281
Directive 2011/36/EU of the European Parliament and of the Council of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims and replacing Council Framework Decision 2002/629/JHA [2011] *OJ L 101*
Directive 2011/92/EU of the European Parliament and the Council of 13 December 2011. on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA [2012] OJ L 26
Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime (Victim Directive) [2012] OJ L 315/57
Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119

4. Others

African Charter on the Rights and Welfare of the Child (adopted 1 July 1990, entered into force 29 November 1999) art 27
Arab Charter on Human Rights (published in May 2004) art 10
Arab Convention on Combating Information Technology Offences (published 21 December 2010) arts 12, 14 and 16
Association of South East Asian Nations (ASEAN), Convention Against Trafficking in Persons, Especially Women and Children (Published 22 November 2015)

European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment (adopted at the 31st plenary meeting of the CEPEJ, Strasbourg, 3-4 December 2018)
Organization of American States Inter-American Convention on International Traffic in Minors (adopted 18 March 1994, entered into force 15 August 1997)
South Asian Association for Regional Cooperation, Convention on Preventing and Combating Trafficking in Women and Children for Prostitution (adopted 5 January 2002, entered into force 15 November 2005)

B. Soft Law

1. UN Resolutions and Reports

UNGA Res 64/293 (30 July 2010) 'United Nations Global Plan of Action to Combat Trafficking in Persons' UN Doc A/64/293
UNGA Res 71/199 (19 December 2017) on the right to privacy in the digital age, UN Doc A/71/199
UNGA 'Report of the Secretary General, Sale and sexual exploitation of children, including child prostitution, child pornography and other child sexual abuse material; and trafficking in persons, especially women and children', UN Doc A/72/164 (2017).
UNGA 'Report of the United Nations High Commissioner for Human Rights on the promotion, protection, and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective', UN Doc A/HCR/35/9 (2017)
UNGA Res 72/200 (20 December 2017) on information and communication technologies for sustainable development UN Doc A/72/200
UNGA 'Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression' UN Doc A/HRC/3/348 (2018)
UNGA Res 72/195 (19 December 2018) on improving the coordination of efforts against trafficking in persons UN Doc A/2/195
UNGA Res 73/146 (18 January 2019) on trafficking of women and girls UN Doc A/73/146
UNGA 'Report on privacy and technology from a gender perspective', UN Doc A/HRC/40/63 (2019)

2. Other UN instruments

Committee on the Right of the Child, General comment No. 25 (2021) on children's rights in relation to the digital environment (2 March 2021)
Guiding Principles for Business and Human Rights, Implementing the United Nations 'Protect, Respect and Remedy' Framework (2011)
Resolutions of the Commission on Crime Prevention and Criminal Justice (CCPCJ): eg 27.2, 27.3
Sustainable Development Goals 5: Gender Equality, 8: Decent Work and Economic Growth, and 16: Peace, Justice and Strong Institutions
United Nations Inter-Agency Project on Human Trafficking, *Guide to Ethics and Human Rights in Counter-Trafficking Ethical Standards for Counter-Trafficking Research and Programming* (2008)
UN Recommended Principles and Guidelines on Human Rights and Trafficking. Report of the United Nations High Commissioner for Human Rights to the Economic and Social Council (20 May 2002)
UN Guidelines Concerning Computerized Personal Data Files (1990)
UN Human Rights Committee (HRC), CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation (8 April 1988)

3. Council of Europe

General reports of the Group of Experts on Action against Trafficking in Human Being (GRETA)
Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, Draft Declaration of the Committee of Ministers on the manipulative capabilities of algorithmic processes (16 November 2018)
Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, 'Draft Recommendation of the Committee of Ministers to member states on human rights impacts of algorithmics systems' (12 November 2018)
Committee of experts on human rights dimensions of automated data processing and different forms of artificial intelligence, 'Study of the implications of advanced digital technologies (including AI) for the concept of responsibility within a human rights framework' (9 November 2018)

4. European Union

Guidelines 1/2019 on Codes of Conduct and Monitoring Bodies under Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119
Proposal for a Regulation of the European Parliament and of the Council, of 10 January 2017 concerning the respect for private life and the protection of personal data in electronic communications
Anti-Trafficking Data Collection and Information Management in the European Union, A Handbook (10 November 2009)
Declaration on Artificial Intelligence (10 April 2018)
European Parliament's Resolution on Civil Law Rules on Robotics (16 February 2017)
EU Declaration of Cooperation on Artificial Intelligence, Digital Day (10 April 2018)
EU Strategy towards the Eradication of Trafficking in Human Beings 2012-2016
First report (2016) and second report (2018) from the Commission to the European Parliament and the Council on the progress made in the fight against trafficking in human beings (2016)) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims
High-Level Expert Group on Artificial Intelligence set up by the European Commission, 'Ethics Guidelines for Trustworthy AI' (Brussels, 8 April 2019)
Recommendation of the Commission on measures to effectively tackle illegal content online (1 March 2018)

5. Other

Asia-Pacific Economic Cooperation Privacy Framework (December 2015), (APEC).
ASEAN, Declaration Against Trafficking in Persons, Particularly Women and Children (29 November 2004)
ASEAN, Framework on Personal Data Protection (16 November 2016)
CISPE Cloud, 'Data Protection. Code of Conduct for Cloud Infrastructure Service Providers' (27 January 2017) <https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf> accessed 18 June 2020
David F, *ASEAN and Trafficking in Persons. Using Data as a Tool to Combat Trafficking in Persons* (IOM 2007)

IBM, 'Principles for Trust and Transparency' <www.ibm.com/ibm/responsibility/2017/assets/downloads/IBM-2017-CRR-Principles.pdf> accessed 15 June 2020
League of Arab States, Model Law on Combating Offences related to Information Technology Systems (2004)
OAS, Proposed Statement of Principles for Privacy and Personal Data Protection in the Americas, adopted 17 October 2011 pursuant to Resolution AG/RES. 2514 (XXXIX-O/09)
OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980, amended on 11 July 2013)
OECD Principles on Artificial Intelligence, Recommendation of the Council on Artificial Intelligence (22 May 2019)
OECD Recommendation of the Council on Artificial Intelligence OECD/LEGAL/0449 (adopted 22 May 2019) <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449> accessed 29 April 2020
Organization for Security and Cooperation in Europe (OSCE), Plan of Action to fight Human Trafficking, Decision 557 (24 July 2003)
Privacy Shield Frameworks (EU-US and Swiss-US)
Toronto Declaration, Protecting the right to equality and non-discrimination in machine learning systems (May 2018) <www.torontodeclaration.org/> accessed 5 June 2020
United Nations Education, Science and Culture Organization, World Commission on the Ethics of Scientific Knowledge and Technology (COMEST)
C. Reports, guides and studies
Equality Now, 'Technology and Trafficking. The Need for a Stronger, Gendered and Cooperative Approach' (Equality Now 2019) <www.equalitynow.org/technology_and_trafficking_the_need_for_a_stronger_gendered_and_cooperative_response> accessed 11 July 2020
European Institute for Gender Equality (EIGE), *Gender-specific measures in anti-trafficking actions: report* (EIGE 2018)
European Parliament, Directorate General for Internal Policies, Policy Department C, Citizens' Rights and Constitutional Affairs, 'Sexual Exploitation and Prostitution and its Impact on Gender Equality' (2014)
Europol, *Serious and Organised Threat Assessment, Crime in the age of technology* (Europol 2017)
— 'Criminal Networks Involved in the Trafficking and Exploitation of Underage Victims in the EU' (European Union Agency for Law Enforcement Cooperation 2018) 7 <www.Europol.europa.eu/publications-documents/criminal-networks-involved-in-trafficking-and-exploitation-of-underage-victims- in-eu/> accessed 11 May 2020
ICMEC, 'Online Grooming of Children for Sexual Purposes: Model Legislation and Global Review' (1st edn, ICMEC 2017) <www.icmec.org/wp-content/uploads/2017/09/Online-Grooming-ofChildren_FINAL_9-18-17.pdf> accessed 6 May 2020
Independent high-level expert group on AI set up by the European Commission, A Definition of AI. Main Capabilities and Disciplines, Definition Developed for the Purpose of the AI HLEG's deliverables (European Commission 2019)
Inter-Agency Coordination Group Against Trafficking in Persons (ICAT), 'Human Trafficking and Technology. Trends, Challenges and Opportunities' Issue Brief 7 (ICAT 2019)
Myria, 'Tightening the Links. 2015 Annual Report of Trafficking and Smuggling of Human Beings' (Myria 2016)
— 'Trafficking and Smuggling of Human Beings Online, 2017 Annual Report' (Myria 2018)
— 'Combating social fraud to prevent trafficking in human beings, 2010 Annual Report on Human Trafficking and Smuggling' (Myria 2011)
National Association of State Mental Health Program Directors, 'Technology and Human Trafficking' (Assessment #3 2016)

Ohchr, 'Human Rights and Human Trafficking', Fact Sheet No 36 (United Nations 2014)
— 'Recommended Principles and Guidelines on Human Rights and Human Trafficking. Commentary' (United Nations 2010)
Plan International, 'Children sex trade at the digital age. A Study on the Commercial Sexual Exploitation of Children in Metro Manila' (The Girls Advocacy Alliance 2017)
Stop the Traffik. 'Human Trafficking and the Darknet. Insights on Supply and Demand' (Centre for Intelligence Led Prevention 2018)
Surf and Sound, *Improving and sharing knowledge on the Internet role in the processes of human trafficking and smuggling* (UK National Report 2017)
Thorn in collaboration with Bouché V, 'A Report on the Use of Technology to Recruit, Groom and Sell Domestic Minor Sex Trafficking Victims' (Thorn 2015)
Trace Project Consortium, 'Tracing Human Trafficking, Handbook for Policymakers, Law Enforcement Agencies and Civil Society Organizations' (Trace 2016)
UNODC, *Toolkit to Combat Trafficking of Persons, Global Programme against Trafficking in Human Beings* (United Nations Publications 2008)
— *Global Report on Trafficking in Persons* 2009 (United Nations Publications 2009)
— 'Comprehensive Study on Cybercrime, Draft' (United Nations Publications 2013)
— *Global Report on Trafficking in Persons 2018* (United Nations Publications 2018)
— 'Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children' (United Nations Publications 2015)
— and UN.GIFT, 'An Introduction to Human Trafficking. Vulnerability, Impact and Action' (Background paper 2008)
WePROTECT Global Alliance, 'Working together to end the sexual exploitation of children online' (UN.GIFT Global Threat Assessment 2018)
World Bank Group, *World Development Report 2016. Digital Dividends* (International Bank for Reconstruction and Development / The World Bank 2016)

Internet sources

Addepto, 'Using Artificial Intelligence (AI) for Image Recognition' (15 July 2019) <https://addepto.com/using-artificial-intelligence-ai-for-image-recognition/> accessed 17 June 2020
Allen C, 'The Role of the Internet on Sex Trafficking' (*International Observatory Human Rights*, 7 March 2019) <https://observatoryihr.org/blog/the-role-of-the-internet-on-sex-trafficking/> accessed 4 April 2020
Ambassade de France en Bulgarie, 'De l'utilisation frauduleuse d'Internet pour favoriser l'exploitation des personnes… quelles réponses apportées par le secteur public et le secteur privé?' (2018) <https://bg.ambafrance.org/De-l-utilisation-frauduleuse-d-Internet-pour-favoriser-l-exploitation-des> accessed 5 May 2020
Amnesty International España, 'Discriminación y violencia contra las mujeres en los videojuegos más populares de estas navidades' (*Amnistía Internacional*, 29 December 2004) <www.es.amnesty.org/en-que-estamos/noticias/noticia/articulo/discriminacion-y-violencia-contra-las-mujeres-en-los-videojuegos-mas-populares-de-estas-navidades/> accessed 7 May 2020
Apisa C, 'Anti-trafficking Apps of Interest' (*End Slavery Now*, 29 July 2015) <www.endslaverynow.org/blog/articles/anti-trafficking-apps-of-interest> accessed 10 June 2020
AWS, 'Amazon Rekognition' <https://aws.amazon.com/rekognition/?nc1=h_ls&blog-cards.sort-by=item.additionalFields.createdDate&blog-cards.sort-order=desc> accessed 18 June 2020
— 'AWS Service Capabilities for Privacy Considerations' <https://aws.amazon.com/compliance/data-privacy/service-capabilities/> accessed 18 June 2020
— 'Using AWS in the Context of Common Privacy & Data Protection Considerations' (May 2018) 10 <https://d1.awsstatic.com/whitepapers/compliance/Using_AWS_in_the_context_of_Common_Privacy_and_Data_Protection_Considerations.pdf> accessed 18 June 2020

Barr H, 'Bride Trafficking to China Spreads Across Asia' (*Human Rights Watch*, 3 November 2019) <www.hrw.org/news/2019/11/03/bride-trafficking-china-spreads-across-asia> accessed 25 July 2020

Blue V, 'Sex, Lies, and Surveillance. Something's Wrong with the War on Sex Trafficking' (*Engadget*, 31 May 2019) <www.engadget.com/2019/05/31/sex-lies-and-surveillance-fosta-privacy> accessed 11 July 2020

Boyd D, 'When It Comes to Sex Trafficking, Tech Is Far From Neutral' (*Wired*, 6 July 2013) <www.wired.com/2013/06/bias-as-disruption-how-tech-disrupts-sex-trafficking/> accessed 25 May 2020

BSR, 'Tech Against Trafficking' <www.bsr.org/en/collaboration/groups/tech-against-trafficking> accessed 18 June 2020

Buolamwini J, 'Response. Racial and Gender bias in Amazon Rekognition. Commercial AI System for Analyzing Faces' (*Medium*, 25 January 2019) <https://medium.com/@Joy.Buolamwini/response-racial-and-gender-bias-in-amazon-rekognition-commercial-ai-system-for-analyzing-faces-a289222eeced> accessed 29 July 2020

Cambridge Dictionary, 'hacktivism' <https://dictionary.cambridge.org/dictionary/english/hacktivism> accessed 9 June 2020

Campaign to Stop Killer Robots, 'High-level concerns on killer robots at UN' <www.stopkillerrobots.org/2019/10/unga74/?lang=es> accessed 5 June 2020

Canton Ferrer C, 'Machine Learning Can Help Find Kids Faster' (*Thorn*, 18 May 2017) <www.thorn.org/blog/machine-learning-find-kids-faster/> accessed 18 June 2020

Casey K, 'How Big Data and AI Work Together' (*The Enterprisers Project*, 14 October 2019) <https://enterprisersproject.com/article/2019/10/how-big-data-and-ai-work-together> accessed 15 June 2020

Castillo M, 'Sex Workers May be Hurt by Backpage Ad Crackdown' (*The Lily*, 10 April 2014) <www.thelily.com/sex-workers-may-be-hurt-by-backpage-ad-crackdown/> accessed 5 May 2020

Council of Europe, 'CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment' <www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> accessed 5 June 2020

The Counter Trafficking Data Collaborative (CTDC), 'FAQ' <www.ctdatacollaborative.org/faqs> accessed 11 June 2020

— 'Global Data Hub on Human Trafficking' <www.ctdatacollaborative.org/> accessed 10 June 2020

— 'Human Trafficking and Gender: Differences, Similarities and Trends' <www.ctdatacollaborative.org/story/human-trafficking-and-gender-differences-similarities-and-trends> accessed 29 July 2020

— 'Telling Their Stories Through Open Data' <www.ctdatacollaborative.org/about-us> accessed 11 June 2020

Digital Reasoning, 'We Found a Way…' <https://digitalreasoning.com/resources/thorn-case-study/> accessed 23 April 2020

— 'What Offers More Hope – More Data or Better Algorithms?' <https://digitalreasoning.com/resources/offers-hope-data-better-algorithms/> accessed 15 June 2020

Dressember, 'The Link Between Pornography and Human Trafficking' (*Dressember*, 3 April 2018) <www.dressember.org/blog/thepornographylink> accessed 10 June 2020

eCops, 'Child pornography reporting system' <www.ecops.be/request.php?Lang=EN> accessed 9 June 2020

ECPAT International, 'Emerging Global Threats Related to the Online Sexual Exploitation of Children' Briefing paper (2018)

European Commission, 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions - Coordinated Plan on Artificial Intelligence' (7 December 2018) COM(2018) 795 final <https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence> accessed 2 July 2020
— 'Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Artificial Intelligence for Europe' {swd(2018) 137 final}
— 'White Paper on Artificial Intelligence. A European Approach to Excellence and Trust' (19 February 2020) COM(2020) 65 final
European Commission. Eurostat <https://ec.europa.eu/eurostat/statistics-explained/index.php/Glossary:Information_and_communication_technology_ (ICT)>, accessed 14 April 2021
Europol, 'About Europol' <www.Europol.europa.eu/about-Europol> accessed 8 May 2020
— 'Dark Web Child Abuse: Administrator of DarkScandals arrested in the Netherlands' (Europol press release 12 March 2020) <www.europol.europa.eu/newsroom/news/dark-web-child-abuse-administrator-of-darkscandals-arrested-in-netherlands> accessed 9 July 2020
— 'Europol Analysis Projects' <www.Europol.europa.eu/crime-areas-trends/Europol-analysis-projects> accessed 9 June 2020
— 'Publications and Documents' <www.Europol.europa.eu/publications-documents?t=human%20trafficking> accessed 2 June 2020
— 'Stop Child Abuse – Trace an Object' <www.Europol.europa.eu/stopchildabuse> accessed 9 June 2020
— 'Trafficking in Human Beings' <www.Europol.europa.eu/crime-areas-and-trends/crime-areas/trafficking-in-human-beings> accessed 8 May 2020
— 'Trafficking in Human Beings and the Internet' Intelligence Notification 15/2014 (4 November 2014) <www.Europol.europa.eu/publications-documents/trafficking-in-human-beings-and-internet> accessed 7 May 2020
FindLaw, 'Dark Web Crimes' (15 May 2019) <https://criminal.findlaw.com/criminal-charges/dark-web-crimes.html> accessed 11 May 2020
Frei N, 'On "Cyber Trafficking" and the Protection of its Victims' (*Völkerrechtsblog*, 26 July 2017) <https://voelkerrechtsblog.org/on-cyber-trafficking-and-the-protection-of-its-victims/> accessed 19 June 2020
Freshfields Bruckhaus Deringer, 'The extra-territorial scope of the EU's GDPR' <www.freshfields.com/en-gb/our-thinking/campaigns/digital/data/general-data-protection-regulation/> accessed 15 June 2020
GitHub, 'Bornlex/traffickingGrab' <https://github.com/Bornlex/traffickingGrab> accessed 11 June 2020
Global Emancipation Network, 'Products' <www.globalemancipation.ngo/products/> accessed 11 June 2020
Global Modern Slavery Directory <www.globalmodernslavery.org/> accessed 11 June 2020
Greenberg A, 'Over 80 Percent of Dark-Web Visits Relate to Pedophilia, Study Finds' (*Wired*, 30 December 2014) <www.wired.com/2014/12/80-percent-dark-web-visits-relate-pedophilia-study-finds/> accessed 22 April 2020
Grove B and Bedi A, 'It's time we harnessed Big Data for good' (*World Economic Forum*, 17 October 2019) <www.weforum.org/agenda/2019/10/data-big-harness-good-human-trafficking-stop-the-traffic/> accessed 28 April 2020
Hourdeaux J, 'Un Vaste Réseau de Sites Pédophiles Piraté (*L'Obs*, 25 October 2011) <www.nouvelobs.com/les-internets/20111025.OBS3200/un-vaste-reseau-de-sites-pedophiles-pirate.html> accessed 10 June 2020
Howe J, 'The rise of crowdsourcing' (*Wired*, 6 January 2006) <www.wired.com/2006/06/crowds/> accessed 3 June 2020

IBM, 'Big Data Hub' <www.ibmbigdatahub.com/> accessed 15 June 2020
— 'IBM Security and Privacy by Design / SPbD@IBM' <www.ibm.com/trust/security-spbd> accessed 15 June 2020
Interpol, 'International Child Sexual Exploitation database' <www.Interpol.int/How-we-work/Databases/International-Child-Sexual-Exploitation-database> accessed 8 May 2020
Konrad R and Trapp A, 'Data Science Can Help us Fight Human Trafficking' (*The Conversation,* 28 July 2017) <https://theconversation.com/data-science-can-help-us-fight-human-trafficking-81647> accessed 11 June 2020
Langston J, 'How PhotoDNA for Video is being used to fight online child exploitation' (*Microsoft*, 12 September 2018) <https://news.microsoft.com/on-the-issues/2018/09/12/how-photodna-for-video-is-being-used-to-fight-online-child-exploitation/> accessed 14 July 2020
Lexico, 'digital footprint' <www.lexico.com/definition/digital_footprint> accessed 4 April 2020
The Library of Congress, 'Regulation of Artificial Intelligence: Europe and Central Asia' <www.loc.gov/law/help/artificial-intelligence/europe-asia.php> accessed 24 April 2020
Lieberman H, 'Why Laws Fighting Sex-Trafficking Often Backfire' (*The Washington Post*, 4 March 2019) <www.washingtonpost.com/outlook/2019/03/04/why-laws-fight-sex-trafficking-often-backfire/> accessed 25 May 2020
Lucanus A, 'Can Big Data Help Us Stop Human Trafficking?' (*DataFloq*, 3 February 2020) <https://datafloq.com/read/can-big-data-help-us-stop-human-trafficking/7611> accessed 10 June 2020
Marchant G, '"Soft Law" Governance Of Artificial Intelligence' (*AI Pulse*, 25 January 2019) <https://aipulse.org/soft-law-governance-of-artificial-intelligence/> accessed 12 July 2020
Marinus Analytics, '27th Annual Crimes Against Children Conferences' (28 August 2015) <www.marinusanalytics.com/articles/2015/8/28/27th-annual-crimes-against-children-conference> accessed 18 June 2020
Microsoft, 'Privacy: It's All About You' <www.microsoft.com/en-us/trust-center/privacy> accessed 12 July 2020
Myria, 'Le rôle des réseaux sociaux et d'internet dans la traite des êtres humains. Apercu du phénomène' (Myria 2017) <www.myria.be/files/RATEH-2017-fiches-r%C3%A9sum%C3%A9s_(1).pdf> accessed 6 May 2020
McCarthy J, 'What is Artificial Intelligence?'(Computer Science Department, Stanford University 12 November 2007) <www-formal.stanford.edu/jmc/whatisai.pdf> accessed 5 June 2020
The New York Times, 'Read Mark Zuckerberg's Blog Post on His "Privacy-Focused Vision" for Facebook' (*The New York Times*, 6 March 2019) <www.nytimes.com/2019/03/06/technology/facebook-privacy-blog.html> accessed 10 June 2020
NC Harm Reduction Coalition, 'Why are Sex Worker and Public Health Advocates Annoyed with Google?' (*Daily Kos*, 21 December 2011) <www.dailykos.com/stories/2011/12/21/1047597/-Why-are-Sex-Worker-and-Public-Health-Advocates-Annoyed-with-Google> accessed 11 June 2020
OECD, 'Glossary of Statistical Terms: Data Set' <https://stats.oecd.org/glossary/detail.asp?ID=542> accessed 5 June 2020
Office for Democratic Institutions and Human Rights and Organization for Security and Co-operation in Europe, 'Cross Linkages of Human Trafficking and Pornography. Myth or Reality' Conference (4 May 2020), <www.osce.org/odihr/450952> accessed 10 April 2021.
Payoke, 'Loverboys' <www.payoke.be/fr/loverboys/> accessed 8 May 2020
Peace B, 'Using Data and Analytics to Combat Human Trafficking' (*IBM,* 18 October 2018) <www.ibm.com/blogs/think/2018/10/using-data-and-analytics-to-combat-human-trafficking/> accessed 6 June 2020

Polaris, 'Responding to Human Trafficking' <https://polarisproject.org/responding-to-human-trafficking/> accessed 11 June 2020
Ram A, 'Modern Slavery Campaigners Turn to Online Exploitation' (*FT*, 28 August 2018) <https://next.ft.com/content/c6d6edce-3792-11df-88c6-00144feabdc0> accessed 6 May 2020
Sadwick R, '7 Ways Technology is Fighting Human Trafficking' (Forbes, 11 January 2016) <www.forbes.com/sites/rebeccasadwick/2016/01/11/tech-fighting-human-trafficking/#65ad3a686cacn> accessed 15 May 2020
Schreiner K, 'Data for Social Good Case Study: Global Emancipation Network' (*SIX*, 2 July 2018) <https://socialinnovationexchange.org/insights/data-social-good-case-study-global-emancipation-network> accessed 11 June 2020
Sheils C, 'Enter the Deep and Dark Web If You Dare (And Get Ready for a Surprise). Inside the Onion. Here's What You Need to Know About the Deep Web', <https://digital.com/online-privacy/deep-dark-web/>, accessed 5 March 2020.
Slavery Footprint, 'Made in a Free World. How many slaves work for you?' <http://slaveryfootprint.org> accessed 24 April 2020
Smith F, 'Case Study. Thorn Frees up Resources with MemSQL Helios to Identify Trafficked Children Faster' (*SingleStore*, 5 December 2019) <www.memsql.com/blog/case-study-thorn-frees-up-resources-with-memsql-helios-to-identify-trafficked-children-faster/> accessed 29 July 2020
Splunk, 'Guiding Principles' <www.splunk.com/en_us/legal/splunk-data-security-and-privacy.html> accessed 31 July 2020
Slunk, <www.splunk.com/en_us/legal/splunk-data-security-and-privacy.html#tabs/tab_parsys_tabs_CustomerDataPrivacy_1> accessed 17 June 2020
Stop the Traffik, 'The Stop App' <www.stopthetraffik.org/stopapp/> accessed 11 June 2020
— 'Traffik Analysis Hub' <www.stopthetraffik.org/what-we-do/traffik-analysis-hub/> accessed 15 June 2020
Thinyane H, 'How Can Human Trafficking Front Line Responders Use Technology?' (*Thomson Reuters Foundation News*, 30 May 2017) <https://news.trust.org/item/20170530133713-c7ik0/> accessed 23 April 2020
Thorn, 'Microsoft's PhotoDNA: Leading the Fight Against Child Sexual Abuse Imagery' (*Thorn*, 25 April 2016) <www.thorn.org/blog/photodna-leads-fight-against-child-sex-abuse-imagery/> accessed 23 April 2020
— 'Child Safety Hackathon Brings Silicon Valley Together' (*Thorn*, 12 May 2016) <www.thorn.org/blog/child-safety-hackathon/> accessed 20 June 2020
— 'Meet the new anti-grooming tool from Microsoft, Thorn, and our partners' (*Thorn*, 11 February 2020) <www.thorn.org/blog/what-is-project-artemis-thorn-microsoft-grooming/> accessed 22 April 2020
Traffik Analysis Hub <www.traffikanalysis.org/> accessed 15 June 2020
— 'How It Works' <www.traffikanalysis.org/how-it-works/> accessed 29 July 2020
— 'Our Mission' <www.traffikanalysis.org/our-mission> accessed 15 June 2020
Ungerleider N, 'How Mobile Phones And The Internet Fight (And Help) Human Trafficking' (Fast Company, 1 August 2013) <www.fastcompany.com/1681155/how-mobile-phones-and-the-internet-fight-and-help-human-trafficking> accessed 10 July 2020
United Nations Global Compact, 'Business as a Force for Good' <www.unglobalcompact.org/what-is-gc/mission> accessed 18 June 2020
University of Southern California, 'Technology & Human Trafficking' <https://communicationleadership.usc.edu/projects/list/trafficking/> accessed 18 June 2020
University of Toledo, 'Study Details Link Between Social Media and Sex Trafficking' (*phys.org*, 8 October 2018) <https://phys.org/news/2018-10-link-social-media-sex-trafficking.html> accessed 5 April 2020

Unodc, 'COVID-19 Seen Worsening Overall Trend in Human Trafficking', 2 February 2021, <www.unodc.org/unodc/frontpage/2021/February/share-of-children-among-trafficking-victims-increases--boys-five-times-covid-19-seen-worsening-overall-trend-in-human-trafficking--says-unodc-report.html>, accessed 10 April 2021.

Wijers M, 'Where do all the data go? European data protection law and the protection of personal data of trafficked persons', DatACT. Conference on data protection and trafficking, Berlin (25 September) <www.datact-project.org/fileadmin/user_upload/pdf/Marjan_Wijers.pdf> accessed 27 May 2020

Wu J, 'AI Is Helping Us Combat The Economic Problem Of Human Trafficking' (*Forbes*, 14 April 2020) <www.forbes.com/sites/cognitiveworld/2020/04/14/ai-is-helping-us-combat-the-economic-problem-of-human-trafficking/#546e08a0752c> accessed 19 June 2020

XPrize, 'AI to Solve Global Issues' <www.xprize.org/prizes/artificial-intelligence> accessed 18 June 2020

XPrize, 'Marinus Analytics' <https://ai.xprize.org/prizes/artificial-intelligence/teams/marinus_analytics> accessed 18 June 2020

Global Campus of Human Rights

Monastery of San Nicolò
Riviera San Nicolò, 26
I-30126 Venice Lido (Italy)

www.gchumanrights.org

Global Campus Europe.

The European Master's Programme in Human Rights and Democratisation (EMA)

EMA is a one-year intensive master's programme with participation of 41 prestigious universities representing all EU Member States. It is based on an action- and policy-oriented approach to learning and combines legal, political, historical, anthropological, and philosophical perspectives on the study of human rights and democracy with targeted skill-building activities. As a measure of its success, EMA has served as a model of inspiration for the establishment of EU-sponsored master's programmes in several other regions of the world, all of which are being coordinated and cooperate in the framework of the Global Campus of Human Rights.

The Global Campus Europe - EMA Awarded Theses

Each year the EMA Council of Directors selects five theses, which stand out not only for their formal academic qualities but also for the originality of topic, innovative character of methodology and approach, potential usefulness in raising awareness about neglected issues and capacity for contributing to the promotion of the values underlying human rights and democracy.

The present thesis - *Improving the International Regulation of Cybersex Trafficking of Women and Children through the Use of Data Science and Artificial Intelligence* written by **Ophélie Stockhem** and supervised by Maria López Belloso and Demelsa Beniso Sánchez, University of Deusto, Bilbao - was submitted in partial fulfillment of the requirements for the European Master's Programme in Human Rights and Democratisation (EMA), coordinated by Global Campus Europe.

This document has been produced with the financial assistance of the European Union and as part of the Global Campus Europe, coordinated by Global Campus of Human Rights. The contents of this document are the sole responsibility of the authors and can under no circumstances be regarded as reflecting the position of the European Union or of Global Campus of Human Rights