KOK

German NGO Network against
Trafficking in Human Beings

TRAFFICKING IN HUMAN BEINGS 2.0 – DIGITALISATION OF TRAFFICKING IN HUMAN BEINGS IN GERMANY

Developments and Courses of Action

TRAFFICKING IN HUMAN BEINGS 2.0 – DIGITALISATION OF TRAFFICKING IN HUMAN BEINGS IN GERMANY

Developments and Courses of Action

KOK
German NGO Network against
Trafficking in Human Beings

Information about the author:

For the past 17 years, Dr Dorothea Czarnecki's work and research has been focused on trafficking in human beings and sexual exploitation of children in Latin America, Europe and South-East Asia. She holds a degree in Intercultural Education and gained her PhD in Social Studies with a thesis on the lived experiences of girls subject to sexual exploitation in Guatemala. Ms Czarnecki's research includes studies on trafficking in children in Germany for the European Commission, on travelling sex offenders in Cambodia for ECPAT Germany, on online child protection for UNICEF Vietnam and on safe accommodation for trafficked persons for KOK. For many years, she was Deputy Director of ECPAT Germany, Vice Chair of the Board of ECPAT International, and until 2021 she was the Deputy and Interim Director of the ECPAT Secretariat in Bangkok, Thailand. Since 2022, Ms Czarnecki has been working as an analyst at a digital forensics consultancy and as an advisor to the initiative 'ACT Against Child Abuse' run by the Wilhelm von Humboldt Foundation, which aims to build a network of institutions that offer support to people who feel sexually attracted to children.

ABSTRACT

Technological advances in the form of digitalisation, further compounded by the COVID-19 pandemic, also play into the hands of traffickers, who can now pursue their criminal activities with greater reach, in any location and with a lesser risk of being discovered. Traffickers use the internet and other information and communications technology (ICT) throughout every phase of the exploitation process, in particular when seeking new recruits on social media platforms, but also in order to control trafficked persons while they are being exploited and exert pressure on them after they have escaped the exploitative situation. This study illustrates the range of options available to perpetrators by way of various case studies. Contrary to general suspicion, the dark web and cryptocurrencies only have a small role to play in these developments.

At EU level, new legal instruments are currently under development in response to the digitalisation of trafficking in human beings, with particular attention to mandatory accountability requirements for online platform operators, a new development in this field. Although law enforcement authorities, the judiciary and specialised counselling centres for trafficked persons in Germany have been unable to identify any other gaps in legislation that would make it harder or even impossible to prosecute cases of trafficking in human beings or provide support to trafficked persons given the technology-related aspects involved, they nonetheless find themselves confronted with new challenges. There is not yet a comprehensive awareness of the subject of digital and technology-facilitated violence in all its forms within government agencies or society at large, and as such law enforcement authorities and specialised counselling centres have so far not always deemed it necessary to develop or expand their capabilities in this area. The technical skills needed to respond appropriately to technological challenges in relation to IT security and the digital modus operandi of traffickers are lacking. Another major obstacle in practice is the uncertainty surrounding how to obtain digital evidence, which can prevent trafficked persons from exercising their rights to protection from violence.

Various stakeholders are working on technology-facilitated solutions for closing these gaps. The study presents four of these, each of which is based on a different technological solution (a website, machine learning, virtual reality and an app).

Moreover, on the basis of the obstacles identified in practice, the study calls for policymakers, law enforcement authorities and specialised counselling centres:

- to extend the cybersecurity agenda to trafficking in human beings and introduce a uniform definition;
- to accelerate the digitalisation of public administration;
- to clarify responsibilities for technology-assisted trafficking in human beings and facilitate interdisciplinary collaboration;
- to hold technology businesses accountable;
- to take IT infrastructure into account in funding for specialised counselling centres;
- to raise awareness about the subject and increase IT capabilities and resources;
- to improve IT security and expand ICT protection schemes.

CONTENT

1

INTRODUCTION

Thirty-two years since it became available for commercial use worldwide, an estimated 66.2% of the global population now has access to the internet. That is equivalent to 4.9 billion internet users, and this number is growing.[1] In Germany, 92% of people use the internet and other information and communications technology (ICT).[2] ICT refers to any technological tools that are used to transmit, store, create, share or exchange information. These tools include computers, the internet (websites, blogs and emails), live broadcasting technologies (radio, television and webcasting), recorded broadcasting technologies (podcasting, audio and video players) and telephony (landline or mobile, satellite, video-conferencing).[3] More broadly, it can also extend to things like digital networks, content, services and applications, networked devices and environments, virtual and augmented reality, artificial intelligence, robotics, automated systems and algorithms.[4]

The COVID-19 pandemic and the resulting lockdowns, which began in the spring of 2020, have acted as a catalyst for digitalisation. Even those who were previously sceptical about using digital technologies became reliant on them, either for working remotely with colleagues, for online classes in schools and universities or for relieving some of the psychological strain by keeping in touch with friends and relatives online. However, this increase in digitalisation was not only used to positive ends: 'In particular, the impact of the COVID-19 pandemic on cyber criminality has created a "new normal" worldwide. Cybercrime evolutions have altered the way criminals behave in order to exploit the current crisis [...] highlighting the readiness of cybercriminals to adapt their modus operandi to take advantage of human and technological vulnerability.'[5]

Traffickers have adapted their business models to the circumstances and now recruit, exploit and control trafficked persons online or using ICT.[6] Trafficking in human beings remains one of the most profitable criminal activities. In the EU, profits derived from trafficking in human beings for the purpose of sexual exploitation—the most common form of trafficking—are estimated at 14 billion Euros a year.[7] It is therefore unsurprising that organised trafficking rings are willing to rapidly adapt their operations to changing circumstances, such as the humanitarian

1 Statista.de: Statistics on global internet usage: https://de.statista.com/themen/42/internet/#dossierKeyfigures (only available in German).

2 Statista.de: Number of internet users in selected European countries in 2021: https://de.statista.com/statistik/daten/studie/184636/umfrage/internetreichweite-anteil-der-nutzer-in-europa/ (only available in German).

3 UNICEF, 2022: *Legislating for the digital age, Glossary.*

4 UNCRC: General Comment No. 25 (2021) on children's rights in relation to the digital environment.

5 Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., Aiken, M. P.: 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies.' In: *Forensic Sciences* 2022(2), p. 394.

6 United Nations Office on Drugs and Crime (UNODC), 2021: *The effects of the Covid 19 pandemic on trafficking in persons and responses to the challenges.*

7 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy on Combating Trafficking in Human Beings 2021–2025, COM/2021/171 final, 14 April 2021, p. 7, with reference to: European Commission, 2021: *Mapping the risk of serious and organised crime infiltration in legitimate businesses.* https://data.europa.eu/doi/10.2837/64101.

crisis resulting from the war in Ukraine that began in February 2022. Women and children are said to be lured in by what appear to be offers of assistance on social media platforms such as Facebook, only to be forced into prostitution in host countries such as Germany.[8]

Moreover, the economic cost of trafficking in human beings in the EU is estimated at around 2.7 billion euros a year.[9] Not only do countries have an additional financial burden to bear, they must also meet human rights obligations with respect to the protection and support of victims and criminal penalties for perpetrators under various international instruments, most importantly the Council of Europe Convention on Action against Trafficking in Human Beings (CETS No. 197) and Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims. However, it is worth noting that these instruments were created over a decade ago, when the internet did not yet play such a pivotal role in trafficking and certain technical and technological possibilities did not even exist.[10] On the ground, too, the support system for trafficked persons, the law enforcement authorities and the justice system are often unable to respond quickly enough to keep up with technological advances and societal changes. Indeed, the pandemic has made it harder for trafficked persons to access all three areas, and the digitalisation of human trafficking has resulted in enormous challenges for prosecutors.[11]

Two years on from the start of the pandemic and the resulting general increase in the use of digital technologies, it is necessary to consider to what extent stakeholders working towards combating trafficking in human beings and supporting trafficked persons have adapted their own use of technology. Currently, only anecdotal evidence is available regarding the situation in Germany and how the internet has affected trafficking in human beings (see Section 3). There has not yet been any academic, evidence-based research into the phenomenon.

1.1 DEFINITION OF TRAFFICKING IN HUMAN BEINGS

This study focuses on trafficking in human beings as defined by KOK,[12] which interprets the term more broadly than Sections 232 to 233a of the German Criminal Code. According to the KOK definition, trafficking in human beings occurs when individuals are recruited by means of deception, threat or use of force and persuaded or forced to commence and continue to perform services and activities in the destination country that infringe upon their guaranteed human rights on the grounds that they are exploitative or akin to slavery. Trafficked persons do not necessarily have to be recruited abroad; exploitation of an individual's position of vulnerability once they have already arrived in the destination country also falls under this definition of trafficking in human beings. Instead, it is the aspects of coercion, use of force and deception that are of primary importance, whereby the use of force can take various forms. It can involve direct physical violence or the threat of violence, blackmail, wrongful withholding of documents and earnings, theft, isolation and fraud. Exploitation of people's position of vulnerability, for example because they find themselves in a foreign country, abuse of authority and debt bondage all fall under the term "use of force" in the case of trafficking in human beings and exploitation.

This definition currently does not mention the use of information and communications technology.

8 Organization for Security and Co-operation in Europe (OSCE), 2022: *Recommendations on enhancing efforts to identify and mitigate risks of trafficking in human beings online as a result of the humanitarian crisis in Ukraine.*

9 European Commission, 2020: *Study on the economic, social and human costs of trafficking in human beings within the EU.*

10 The European Parliament has since commissioned an evaluation of Directive 2011/36/EU, the results of which are due to be published in December 2022. It is believed that the objective is to revise the Directive. The subject of digitalisation in trafficking in human beings will probably also play a role here, though the extent to which this will be the case and the relevant measures proposed remain unclear at the time of writing.

11 Cf. COMMUNICATION FROM THE FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS on the EU Strategy on Combating Trafficking in Human Beings, COM/2021/171 final, 14/04/2021.

12 Cf. KOK definition: https://www.kok-gegen-menschenhandel.de/menschenhandel/was-ist-menschenhandel (only available in German).

1.2 STUDY QUESTIONS AND OBJECTIVE

The specialised counselling centres that are members of the German NGO Network against Trafficking in Human Beings – KOK have recognised the need to learn more about the digitalisation of trafficking in human beings. They wish to bridge the gap between the knowledge previously required in order to handle conventional, "offline" cases of trafficking in human beings and the new digital and IT skills needed in order to keep up with the latest technological developments. That is why KOK has commissioned this study, which takes an initial look at how information and communications technology is affecting cases of trafficking in human beings in Germany, what consequences and challenges this brings for specialised counselling centres working with trafficked persons and for law enforcement and judiciary authorities, and what actions and recommendations are required in the fields of politics, law enforcement and justice as well as for the specialised counselling centres. The study aims to provide information and raise awareness and is directed at providers of counselling services in relation to trafficking in human beings in Germany as well as other professionals who deal with the subject. Since there are currently no other publications on this subject in Germany, this study can be regarded as a framework paper.

1.3 METHOD

In accordance with the principles and mandate of KOK, this study focuses primarily on the needs and perspective of the specialised counselling centres in Germany that provide support to persons affected by trafficking in human beings and exploitation. As a result, the majority of the expert interviews held for the purposes of this study were with counsellors from specialised counselling centres in Germany. In the period from 5 July to 1 September 2022, a total of 10 semi-structured interviews were carried out: six with practitioners from (specialised) counselling centres, one with a member of the Trafficking in Human Beings Department of the German Federal Criminal Police Office, one with a member of the Berlin public prosecutor's office who specialises in trafficking in human beings, one with two analysts from a digital forensics consultancy, and one with a representative of the Organisation for Security and Cooperation in Europe (OSCE) in order to incorporate the international perspective. A list of the interviews can be found in the appendix.

Each interview was transcribed and analysed based on pre-defined categories. The categories were determined based on a literature search at both German and international level. As the objective of the study is to shed light specifically on the situation in Germany, international information was only drawn upon if it appeared relevant to the German context or if no reliable data or well-founded information was available in Germany on a particular matter. This publication is intended as an exploratory study into the digitalisation of trafficking in human beings,

a subject area that has received little academic attention in Germany to date. It presents some initial findings, although given its prescribed scope and the small number of expert interviews held, it really only provides a snapshot of the situation. It is hoped that it will serve as the basis for further research and as a starting point for political discussions on the subject of the digitalisation of trafficking in human beings in Germany.

1.4 EXCLUSIONS FROM AND DELINEATION OF THE SCOPE: CHILD SEXUAL ABUSE MATERIAL AND LIVESTREAMING OF SEXUAL VIOLENCE

In Germany, online material depicting the abuse of children and young people in the form of photos, videos, animations and livestreaming of sexual violence are treated under a separate offence to trafficking in human beings under criminal law, instead falling under the offence of child sexual abuse and child pornography. As such, this subject was not investigated in this study. There may well be some overlap between trafficking in human beings involving the use of digital technologies and the livestreaming of child sexual violence in particular, primarily in that they both involve commercial exploitation. Indeed, this was recognised in General Comment No. 25 (2021) of the United Nations Committee on the Rights of the Child, which was the first paper to look at the subject of children's rights in the digital realm. [13] This paper identifies sexual exploitation and child trafficking as potential risks faced by children in the digital environment.[14] However, it stresses that in order to prevent and combat these risks, as well as support victims, an enormous policy effort is required at national level.[15]

Initial discussions on this subject have been held both at international level and at national level in Germany, which have raised numerous questions that require further consideration. To start with, cases of trafficking in human beings are usually hard to investigate and prosecute, and the rate of sentencing remains low. In cases of child sexual abuse and offences related to child sexual abuse material, the law provides the possibility to impose an obligation to undergo therapy upon perpetrators. This is not the case for trafficking in human beings. Moreover, trafficking in human beings also covers forms of exploitation other than sexual exploitation (forced labour, organ trafficking, forced begging, exploitation of criminal activities) that bear no relation to livestreaming. Furthermore, if child sexual violence by means of ICT does come to be included in legislation on trafficking in human beings, this should not mean that the sexual and child-

13 General Comment No. 25 (2021) on children's rights in relation to the digital environment.

14 Cf. ibid., paragraph 82: 'States parties should take legislative and administrative measures to protect children from violence in the digital environment, including the regular review, updating and enforcement of robust legislative, regulatory and institutional frameworks that protect children from recognized and emerging risks of all forms of violence in the digital environment. Such risks include physical or mental violence, injury or abuse, neglect or maltreatment, exploitation and abuse, including sexual exploitation and abuse, child trafficking, gender-based violence, cyberaggression, cyberattacks and information warfare. States parties should implement safety and protective measures in accordance with children's evolving capacities.'

15 Cf. ibid., paragraph 25: 'Children's online protection should be integrated within national child protection policies. States parties should implement measures that protect children from risks, including cyberaggression and digital technology-facilitated and online child sexual exploitation and abuse, ensure the investigation of such crimes and provide remedy and support for children who are victims.'

specific aspects of the offences and the associated impact on the affected children fade into the background or that preventative measures are no longer taken.[16]

A politically significant step was the inclusion of the subject of 'trafficking in human beings and online and offline child abuse' in the G7 Leaders' Communiqué of 28 June 2022.[17] Since then, discussions and exchanges have been held at the level of the Ministries of the Interior and law enforcement authorities of the G7 states with the objective of identifying possible overlap between these areas in order to ensure more effective prosecution and better protection of victims. Recommendations are due to be drafted by the G7 Interior Ministers in November 2022, but further efforts to address these issues at both national and international level remain to be seen.

2

TRAFFICKING IN HUMAN BEINGS AND THE INTERNET – WHAT IT MEANS IN PRACTICE AND ADDITIONAL DEFINITIONS

2.1 UNDERSTANDING OF THE SUBJECT AMONG PRACTITIONERS – STATUS QUO

In Germany, there do not yet appear to be any common definitions of trafficking in human beings used by professionals that cover the aspect of digitalisation. The interviewed experts couched the subject in broad terms such as "the role of the internet in trafficking in human beings" or "trafficking in human beings in connection with the internet" and unanimously noted that there had not yet been a real need for discussions and exchanges on the topic within their institutions or with their partners. It seems that the subject is not yet so relevant in practice that there is a need for specific terms. When cases do arise, certain aspects are considered separately, for example the platforms used to recruit trafficked persons. This is not because the counselling centres have not had to deal with such cases; rather, it can be put down to the internal categorisation of cases and the lack of knowledge within the specialised counselling centres about information and communications technologies and social media. 'I wouldn't have really considered the topic if we weren't talking about it now. However, it's always a relevant aspect and we're seeing

16 Cf. WeProtect Global Alliance, 2021: *Framing Child Sexual Abuse and Exploitation Online as a Form of Human Trafficking: Opportunities, Challenges and Implications. Expert Roundtable Outcomes Briefing*; ECPAT Germany and International Justice Mission Deutschland: Interdisziplinäres Fachgespräch zur sexuellen Ausbeutung von Kindern per Livestream, Mai 2022 ('Interdisciplinary Expert Seminar on Sexual Abuse of Children via Livestream', May 2022).

17 G7 Leaders' Communiqué, 28 June 2022, p. 25: 'We commit to step up our fight against trafficking in human beings and our efforts to prevent and combat child sexual abuse and exploitation globally, both online and offline. We ask our Interior Ministers to take forward the implementation of the Action plan to combat Child Sexual Exploitation and Abuse from September 2021.'

more and more of it, we just haven't explicitly started thinking about it yet' (specialised counselling centre interview, all quotations are our translations).

All of the specialised counselling centres that were interviewed identified gaps in their own knowledge and admitted to being unfamiliar with information and communications technologies in general and with the subject of digitalisation of trafficking in human beings in particular. For example, when questioned for the purpose of this study, the team at one specialised counselling centre raised questions about certain fundamental concepts: What is understood by "information and communications technology"? What is meant by "technology-facilitated"? 'We're definitely lacking on that front. […] When you asked the question, my first thought was that we haven't had a purely digital case of trafficking in human beings. But then I realised: we're talking about mixed forms. I think that's the trick, recognising that it's already part of what we do' (specialised counselling centre interview). Despite this, all of the specialised counselling centres demonstrated an enormous willingness to plug these gaps in their knowledge. They understand the need for basic awareness raising and training for providers of counselling services: 'Many counsellors don't realise and are surprised to hear about all the things that can happen. First and foremost, we need to get up to date with everything that's going on' (specialised counselling centre interview). Only then will it be possible to discuss what terms to use.

There is a lot of work to be done on this front, as use of different terminology both at national and international level mean that the different countries and authorities working together on the subject have diverging concepts and understandings thereof. As identified in the ECPAT *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse* (and this also applies to the terminology used in the case of trafficking in human beings in connection with the internet),[18] 'the […] inconsistent use of language and terms can lead to inconsistent laws and policy responses on the same issue. […] Even where the same terms are used, there is quite often disagreement concerning their actual meaning, leading to use of the same words to refer to different actions or situations. This has created significant challenges for policy development and programming, development of legislation and data collection […]' (ECPAT International 2018, p. XIII). The same applies to the terms used in relation to trafficking in human beings and the internet.

2.2 RELATED DEFINITIONS

As a foundational agreement in the fight against trafficking in human beings, the Optional Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime (Palermo Protocol, 2000) provides an internationally recognised definition of the phenomenon, which has become well established since the protocol was adopted and has found its way into national legislation.

However, there is not yet a comparable document that addresses the technology-related components involved in trafficking in human beings in the digital realm. Even more recent expert publications, such as the *Human Trafficking Glossary* by the Council of the Baltic Sea States (2019) do not contain any references to information and communications technology or other

18 ECPAT International, 2018: *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.*

digital aspects, choosing to focus solely on 'offline trafficking'.[19] Given the existence of this gap, it seems pertinent to expand the debate around the concepts related to the digitalisation of crime to include trafficking in human beings using information and communications technology.

2.2.1 Cybercrime

Currently, the most relevant international agreement on the matters under discussion here is the Council of Europe Convention on Cybercrime (Budapest Convention, 2001), including its second Optional Protocol (2022) that was drawn up in response to recent technological advances.[20] Germany signed the Convention in 2001, and ratified it on 9 March 2009.[21] The intention of the Budapest Convention is to implement an internationally agreed framework of legal principles and a classification system for cybercrime-related offences. However, a study conducted in 2022 concluded that there is still no precise and universally accepted definition of cybercrime,[22] despite the fact that exactly such a definition is needed in order to effectively combat this phenomenon. According to the authors of this study, difficulties in classifying cybercrime prevent the introduction of specific criminal offences, resulting in major challenges for police and justice systems due to limited knowledge and response capacity.[23] The study was unable to identify a single jurisdiction in the world that has a specific single offence of "cybercrime".

Following the same line of reasoning as that behind the creation of the ECPAT Terminology Guidelines, the authors of the study argue in favour of establishing a shared lexicon for policy makers and practitioners in order to clarify and implement common language on an international scale, as the introduction of a common language will be a key feature to the universal acceptance of cybercrime concepts.[24] With the aim of providing the foundations for such a lexicon, the authors attempted to draw up a typology of the phenomenon based on English-language literature (see Figure 1).[25] In this typology, they differentiate between the two broad categories of "cyber-dependent" and "cyber-enabled" crime. Cyber-dependent crimes are crimes that are based on use of the internet and could not exist without the internet. Cyber-enabled crime, on the other hand, would still exist without the internet, but on a much more limited and localised level.

The authors then set out four modi operandi that fall under these two categories, each covering different target groups, perpetrator motivations and victimisation tactics:

19 Council of the Baltic Sea States, Task Force against Trafficking in Human Beings, 2019: *Human Trafficking Glossary.*

20 Cybercrime Convention Committee (T-CY), Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. *Explanatory Report,* 17 November 2021, Article 5: 'Information and communication technology has evolved and transformed societies globally in an extraordinary manner since the Convention was opened for signature in 2001. However, since then, there has also been a significant increase in the exploitation of technology for criminal purposes. Cybercrime is now considered by many Parties a serious threat to human rights, the rule of law and to the functioning of democratic societies. The threats posed by cybercrime are numerous. Examples include online sexual violence against children and other offences against the dignity and integrity of individuals; the theft and misuse of personal data that affect the private life of individuals; election interference and other attacks against democratic institutions; attacks against critical infrastructure, such as distributed denial of service and ransomware attacks; or the misuse of such technology for terrorist purposes. In 2020 and 2021, during the Covid-19 pandemic, countries observed significant Covid-19 related cybercrime […].'

21 List of current signatures and ratifications on the website of the Council of Europe. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=5isnGr2b

22 Phillips, K./Davidson, J. C./Farr, R. R./Burkhardt, C./Caneppele, S./Aiken, M. P.: 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies.' In: *Forensic Sciences* 2022(2), pp. 379–398.

23 Cf. ibid., p. 391.

24 Cf. ibid. p. 394.

25 Cf. ibid. p. 383.

I) “Crimes against the machine” involve attacks against data and systems as well as against states and include hacking or data espionage for political ends.
II) “Crimes with the machine” usually involve attacks against property or theft, including fraud.
III) “Crimes in the machine” cover interpersonal violence, sexual violence and violence against groups, including some forms of trafficking in human beings for the purpose of sexual exploitation, child sexual abuse material and crimes using social media platforms.
IV) “Cyber-assisted crimes” involve incidental use of technology, i.e. although technology is used to organise and carry out the intended offence, the crime would still take place even if that technology did not exist, for example drugs trading and trafficking in human beings. Another example is a murderer performing a Google search on how to dispose of a body.[26]

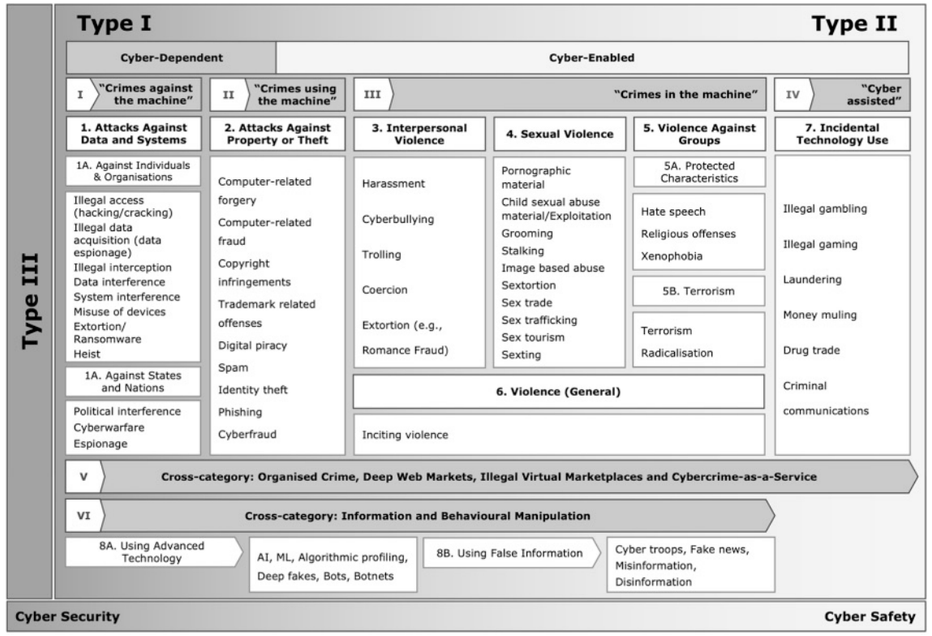

Figure 1: Cybercrime and cyberdeviance, Classification Framework Source: *Forensic Sciences* 2022(2).

2.2.2 Definition of cybercrime used by the German Federal Criminal Police Office

According to the German Federal Criminal Police Office, cybercrime is a highly complex criminal sector with its own value chains and is one of the most rapidly evolving criminal phenomena.[27] In order to take account of this complexity, the term “Cyberkriminalität” (“cybercrime”) is increasingly being used in Germany instead of “Computerkriminalität” (“computer crime”),

26 Cf. Wall, 2007.

27 German Federal Criminal Police Office, *Cybercrime* (in German). https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (only available in German).

which was how the term was translated in the German version of the Budapest Convention. In 2020, the German Federal Criminal Police Office, which publishes an annual Federal Situation Report on Cybercrime, and the editors of the police crime statistics agreed to introduce “cybercrime” as a new category of offence in the statistics in order to ensure that a common denomination was used for these crimes at national level. Since 2021, the term “cybercrime” has been used to describe this category of offence instead of “Computerkriminalität”.[28] Similarly to the “cyber-dependent” and “cyber-enabled” dichotomy, the German Federal Criminal Police Office differentiates between *cybercrime in a narrow sense* (i.e. offences targeted against the internet, data networks, IT systems or their data) and *cybercrime in a broad sense* (i.e. offences committed using information technology). ‘In simple terms, therefore, “cybercrime in a broad sense” covers offences that could also be committed offline, such as drugs trading. “Cybercrime in a narrow sense”, on the other hand, refers to extremely technical crimes that also require highly technical investigative work to be performed by the police. […] In the underground economy, there are numerous marketplaces for illegal goods such as drugs, weapons, child pornography, stolen data and identities, but also “cybercrime-as-a-service”, where people can be hired to carry out cybercrime.’[29] However, the definition of cybercrime used by the German Federal Criminal Police Office does not cover offences falling under trafficking in human beings, which are therefore not included in the Federal Situation Report on Cybercrime.

2.2.3 Sexual violence in the digital realm/digital violence

Although there is no lack of cybercrime definitions and concepts at international level, the majority of this economic, legal and criminological theorising is dominated by men. Thus, the authors of the study in Forensic Sciences argue: ‘Given that there is male dominance in the field of cybercrime and cybersecurity, and the high prevalence of gender-based crimes online, arguably, the application of feminist approaches to both defining and exploring cybercrime is lacking. Future contributions to the field should look to apply criminological feminist contributions and perspectives of cybercrime, in particular to crimes that manifest as sexual violence online.’[30]

As will be illustrated in greater detail in the following sections, traffickers use social media platforms to exert psychological pressure on trafficked persons. This occurs not only during the period of their exploitation, for example in order to keep them under control, but also afterwards, in order to discourage trafficked persons from reporting their ordeal. Specialised counselling centres have reported cases of identity theft in the form of fake accounts, which are created using the trafficked person’s name against their will or without their knowledge, and which are used to contact families and acquaintances. This is often associated with image-based violence, in other words sending intimate images without the consent of the person in question.

A study by the Council of Europe (2021),[31] which considered links between the Istanbul Convention and the Cybercrime Convention from the perspective of preventing violence against women and girls, identified the following forms of violence, among others, which have also been reported by the specialised counselling centres in cases of trafficking in human beings in Germany:

28 Cf. German Federal Criminal Police Office, *Bundeslagebild Cybercrime 2021* (‘2021 Cybercrime Situation Report’, only available in German).

29 German Federal Criminal Police Office, *Cybercrime* (in German). https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Cybercrime/cybercrime_node.html (only available in German).

30 *Forensic Sciences* 2022, p. 395.

31 Council of Europe, 2021: *Protecting women and girls from violence in the digital age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women*, p. 10.

- Online sexual harassment: sending of unsolicited sexual images, sexualised comments, sexualised defamation and sexualised slander;
- Image-based sexual harassment: sexually suggestive or private pictures taken without consent and shared online, also known as "creepshots", sexual or private pictures taken under the skirt or dress without consent and shared online, also known as "upskirting";
- Image-based sexual abuse: non-consensual sharing of intimate image or video material, as well as web-based sexual violence (previously known as "revenge porn"), deepfakes, recorded sexual assault and rape, including "happy slapping" (either live-streamed or distributed on pornographic sites);
- Threats and coercion, sexting, sextortion, rape threats, incitement to commit rape;
- Forms of online stalking, surveilling or spying on social media or messaging, password stealing, spyware installation on the devices of those affected, tracking via GPS or geolocation.

In Germany, the *Bundesverband Frauenberatungsstellen und Frauennotrufe* (Federal Association of Women's Counselling Centres and Helplines, bff) was one of the first civil society organisations to address the subject of digital violence against women. The digitalisation of gender-based violence began to emerge as soon as 2000, though it has grown in momentum and relevance in recent years. 'There is a radical transition going on right now that no-one fully understands' (bff interview). On its website,[32] bff defines digital violence as: '[...] An umbrella term for various forms of gender-based violence. It refers to acts of violence committed using technical aids and digital media (mobile phones, apps, internet applications, emails, etc.) and violence committed in the digital realm, e.g. on online portals or social platforms. We believe that digital violence is not separate from "offline violence", but is usually a manner of continuing or compounding violent relationships or dynamics.'

bff believes it is particularly important to use appropriate and non-stigmatising language that respects the perspective of those affected by these crimes, highlights the structural nature of language dynamics and does not individualise the problem of digital sexual violence, '[...] because it is not individual, but varies between genders' (bff interview). In some cases, this approach has already resulted in the development of alternative terminology, for example "image-based sexual violence" instead of "revenge porn".

2.2.4 Psychological violence in the digital realm

There appears to be a fine line between psychological pressure and psychological violence, both offline and in the digital world. All of the aforementioned forms of violence can also be categorised as psychological violence. The Istanbul Convention defines this term as intentional conduct which seriously impairs and damages a person's psychological integrity. However, the Convention does not define what is to be understood by "serious impairment". As the explanatory report to the Convention explains, coercion or threats must be made for behaviour to come under this

32 bff: *Aktiv gegen digitale Gewalt.* ('Action Against Digital Violence'). https://www.frauen-gegen-gewalt.de/de/aktionen-themen/bff-aktiv-gegen-digitale-gewalt.html (only available in German).

provision. It should be highlighted that the Istanbul Convention does not understand this term to mean a single event, but an abusive pattern of behaviour occurring over time.[33]

All forms of violence against women and girls in the digital environment have a psychological impact on those affected and can therefore be categorised as psychological violence committed online using information and communications technology. Certain characteristics of digital violence enhance its effect on targets, including the following elements:[34]

- It can be difficult to even recognise digital violence, as the boundaries between the different forms of violence are often blurred and are not always clearly delineated in criminal law.
- Most forms of digital violence occur on various platforms, both public and private; perpetrators can exert a stronger influence on their targets by using all of these platforms simultaneously. For example, a person may be discredited in public using social media such as Instagram and Facebook and at the same time be subjected to email threats, telephone harassment or physical intimidation on the street.
- Typical forms of digital violence comprise a repetitive aspect, and the harmful content is often of a permanent nature. For example, in most cases of image-based abuse there is the potential for the images to be shared via thousands of accounts across the internet, meaning that the target can be victimised over and over again.
- The burden of proof lies with the target of the crime, but digital evidence can simply be deleted or obscured by perpetrators; those affected often lack the technical skills to collect digital evidence, as do the counsellors and police in many cases, as discussed further in Section 6 under 'Challenges'. In some cases, those affected may not even realise that they need to keep evidence of acts of violence even when they are digital.

All of these specificities of digital violence serve to amplify its negative effects on those targeted, and as a consequence it often also impacts their families, children and relationships, their job situation, their health, and even their life expectancy. According to an EU study, the total estimated cost of the consequences of cyber-bullying and cyber-stalking of women amount to around 49–89.3 billion Euros a year. This includes health and legal costs, labour market costs and costs in connection with reduced quality of life.[35]

Specialised counselling centres have observed that an increasing number of cases of trafficking in human beings in Germany feature these forms of violence and related aspects in addition to exploitation.

33 Council of Europe, 2011: *Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence, Council of Europe Treaty Series No. 210.*

34 Cf. Council of Europe, 2021: *Protecting women and girls from violence in the digital age.* p. 11.

35 European Parliamentary Research Service, 2021: *Combating gender-based violence: Cyber violence.*

3

MODUS OPERANDI IN A DIGITAL ENVIRONMENT

In the field of cybercrime in general, 'perpetrators adapt to technical and societal developments, act at a global level, and focus their operations where it is most profitable from their perspective', according to the German Federal Criminal Police Office.[36] Trafficking in human beings is above all financially motivated. It is a commercial activity that responds to supply and demand like any other market. The internet has come to be used as a tool for carrying out trafficking offences (German Federal Criminal Police Office interview), and information and communications technology has greatly improved and facilitated business for traffickers,[37] for example by opening up a huge array of new possibilities and extending their reach, both in terms of finding new recruits and acquiring new customers. Like any business, traffickers compete with one another and try to keep their costs down. ICT makes their job easier in this regard, as they no longer need to run a physical brothel, for example. As a result, they can save on rent, electricity, security and so on. Instead, they can advertise sexual services online and simply book a room in a motel, hotel or Airbnb (OSCE interview).

Even before the pandemic, Professor of Criminology David Wall (2017) had identified three key aspects of digital network technologies that have changed criminal behaviour.[38] First of all, they have caused a "glocalising" effect due to their global impact on local policing services. For example, new types of crime committed by offenders in one country upon people in another create the need for local police to adapt their crime-fighting capacity. Secondly, network technologies allow perpetrators to victimise many individuals across the planet at the same time, creating the potential for new types of asymmetric relationships. This effect can be observed in cases of cyber-grooming, for example, where perpetrators have several chat threads ongoing in parallel with their potential targets. Thirdly, network technologies and the related platforms and social media are creating new forms of networked and non-physical social relationships that provide a source of new criminal opportunities. These include digital stalking and sextortion, where perpetrators threaten to publish private nude photos of their targets on social platforms. Instead of committing a large-scale crime at great risk to themselves, it is now just as profitable for criminals to commit numerous small offences that pose a much lesser risk of being caught. According to Wall (2017), this is the essence of how criminals use digital technology.

Traffickers use the internet and ICT in every phase of the exploitation process: 1) to find new recruits; 2) for transport and logistics; and 3) in order to control and monitor trafficked persons.[39] In addition, specialised counselling centres have identified another way in which criminals use ICT in their day-to-day practice, namely 4) in order to commit digital violence after

36 German Federal Criminal Police Office, *Was ist Cybercrime?* ('What is cybercrime?', only available in German).

37 EUROPOL 2022: *European Migrant Smuggling Center. 6th Annual Report.*

38 Wall, D. S., 2017: 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing.' In: Brownsword, R., Scotford, E., Yeung, K. (eds): *The Oxford Handbook on the Law and Regulation of Technology,* unpaginated.

39 Cf. Raets, S., Janssens, J., 2019: 'Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business.' In: *European Journal on Criminal Policy and Research* (2021) 27, pp. 15–238; cf. EU Strategy on Combating Trafficking in Human Beings 2021–2025.

a relationship of exploitation has come to an end, usually to prevent the person in question from testifying as a witness. Therefore, the following sections will discuss the role of ICT in the modus operandi of perpetrators across all four phases, illustrating the various ways in which it is used through case studies. To date, the use of technology has only been observed in cases of trafficking in human beings for the purpose of sexual exploitation and labour exploitation; there is very little reliable evidence regarding the potential involvement of ICT in other forms of exploitation such as forced begging.[40]

Whilst there have already been numerous international articles, studies and media reports written on the role of social media, ICT and digitalisation in trafficking in human beings,[41] the phenomenon appears relatively under-researched in Germany based on the scant reporting and piecemeal data available on the subject, and information is usually only based on anecdotal findings from cases.

3.1 USE OF TECHNOLOGY FOR RECRUITMENT

Alongside the actual period of exploitation, the period of recruitment of individuals by traffickers is the phase in which information and communications technology appears to play the biggest role, as observed in the current literature[42] and by the German Federal Criminal Police Office and specialised counselling centres. Perpetrators use social media platforms such as Facebook, Instagram and TikTok, as well as messaging services like Telegram and WhatsApp to dramatically increase their reach compared to offline recruitment methods like word-of-mouth or middlemen, all with little effort or expense. There is not one platform that is preferred above all others; any interactive channel that allows direct contact with potential recruits is considered an 'enabler' and harbours the potential for exploitation (German Federal Criminal Police Office interview).

CASE STUDY A

PART I – JADWIGA MUNICH – LOVERBOY ON FACEBOOK – RECRUITMENT

A. lives with her parents and younger brother in a rural area of Romania. Her family lives on the breadline, and they only have electricity and running water when her mother is able to scrounge for some work, for example as an agricultural labourer. Her father is an alcoholic and is unemployed. Domestic and sexual violence are a common occurrence at home. Against her father's will, both children go to school and gain their school-leaving qualifications, though this is a constant source of dispute.

40 Cf. Council of Europe, 2022: *Online and technology-facilitated trafficking in human beings;* OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, 2022: *Policy Responses to Technology-Facilitated Trafficking in Human Beings: Analysis of Current Approaches and Considerations for Moving Forward.*

41 See, for example, *Anti-Trafficking Review No. 14, 2020: Special Issue – Technology, Anti-Trafficking, and Speculative Futures.*

42 Cf. Council of Europe, 2022; Raets, Janssens, 2019; OSCE, 2022.

After finishing school, A. is unable to find work and spends a lot of time online to distract herself from her troubles at home. A young Romanian man living in Germany contacts her on Facebook. They chat frequently: A. tells him about her problems with her parents, the family's difficult financial situation, her emotional stress and her desire to protect her brother from domestic violence. Within a few weeks, A. has fallen in love with the man, and they make a plan to get married. He offers to come over from Germany and pick her up from home and promises to find her a job as a manager in Germany. At this point, A. is 18 years old. She does not tell her parents about her plans to move to Germany but says she is just moving to another town in Romania. Her father threatens to sever all ties with her if she leaves.[43]

The criteria normally used by traffickers when identifying potential recruits for sexual exploitation on social media revolve around vulnerability, accessibility and attractiveness.[44] The next step of making contact and gaining their trust takes a little more effort, and perpetrators may employ one of two strategies: they either "fish" for as many potential recruits as possible in the hope that one of them takes the bait, or they take a more targeted approach and personalise cyber-grooming by searching for any publicly available data on the individual in question. This personalised method is made easier by the fact that many people are willing to share information about themselves online and are open to being contacted by people they do not know. Perpetrators are very skilful at creating an online persona that is precisely what their target is looking for, both through their emotional, interpersonal interactions and by way of fake profiles suggesting that they are wealthy individuals with a high quality of life.[45] In expert circles, the strategy of feigning a romantic relationship whilst controlling and socially isolating their target is known as the "loverboy" ploy.[46] This paves the way for 'pseudo-intimate and eroticised interactions'[47], in which the individual is gradually prepared for commercial sexual activities by convincing them that this is "normal". Investigations by the Bulgarian authorities have found that 'before approaching their potential victims and starting the recruitment, perpetrators carefully examine the photos of their targets [in order to] explore their living conditions, social status and environment, family relations and relationship status, such as marriage, divorce or engagement. […] It is only after such careful examination that the perpetrators contact their victims, employing remarkable psychological skills of persuading and motivating victims to engage in certain behaviours.'[48]

43 See also the ARD documentary *Illegale Prostitution – Das gefährliche Geschäft mit dem Sex* ('Illegal prostitution – the dangerous trade in sex'), 9 February 2022: https://www.ardmediathek.de/video/betrifft/illegale-prostitution-in-der-pandemie/swr/Y3JpZDovL3N3ci5kZS9hZXgvbzE2MTAxMzQ (only available in German).

44 Cf. Raets, S., Janssens, 2019.

45 Cf. Council of Europe, 2022.

46 See, for example, KOK case law database, Aachen Regional Court judgment of 25 September 2019, case no. 62 KLs 4/19. Aggravated trafficking in human beings using the loverboy method, contact made via internet platforms. https://www.kok-gegen-menschenhandel.de/rechtsprechungsdatenbank/datenbank/detailansicht?tx_t3ukudb_urteile%5Baction%5D=show&tx_t3ukudb_urteile%5Bcontroller%5D=Item&tx_t3ukudb_urteile%5Bitem%5D=385&cHash=eebac44fea7e8640008eae82c4c3642f (only available in German).

47 Raets, Janssens 2019, p. 221.

48 Council of Europe, 2022, p. 32.

CASE STUDY B

FIZ – RECRUITMENT VIA TIKTOK AND ONLINE EXPLOITATION

When B., a 15-year-old schoolgirl from Dresden, returns to in-person lessons as schools reopen after lockdown, her teachers notice that at certain times each day she is very absorbed in her smartphone and stops participating in class. It turns out that B. had met an older man from East Frisia over TikTok, who was feigning a romantic interest in her and convinced her they were in a relationship. When they first got to know each other, she was asked to send him erotic images of herself. They met multiple times a day, first on TikTok and then on a secure digital platform where they were completely unsupervised, without any moderation or reporting mechanisms. He told her to perform specific sexual acts on herself and took photos and videos which he then sold online. There are currently four court cases ongoing involving the suspect in four different locations, and FIZ is providing psychosocial support during the court cases.

The police statistics of the German Federal Criminal Police Office (2019 and 2020 Federal Situation Report on Trafficking in Human Beings) also indicate that in recent years, it has become increasingly common for initial contact to be made via the internet. This was true of 55 cases (13.1%) in 2021, with those affected being recruited both via social media and via posts on online advertising portals.[49] The German Federal Criminal Police Office suspects a link between this increase and the prohibition of prostitution during the pandemic, which forced perpetrators to instead seek sexual services on social media and dating platforms. The fact that perpetrators often operate under pseudonyms or fake accounts is said to complicate police investigations into such cases. 'It is likely that perpetrators figure that there is a lower risk of being caught when they commit their crimes in the digital realm.'[50]

Available technologies allow traffickers to react immediately to changing circumstances. For example, the specialised counselling centres report that since the start of the war in Ukraine in February 2022, traffickers have begun operating in existing diaspora groups for Ukrainians and emergency response groups on internet platforms like Facebook in order to recruit women for sexual or labour exploitation. The specialised counselling centres interviewed for this study also reported that Eastern European women themselves have started proactively searching online once they make the decision to come to Germany in order to work as prostitutes. They use social media to contact brothels, negotiate their salary and receive relevant information such as cost of living calculations and photos of their room on their smartphone. Often, transportation is also organised by brothel owners, who send a minivan to pick up women from their home address. This presents a major security risk, as providing traffickers with their home address and potentially information about their family situation allows brothel owners to put pressure on these women further down the line.

49 German Federal Criminal Police Office *Bundeslagebild Menschenhandel 2021* ('2021 Federal Situation Report on Trafficking in Human Beings', only available in German).

50 German Federal Criminal Police Office, *Bundeslagebild Menschenhandel 2020* ('2020 Federal Situation Report on Trafficking in Human Beings', only available in German), p. 24.

3.2 RECRUITMENT FOR LABOUR EXPLOITATION

Social media and the internet are not only being used to recruit people for sexual exploitation, but also for the purpose of labour exploitation. According to the German authorities, the internet and social media are also playing an increasingly important role in this area. This was probably further driven in part by the pandemic, as face-to-face interactions had to move online during lockdowns.[51] To start with, perpetrators post a job offer on various online portals. Despite not requiring any professional qualifications, the positions often appear promising, yet the adverts are kept as vague as possible.[52] The jobs are presented as being well-paid and are said to involve regular working hours. However, upon arriving in Germany, workers find themselves without an official employment contract, they are not paid or only receive a fraction of what they were promised.[53]

Traffickers not only advertise on conventional job websites but also use special groups set up for people looking for work in Germany, such as 'Bulgarians Abroad' or 'Nguoi tim viec' (Vietnamese for 'job-seekers').[54] Specialised counselling centres and the German Federal Criminal Police Office also note that the messaging service Telegram is often used for recruiting individuals for the purpose of labour exploitation, especially from Eastern Europe.[55] These days, the internet is the first port of call for job-seekers, rather than newspapers or employment agencies. The fact that recruitment now takes place in the digital realm makes it even more likely that people will fall for "bait offers". The recruitment phase is much shorter when there is no need for a physical agency, and communication is quicker and more anonymous. The German authorities have identified the following fields as particularly susceptible to trafficking in human beings: seasonal agricultural work, cleaning services, hospitality, construction, food industry, transport, and nail and massage salons.

Compared to trafficking in human beings for the purpose of sexual exploitation, the use of technology to recruit individuals for the purpose of labour exploitation appears to be less widespread, despite all of the options out there for criminals. This could be down to the fact that workers are often recruited from marginalised regions, where access to modern technologies is far from guaranteed. 'Thus, from this perspective, online recruitment in labor trafficking is hindered by a technology gap between victims and perpetrators.'[56]

3.3 TECHNOLOGY-ASSISTED TRANSPORT AND LOGISTICS

Trafficking in human beings, especially when it is of a cross-border nature, requires agreements and coordination between multiple individuals. There is not one single trafficker who accompanies the trafficked persons over the entire journey; instead there are individuals with different tasks and roles. There are recruiters in the home location of the trafficked persons; there are those who are in contact with madames or other types of exploiters; there are those that help the

51 Cf. Council of Europe, 2022.

52 Cf. Raets, Janssens, 2019.

53 Cf. Council of Europe, 2022.

54 Cf. ibid.

55 Cf. OSCE, 2022.

56 Raets, Janssens 2019, p. 222.

trafficked persons flee home or accompany them on their journey; and there are perpetrators who pocket the trafficked persons' wages as well as traffickers present at the location where the exploitation takes place. The use of technology facilitates the management and organisation of trafficking in human beings, and can therefore be regarded as a 'essential business resource'.[57] Thanks to digital communications technology, perpetrators do not even need to be physically present during the transportation of trafficked persons any more. The fact that ICT facilitates online recruitment and helps to streamline logistics could mean that in future, trafficking in human beings will increasingly become a one-person operation, without the need for larger organised structures.[58]

CASE STUDY

FROM THE GERMAN FEDERAL CRIMINAL POLICE OFFICE – 'CALL CENTRE TRAFFICKING' – TRANSPORT AND LOGISTICS

One case referred to the German Federal Criminal Police Office by the French authorities is a particularly good example of a new modus operandi used in trafficking in human beings for sexual exploitation in the form of prostitution. In this case, groups of perpetrators recruited women in Bulgaria on the pretext that they were being hired for regular work in France, Germany and Bulgaria. Unlike in most of the trafficking in human beings cases seen to date, these women organised their own transport to the accommodation provided, following instructions from the perpetrators. At no point were they picked up, accompanied or met by anyone from the groups of perpetrators or by other trafficked persons. The women received all the information digitally and saved it on their smartphones. That included electronic bus tickets to their destination, Google Maps addresses, Google Street View images to help them navigate based on what the streets and buildings looked like, photos of the accommodation and codes for the electronic locks to get in. The women were instructed to call the perpetrators upon their arrival.

Customers were acquired by "managers" in Poland, Romania and Germany. They informed the women of their appointments by telephone each day, providing them with the time and the name of the client. They also called afterwards to check what they had been paid. The women either received payment in cash, which they then had to transfer via Western Union, or the clients paid the perpetrators directly using PayPal. Due to the central role of telephones in this case, the investigating officers referred to it as 'call centre trafficking'. The case was uncovered during police checks in relation to the illegal operation of prostitution services from residential properties, as it seemed peculiar that all properties were being rented by one and the same person, yet the only people present during the checks were the women, who were always the same.

A similar case has been reported by the authorities from Bosnia and Herzegovina.[59] A trafficking ring based there was organising and managing the sexual exploitation of Bosnian women in Germany and Austria, without ever having to leave the country. The perpetrators monitored the online profiles of the trafficked women and set appointments with clients.

57 Ibid., p. 223.

58 Cf. ibid.

59 Cf. Council of Europe, 2022, p. 29.

The 'call centre' case also illustrates another major issue, namely the ability of traffickers to render trafficked persons invisible. They are isolated, for example in apartments used exclusively for prostitution, leaving them hidden away and out of reach for traditional support services like social outreach work on the streets done by the specialised counselling centres.

3.4 DIGITAL CONTROL, MONITORING AND INTIMIDATION DURING THE PERIOD OF EXPLOITATION

Digital technologies are primarily used during the exploitation phase in order to allow perpetrators to use force to control, monitor and intimidate trafficked persons to make sure they continue working and are unable to escape the exploitative situation. Prostitution has shifted away from traditional brothels and towards more private locations or online; something that was particularly apparent during the pandemic-related lockdowns.[60] Perpetrators offer the "services" of trafficked persons more or less overtly via social media, escort websites, platforms such as the former kaufmich.de (literally 'buy me'), as well as general sales platforms like Ebay Classified Ads and second-hand goods platforms. The perpetrators usually agree appointments with clients via telephone.

KOK case law database – monitoring of prostitution activities via martphone in a 'Chinese brothel' [61]

The principal defendant, Z., had operated numerous brothels and apartments used for prostitution in various German cities between 2011 and 2015. The 40 Chinese women working at these locations had been recruited for prostitution via Chinese websites and travelled to Germany on forged tourist visas. Sometimes the procurers bore the cost of the forged paperwork and travel, a debt the women then had to "work off" by selling prostitution services in Germany. The recruited women slept where they worked, required permission to leave the premises and were supplied with groceries by their procurers.

Z. ended up earning nearly 2 million euros in total. The premises were open 24/7, and the women worked the entire time. They waited in the apartments for clients who made appointments by telephone and were available around the clock. Each time they met a client, the women had to report to their procurer either by telephone or WeChat (similar to WhatsApp), as directed, and sometimes the women sent them a photo of their completed schedule for the day each evening. They always had to record the time and duration of the appointment, as well as how much they earned and their name.

Information and communications technology made it possible for the perpetrators to operate from a different location to that in which the exploitation was taking place and where the trafficked persons were being held, for example in that they were instructed to send the perpetrators evidence that they had performed each "service" using the internet. Digital technologies also eliminate the need to hire a guard to keep an eye on the trafficked persons. Cypriot, Swiss and Austrian authorities have noted an increase in the use of apps for monitoring trafficked persons. Examples include automatic notifications sent to perpetrators' mobile phones when the trafficked persons perform a certain action, such as opening the front door of the apartment. Perpetrators also use tracking apps in order to determine the exact location of the individuals they traffic, which are often installed on their smartphones without them knowing.[62] Tracking apps belong to the overarching category of spyware, i.e. software or apps that are used to monitor people without their knowledge. Spyware technology is easy to use and can be bought cheap and allows perpetrators to '[…] directly control or harass the victim or to penetrate and surveil the victim's phone, providing the perpetrator with access to the victim's communication and whereabouts, including browsing history, texts, e-mails, calls, social networks, media such as videos and photos, their passwords, including bank account passwords and their real-time GPS location.'[63]

60 Cf. Teschner, G.: 'Sex on Demand. Prostitution geht online, Menschenhandel und Ausbeutung auch?' ('Sex on Demand. Prostitution is going online – what about trafficking and exploitation?'), In: *Kriminalistik* 11/2021, pp. 645–648.

61 KOK case law database: Kleve Regional Court of 21 February 2017, case no. 190 KLs-203 Js 98/15-2/16. https://www.kok-gegen-menschenhandel.de/rechtsprechungsdatenbank/datenbank/detailansicht?tx_t3ukudb_urteile%5Baction%5D=show&tx_t3ukudb_urteile%5Bcontroller%5D=Item&tx_t3ukudb_urteile%5Bitem%5D=274&cHash=9c2a405e13a891876c89fb7588fd51c3 (only available in German).

CASE STUDY A, PART II

JADWIGA MUNICH – LOVERBOY ON FACEBOOK – INTIMIDATION

A. carries out the plan as agreed. After a few days in Munich, her fiancé reveals that she is going to have to start working as a prostitute. A. is shocked and initially refuses, but after being subjected to both psychological and physical violence she submits. He threatens her with things like throwing her out of a window, sending naked photos of her to her parents via social media, and hurting her family, whose home address he knows as he picked A. up from her house in Romania. He organises for her to work as a prostitute in Munich, where A. has to register as a sex worker with the Local Administrative Office. The staff there notice signs that she is being coerced and call the specialised counselling centre Jadwiga.

In addition to using these technological tools, perpetrators also control trafficked persons by issuing threats and exerting pressure on them via social media. According to the specialised counselling centres, this has become the norm, especially in cases where the trafficked persons were recruited online in the first place. If trafficked persons begin to resist exploitation or say they want to stop, perpetrators use the internet as a way of threatening them. 'I'll put your photos online, I'll tell your family what you're doing' (specialised counselling centre interview) are common threats issued by perpetrators in order to bend trafficked persons to their will. In addition, perpetrators regulate the use of the internet by trafficked persons and even take over their social media profiles to isolate them even further from their social network.[64]

62 Europol, 2020: *The challenges of countering human trafficking in the digital era.*

63 Council of Europe, 2021, p. 33.

64 Cf. Raets, S., Janssens, 2019.

CASE STUDY FIZ STUTTGART, PART I

SEXUAL EXPLOITATION OF AN ILLITERATE NIGERIAN WOMAN

J. is imprisoned in Nigeria for having sexual relations with another woman. An acquaintance of her family gets her out of prison, although she is unsure whether he has bought her freedom or smuggled her out. It turns out that he wields a certain amount of power there because he is a trafficker. He takes J. from the prison to a hotel in Lagos, which she does not leave for six months. The perpetrator commits acts of severe violence against J. in order to make her more 'biddable'. Whenever she says she wants to leave or refuses to have sex with him, he beats her. During this time, she falls pregnant twice and both times must undergo a forced abortion that is also performed in the hotel. The perpetrator intends to send J. to Europe, where she will be forced to work as a prostitute. However, he suggests that he will actually help her and dangles the prospect of going to school and getting a job there. J. does not understand how she has ended up in the hands of a trafficker, but 'she really had no choice. Given her lack of resources, criminal record and sexual orientation, she had nowhere else to go'.

J. is illiterate. Despite this, she is sent alone on a plane to Europe, where her final destination is Germany. The perpetrator sends her a boarding card via WhatsApp and guides her by telephone throughout the journey. She is given a number to call when she arrives in Stuttgart. The perpetrator also gives J. precise instructions on where and how she should submit an asylum application. Once she has arrived, a procurer from a brothel in Stuttgart takes over control of J. She is forced to work in various brothels and apartments and once again receives telephone instructions telling her to meet yet another person at Stuttgart train station who will collect the money. J. keeps in touch with the Nigerian trafficker by telephone and asks to stop on multiple occasions. She says she had not imagined her life in Europe would be like this. At one point when she refuses to continue working, her family in Nigeria is threatened and ultimately her brother is shot dead. This is the turning point for J. She manages to escape after speaking to a street social worker from a counselling centre for displaced persons and victims of torture, where she receives therapy and is referred on to the FIZ specialised counselling centre. J. changes her mobile number and, since she has no social media profiles, the group of perpetrators can no longer reach her. However, as the trafficker is an acquaintance of the family, he continues his threats of violence against her family in Nigeria.

3.5 DIGITAL VIOLENCE AFTER EXPLOITATION HAS CEASED

CASE STUDY A, PART III

JADWIGA MUNICH – LOVERBOY ON FACEBOOK – PSYCHOLOGICAL ABUSE AFTER THE EXPLOITATION HAS CEASED

A. quickly opens up to one of the counsellors at Jadwiga, tells her about her desperate situation and is taken to secure accommodation. To begin with, she does not want to press charges against the man she refers to as her fiancé. Although A. changes her phone number after two days at the accommodation, the man continues sending her threats on Facebook, and even her mother and grandmother put pressure on A. via messenger to return to him. When the threats against A.'s family in Romania become more serious, she decides that she does want to report him. The man is arrested that same day. During the criminal proceedings, A. initially remains in Germany to testify as a witness. Later on in the proceedings, when she is back in Romania studying and cannot travel to Germany because of the COVID-19 pandemic, she testifies via video call. The court condemns the perpetrator to three years and three months in prison on grounds of attempted sexual exploitation.

When trafficked persons manage to escape their exploitative situation, traffickers' business naturally suffers. They have a strong interest in preventing trafficked persons from giving a statement to the law enforcement authorities, and perpetrators exerting pressure to stop this from happening, e.g. by issuing threats via telephone, is not a new phenomenon. According to the specialised counselling centres, posting naked pictures on social media platforms like Facebook, or even just threatening to do so, is standard practice for perpetrators. What is new, however, is the increased vulnerability of and lack of control over private data. The fact that the trafficked persons often have multiple social media accounts provides additional opportunities for perpetrators. 'Our clients are mostly young women under the age of 30. They will inevitably continue to use the internet after the offence has been committed' (specialised counselling centre interview). As they are so easily contactable, always online and active on social media, it is therefore much easier for traffickers to contact both trafficked persons and their social circle. Although there are not yet any statistics on this aspect for Germany, figures from the Netherlands and the USA indicate that this strategy is employed in one-third of trafficking cases.[65] The fact that trafficked persons tend to be active internet users also means it is necessary to update the protection schemes and ICT codes of conduct in shelters (see Section 8).

According to the specialised counselling centres, however, perpetrators are now going even further in their violation of trafficked persons' privacy in the digital realm. For example, perpetrators create fake profiles in the name of their former victims and contact their families using these profiles. This identity theft, coupled with the exertion of psychological pressure on traf-

65 Cf. Council of Europe, 2022; Polaris, 2018: *On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking*.

ficked persons, represents a new category of offence in relation to trafficking in human beings, but at present the way in which it is handled by the police varies greatly (see Section 6).

It was noted, however, that all of these methods only extend and complete the acts committed by perpetrators; they are not necessarily used in place of other known tactics used by traffickers. For example, a trafficked person may delete their social media accounts after receiving threats online but still receive threats by telephone that indicate that the perpetrator is monitoring them in real life, for example because they can describe the clothes they wore on a particular day. 'This results in a constant state of anxiety. Will they act on their threat? When there are also intimate photos circulating online, the psychological stress for clients is never-ending' (specialised counselling centre interview).

3.6 LIVESTREAMING OF TRAFFICKED ADULTS AS A TREND

When researching for this study, it was only possible to identify one new form of trafficking in human beings that is purely technology-based: livestreaming of sexual violence committed against trafficked adults. This is a phenomenon that has in the past only been observed in connection with child sexual violence. Specialised counselling centres in Germany have already come across cases in which women are forced to perform sexual acts on themselves in front of a webcam as instructed by their traffickers, which is then livestreamed on certain platforms. The traffickers' clients can record the act live and sell it as a pornographic video. The German Federal Criminal Police Office is also aware of this new trend (German Federal Criminal Police Office interview). Today, webcam shows are commonplace in adult pornography. However, clever editing and the use of filters makes it almost impossible for clients to tell whether the person performing in front of the webcam has been forced to do so or not. Other countries, including Cyprus, Spain, Finland and the Netherlands, have also reported that livestreaming featuring trafficked persons is a fast-growing area. In Ireland, a shift has been observed from conventional platforms to 'pay-as-you-go' video chat apps like Escortfans and Onlyfans, which offer both private and public video chat rooms. However, dating apps and social media that are not primarily aimed at sexual services are also increasingly being used for this purpose.[66]

66 Cf. Council of Europe, 2022.

4

THE RELEVANCE OF THE DARK WEB AND CRYPTOCURRENCIES FOR TRAFFICKING IN HUMAN BEINGS

The terms "dark web" and "cryptocurrencies" are often used in conjunction with trafficking in human beings. It is a popular myth that the dark web is a criminal underworld that acts as an important hub for traffickers, who conduct their criminal operations using bitcoins. All three assumptions are incorrect. The use of the dark web is not technically illegal, nor is there any reliable evidence that it is used for trafficking in human beings to any relevant degree. Moreover, cryptocurrencies are not yet widely used in financial transactions in relation to this type of trafficking. In order to provide a general overview of these issues, the dark web will first be discussed in the general context of the internet, and then its relevance to trafficking in human beings will be considered. Then, it will be discussed whether or not cryptocurrencies are used as a form of payment in relation to trafficking in human beings, and finally there will be a brief overview of monetary transfers in cases of trafficking.

4.1 CLEARNET, DEEP WEB AND DARK WEB[67]

The world wide web can be compared to an iceberg (see Figure 2): the internet that most people use in their day-to-day lives is like the 10% of the iceberg that is visible above the water, representing only a small portion of the entire world wide web. This is referred to as the clearnet, visible web or surface web. It includes those areas of the internet that can be accessed using conventional browsers (Chrome, Firefox, Safari etc.) via a search engine (Google, Bing, DuckDuckGo etc.) or by directly entering a URL in the address bar, and which are not subject to any other restrictions.

The remaining 90% of the world wide web, however, can be found under the surface. This is called the deep web. The deep web refers to those areas of the internet that are not indexed for access using conventional search engines. This generally means specific databases or websites dedicated to a certain topic, which are usually unavailable due to access restrictions (login, e.g. online banking, government websites, universities) or economic interests (online shops). In order to access this usually innocuous, password-protected or paid content, you only have to know where to find it. No special tools are required.

67 The following information is based on Fuß, M., 2020: *Forensische Linguistik – Sprachanalyse in Darknet-Foren zu sexuellem Missbrauch und Ausbeutung von Kindern.* ('Forensic Linguistics – Linguistic analysis of dark web forums on sexual abuse and exploitation of children') https://dpt-statisch.s3.eu-central-1.amazonaws.com/dpt-digital/dpt-25/medien/dateien/454/2020_Darknet_Sprachanalyse_ECPAT-kurz.pdf (only available in German); Gdata.at: *Was ist eigentlich das Darknet?* ('What is the dark web?') https://www.gdata.at/ratgeber/was-ist-eigentlich-das-darknet (only available in German).

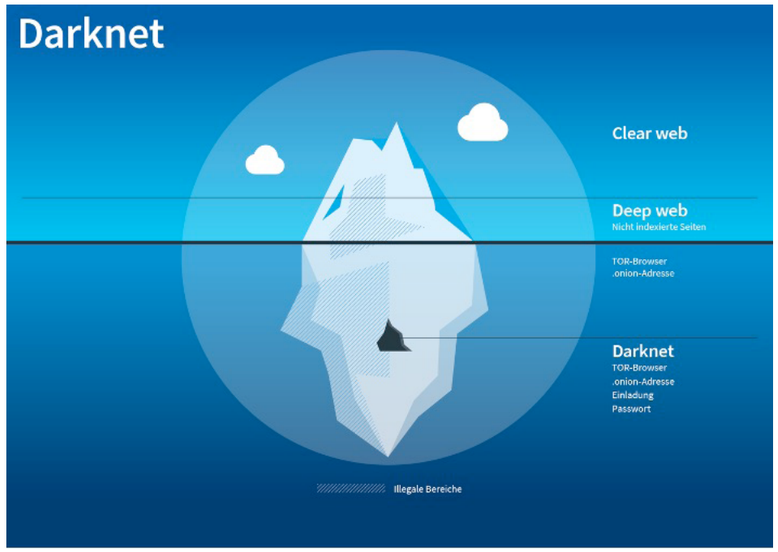

Figure 2: Illustration of the clearweb, deep web and dark web. Source: Gdata.at, *Was ist eigentlich das Darknet?* ('What is the dark web?', only available in German)

As for the dark web, it only forms a small part of the deep web. The terms "dark web" and "deep web" are often used interchangeably, but this is incorrect; they are by no means the same thing. Technically speaking, the deep web functions in the same way as the normal clearweb above the surface. The dark web, on the other hand, requires encrypted access, as it communicates and functions using its own protocol, called onion routing.

4.2 THE TOR NETWORK

Onion routing does not create a direct connection between two communicating end devices (computers) but relays traffic through a sequence of devices referred to as "onion routers". Each onion router can only identify the previous and subsequent router, meaning that the connection between the sender and the recipient remains anonymous. In simple terms, data traffic is directed via multiple servers and is encrypted at each stage.

The dark web cannot be accessed using a normal browser. Instead, a special browser is required that allows communication with the onion routing network. The most well-known of these is probably the Tor browser, short for "The Onion Router", a reference to the many layers the data must penetrate, like the layers of an onion. This browser is freely available from the homepage of the Tor project.[68] On the surface, the Tor browser looks like any normal browser used to surf the internet as we know it.

However, if you want to actually explore the dark web, the next step is usually to open one of the many available "hidden wikis", a kind of dark-web-specific search engine. Hidden wikis are a type of catalogue that compile various addresses on the dark web. Dark web addresses do not

68 Tor project: https://www.torproject.org/

have normal names, like Google's web address google.com; instead they consist of essentially meaningless character sequences that always end in ".onion" (e.g. 93hgh2vbia92gd874hnaob.onion). These addresses can only be accessed using a browser that can connect to the onion routing network.

It is not technically illegal to use the dark web, it just depends what you do there. Since it was introduced in the mid-90s, Tor has also been used by activists, opposition groups and journalists as a platform and tool to circumvent censorship in their home country, access geo-blocked content and communicate anonymously with like-minded people, for example during the protests that took place as part of the Arab Spring.[69] Even renowned news services and social media platforms provide ".onion" versions of their websites, including Deutsche Welle, BBC News, Twitter and Facebook.[70] However, the anonymity of the dark web also offers protection for criminals and fraudsters, making it a popular marketplace for illegal activities. The most commonly available goods and services are illegal drugs, weapons, forged identity documents and visas, contract killings, viruses and malware. One of the biggest areas of the dark web concerns child sexual violence and online content depicting that abuse, either by way of specific forums for sharing images of abuse, livestreaming of sexual violence of children or advertising of children for sexual violence outside of the digital realm.[71]

4.3 TRAFFICKING IN HUMAN BEINGS ON THE DARK WEB

Contrary to expectations, the dark web still does not play a significant role in trafficking in human beings, as recent findings demonstrate.[72] If we bear in mind that trafficking in human beings, especially for the purpose of sexual exploitation, is a business based on supply and demand and that traffickers therefore want to reach the widest possible customer base, the dark web is not actually that suitable for their purposes, nor is it particularly useful for finding potential recruits. In the case of niche markets like organ trafficking, however, the dark web is indeed a relevant marketplace.[73]

The interviewed stakeholders in Germany confirm that this is the case. Unlike with respect to online child abuse content, the German Federal Criminal Police Office does not have any evidence of the use of the dark web for trafficking in human beings for the purpose of sexual exploitation. Nor have the specialised counselling centres yet identified any cases in which trafficked persons have been advertised or exploited on the dark web, though there is a degree of uncertainty: 'We can confirm that we aren't aware of any such cases, but not that the dark web is never used to these ends.' 'We tend to operate more in the offline realm. It's possible that we just don't know about [the involvement of the dark web]' (specialised counselling centre interviews). Indeed, it is questionable whether trafficked persons would even know if the perpetrators had used the dark web as a platform for advertising the services of those they exploited.

69 Federal Agency for Civic Education, *Der Arabische Frühling und seine Folgen.* ('The Arab Spring and its consequences', only available in German).

70 Alec Muffet, *Real World Onion Sites,* 2022.

71 Kaspersky: *Was ist das Darknet?* ('What is the dark web?') https://www.kaspersky.de/resource-center/definitions/darknet (only available in German); Council of Europe 2022.

72 Council of Europe 2022; Stop The Traffik, 2018: *Human Trafficking and the Darknet: Insights on supply and demand.*

73 OSCE 2020; Reid, R., Fox, B., 2020: *Human Trafficking and the Darknet: Technology, Innovation, and Evolving Criminal Justice Strategies.*

4.4 CRYPTOCURRENCIES, BITCOIN AND BLOCKCHAIN

On the dark web, illegal services are normally paid for using cryptocurrencies, the most well-known of which is bitcoin. Cryptocurrencies are digital means of payment based on blockchain technology. Blockchain technology makes it possible to manage data in a distributed, decentralised network by consensus. It works by grouping data into blocks, which are linked together in an ever-growing chain, known as a blockchain. Cryptographic mechanisms ensure that files in the blockchain are uneditable and therefore immune to manipulation.[74] Their ability to be directly, quickly and transparently transferred means that cryptocurrencies do not involve centralised oversight, which is one of the biggest differences between them and traditional financial systems like banks.

Credit is transferred between two users in the form of a computer code. Such transfers are documented in the blockchain via a cryptographically signed transaction in which only the addresses of the user and sender are recorded. These addresses do not reveal the identity of the bitcoin, the users or the senders – they only identify the relevant transaction. Users and senders are connected by means of a "wallet". Wallets hold private keys that function somewhat like passwords and allow individuals to distribute bitcoins to wallets.

Bitcoin was designed as an open-source currency that does not belong to and is not controlled by any one person, company or government. Although it is technically possible for users to be linked to an address by investigating transactions in a blockchain, bitcoins are generally regarded as a hard-to-trace currency that therefore offers anonymity.[75] It goes without saying that this anonymity is highly desirable for those pursuing illegal activities on the dark web.

4.5 MONETARY TRANSFERS IN CASES OF TRAFFICKING IN HUMAN BEINGS

In the case of trafficking in human beings, cryptocurrencies appear to be less frequently used than traditional monetary transfer methods like Western Union' or MoneyGram.[76] 'In other words, the main caveat of cryptocurrency-backed money laundering seems to be that 'you have to have at least some faith in that whole blockchain technology [...]. As a corollary, technological advancements like Bitcoin, while facilitative of trafficking activities, are not necessarily promptly incorporated into the human trafficking modus operandi [...]. '[77]

The German Federal Criminal Police Office has only identified a small number of bitcoin transactions related to trafficking in human beings. For example, according to some investigations, perpetrators of offences in connection with serious and organised crime such as trafficking in human beings, smuggling and money laundering normally use the "Hawala" banking system.

74 Federal Office for Information Security, *Blockchain & Kryptowährung* ('Blockchain and Cryptocurrencies'). https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html

75 Cf. Reid, Fox, 2020.

76 Cf. Council of Europe, 2022.

77 Raets, Janssens 2019, p. 225.

Hawala is not a specific method for transferring money; it describes a form of informal value transfer system based on trust.[78] When international travel became almost impossible during the COVID-19 pandemic in 2020 and hawala was no longer an option, payments in connection with Nigerian trafficking cases were instead made in bitcoins (German Federal Criminal Police Office interview).

The most recent international findings indicate that messaging apps like WeChat are also used to make payment transactions in connection with cases of trafficking in human beings, and further technological developments in this direction are possible.[79]

5

CURRENT REGULATORY FRAMEWORK RELEVANT FOR TECHNOLOGY-FACILITATED TRAFFICKING IN HUMAN BEINGS

5.1 INTERNATIONAL REGULATORY FRAMEWORK

Need to reform the EU Anti-Trafficking Directive

EU Directive 2011/36/EU of 5 April 2011 on preventing and combating trafficking in human beings and protecting its victims[80] is a key anti-trafficking instrument in Germany and Europe. Its implementation has among other things had a positive impact on national legislation and led to coordination and referral mechanisms being set up to facilitate the collaboration between all relevant stakeholders and promote cross-border co-operation.[81] Despite significant improvements, the European Commission's progress report[82] on the implementation of the Directive, for example, reveals that '[...] the decade-old instrument may not be fit for purpose any longer. Despite prevention initiatives undertaken, the demand for using exploited victims' services has not been reduced. The impunity of perpetrators in the EU persists, and the numbers of prosecu-

78 German Parliament, Journal 19/16763, 19th Electoral Period, 20 January 2020. Response of the German Federal Government to a brief enquiry from Members of Parliament Ulla Jelpke, André Hahn, Gökay Akbulut, other Members of Parliament and DIE LINKE parliamentary group. Journal 19/16101 – *Nutzung des Hawala-Systems durch organisierte Kriminalität und terroristische Gruppierungen* ('Use of the hawala system by organised crime and terrorist organisations', only available in German).

79 Cf. Council of Europe, 2022.

80 DIRECTIVE 2011/36/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 05 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA.

81 *EU roadmap on the implementation of the strategy to tackle organised crime,* Roadmap – Ares(2021)1264557.

82 REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, COM(2020) 661 final of 20/10/2020.

tions and convictions of traffickers remain low.'[83] The economic and social impact of COVID-19 has only compounded this issue.[84] Support services find it difficult to reach those affected, whose situation has not only worsened due to COVID-19 but also entails additional risks in view of the recession expected in the wake of the pandemic.[85] As the minimum requirements may no longer be sufficient to protect and support trafficked persons, the European Commission concludes that it must '[…] propose revising it to make it fit for purpose' based on the findings of an evaluation of the implementation of the Directive.[86] The reform process is due to begin in 2023.

EU STRATEGY ON COMBATTING TRAFFICKING IN HUMAN BEINGS 2021–2025 – overview and assessment by the German NGO Network against Trafficking in Human Beings – KOK[87]

KOK's position is that the implementation of many aspects of EU Directive 2011/36 is insufficient. Although Germany has implemented the provisions regarding other forms of exploitation adding corresponding criminal offences to legislation, it has failed to take measures to bolster prevention and especially the protection of trafficked persons taking into account the gender perspective. And yet implementing exactly those provisions is crucial to improving the situation of those affected in Germany and elsewhere. In its Strategy on Combatting Trafficking in Human Beings 2021–2025, the European Commission explains that it continues to help Member States implement the Directive (for example through targeted funding), especially regarding those aspects pertaining to gender and children. However, a better prioritisation of the provisions on the rights of affected individuals and measures to strengthen civil society in Member States is called for.

Addressing the impact of digitalisation: the EU Strategy on Combatting Trafficking in Human Beings 2021–2025 and to Tackle Organised Crime 2021–2025

The digitalisation of criminal activities is another key aspect presented by the European Commission as explaining why some existing legal instruments may have limited impact, with criminal networks adapting more quickly to new social and economic realities than law enforcement and judicial authorities: 'While criminals have managed to take advantage of the latest capacities offered in the digital era, law enforcement faces major challenges keeping pace, including detecting signs of exploitation in the increasing magnitude of online advertisements and obtaining crucial digital evidence.'[88] Based on the legal and policy framework defined by the EU Anti-trafficking Directive, the EU Commission has published a Strategy on Combatting Trafficking in Human Beings

83 *EU Strategy on Combatting Trafficking in Human Beings 2021–2025.*

84 *EU roadmap on the implementation of the strategy to tackle organised crime,* Roadmap – Ares(2021)1264557.

85 REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, COM(2020) 661 final of 20/10/2020.

86 *EU Strategy on Combatting Trafficking in Human Beings 2021–2025.*

87 KOK, 02/06/2021. https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/images_web/_Kommentar_zur_neuen_EU-Strategie_zur_Bekaempfung_des_Menschenhandels__2021-2025__.pdf (only available in German).

88 *EU Strategy on Combatting Trafficking in Human Beings 2021–2025,* p. 13.

2021–2025.[89] One of the aims set out by the Strategy is to destroy the criminal business model of traffickers, be it online or offline. More specifically, it focuses on online recruitment, intermediation, exploitation and threats with regard to minors in order to ensure prosecution of '[…] those who exploit minors for forced criminality; those who use or threaten with violence against victims and their families, or mislead victims by simulating to officialise the exploitation; those who recruit and advertise victims online, and are serviced by brokers providing digital services'.[90]

In order to destroy the increasingly digital model used by traffickers, the Strategy focuses on capacity building by systematically training law enforcement and judicial authority staff on how these technologies and social media work, what role they play and how they are used, among other things. Authorities should be equipped to offer '[…] a modern law enforcement response to technological developments.'[91] Another of the Strategy's priorities is to encourage closer co-operation between law enforcement authorities and the legal system in cross-border and international cases. Another plan is to remove some of the burden from witnesses by accepting digital evidence in criminal proceedings more readily than in the past. As a consequence, the proceedings would no longer hinge mainly on their testimony. Europol would also be able to offer more help to uncover online content used by perpetrators. The measures set out in the EU Strategy to tackle Organised Crime 2021–2025[92] are also closely related; they include legislative provisions and aim to improve collaboration between law enforcement authorities but also to enable monitoring of illicit financial flows.

THE EU STRATEGY ON COMBATTING TRAFFICKING IN HUMAN BEINGS 2021–2025 – summary and assessment by German NGO Network against Trafficking in Human Beings – KOK[93]

The EU Strategy aims to improve the collection and disclosure of data and information as part of the cross-border prosecution of perpetrators. One point, however, that was not sufficiently addressed is data protection, a safeguard seen as absolutely crucial by KOK if more data is to be collected and shared. 'Such measures are at great risk of being misappropriated, and could be detrimental to the right to privacy and protection of trafficked persons. With regards to data security, the EU would have been well advised to highlight once again the need to establish independent national rapporteurs or similar mechanisms, which were provided for in the Anti-Trafficking Directive but have not yet been implemented by some countries, including Germany. A planning and trial phase for establishing such a rapporteur within the German Institute for Human Rights (DIMR in German) was launched in 2021, with its official launch planned for late 2022.

89 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS. The EU Strategy on Combatting Trafficking in Human Beings, COM(2021) 171 final, 14/04/2021. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0171&from=EN

90 *Council conclusions setting the EU's priorities for the fight against seriousand organised crime for EMPACT 2022–2025,* Brussels, 12 May 2021 (OR. en), 8665/21, p. 6. https://data.consilium.europa.eu/doc/document/ST-8665-2021-INIT/en/pdf

91 *EU Strategy on Combatting Trafficking in Human Beings 2021–2025,* p. 13.

92 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021–2025, COM/2021/170 final.

93 KOK, 02/06/2021. https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/images_web/_Kommentar_zur_neuen_EU-Strategie_zur_Bekaempfung_des_Menschenhandels__2021-2025__.pdf (only available in German).

Electronic evidence: the Second Additional Protocol to the Cybercrime Convention

As shown in the previous sections, perpetrators use social media platforms and other electronic service providers to perform their criminal activities, e.g. to find potential recruits, to unleash psychological and image-based violence through digital means or to distribute child sexual abuse material. However, when using modern ICT, perpetrators also leave behind digital trails, such as IP addresses that can prove very useful in criminal investigations into cases of trafficking in human beings. To date, the Council of Europe Cybercrime Convention (also known as the Budapest Convention, dating back to 2001) is the only international agreement specifically addressing cross-border action against online crime (see Section 2). Its aim is to harmonise criminal legislation in relation to cybercrime, to provide instruments for use in criminal proceedings to prosecute any crime committed using a computer system and to promote efficient international collaboration.[94] However, ICT developments also mean that legal solutions must now be found to problems that simply did not exist back in 2001. According to the European Commission, over half of all criminal investigations now entail cross-border requests for access to electronic evidence such as text messages, emails or data from messaging apps.[95] To respond better to these changes, the Council of Europe drew up the Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence after four years of negotiations. It has been open for signature since May 2022.[96] As in the two EU strategies mentioned above, the second Additional Protocol provides for measures to improve international collaboration between law enforcement and judicial authorities, mutual assistance between authorities and co-operation and information exchanges between authorities and private service providers (including with countries outside the EU) to secure electronic evidence. Because evidence is a key factor in any criminal proceedings, ensuring cross-border access by law enforcement agencies to data stored (for example data from a person's social media accounts) that can then be used as electronic evidence is of paramount importance in combating cybercrime and therefore trafficking in human beings.[97] The Additional Protocol also includes safeguards to protect personal data as well as a system that guarantees human rights and the rule of law.[98]

Online service providers and platform operators to step up to their responsibilities

The 2000 e-Commerce Directive[99] is seen as a milestone in terms of regulating digital services. Since it came into force over 20 years ago, new possibilities for doing business and offering internet-based services using ICT have emerged. Although this has brought significant benefits, it has also created new challenges and risks that are not covered by the existing regulatory framework. Because of this, platform operators and online service providers have rarely been held accountable for content published via their services, even if these were illegal. This is why the European Commission has deemed it necessary to expand the regulatory framework and to introduce new regulations to ensure the internet is a safe place for all in Europe. In December 2020, it proposed a comprehensive new package including the Digital Services Act (DSA)[100] and the Digital Markets Act (DMA)[101]. The latter provides for harmonised obligations and prohibitions for systemically important platforms with significant market power in the EU (known as 'gatekeepers'). Due to its limited relevance for this study, it will not be examined in further detail.

The DSA accounts for the fact that the digital realm cannot be or remain unregulated and in a legal vacuum. The new regulations mainly aim to protect users' fundamental rights, to combat illegal content and misinformation, and to create a common and solid framework across the EU to ensure online platforms and electronic providers operate transparently and are held accountable. Providers of electronic services help users access goods, services and content in the digital realm, which is why they should shoulder significantly more responsibility than they have done in the past. The same goes for stakeholders acting as online middlemen, such as internet service providers, as well as operators of cloud and messaging services, market places or social networks. Hosting services and especially online platforms such as social networks, platforms for sharing content, app stores, online market places and online ride-share and accommodation booking platforms are subject to specific due diligence requirements. The provisions are proportionate to the type of services offered and the volume of users. Very large online platforms and search engines with at least 45 million users in the EU or used by 10% of the population are required to comply with stricter rules than start-ups, for example. In future, they will have to carry out risk reduction analyses taking into account risks such as digital violence against women, spreading illegal content or material harmful to young people. All measures must be carefully weighed against restrictions of freedom of expression. These activities will be monitored in the form of independent audits of such risk management measures.

The new rules include EU-wide provisions to identify, report and delete illegal content and specifically aim to ensure minors are protected on all platforms within the EU. If, for example, the operator of an online platform obtains knowledge of a past, current or planned serious offence threatening somebody's life or security, they must immediately report this to law enforcement or judicial authorities and provide all necessary information. All platform operators will also be required to enforce a principle known as *notice and takedown*, whereby they will have to delete any illegal or infringing content from their platforms within a certain period after being notified of this content, which will empower targets of image-based violence. The document still provides no obligation to monitor or to actively seek out information transmitted or stored on the platform pointing to illegal activities, as was already the case in the e-Commerce Directive. [102]

On 23 April 2022, the European Parliament and the Council reached an agreement on the provisions of the DSA and DMA.[103]

94 Cf. German Bundestag, *Kurzinformation: Die Budapest-Konvention (Cybercrime-Convention) – Aktueller Stand der Verhandlungen zum Zweiten Zusatzprotokoll des Europarates* ('Overview of the Budapest Convention (Cybercrime Convention) – status quo of negotiations on the Council of Europe's Second Additional Protocol', only available in German).

95 European Commission 2019: *E-evidence – cross-border access to electronic evidence.*

96 *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and the disclosure of electronic evidence,* 12/05/2022.

97 Council of Europe 2022, pp. 92 et seq.

98 See Council of Europe – Cybercrime. https://www.coe.int/en/web/cybercrime/opening-for-signature-of-the-second-additional-protocol-to-the-cybercrime-convention

99 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('E-Commerce Directive').

100 European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)).

101 European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)).

102 BVDW. Digital Services Act/Digital Markets Act; EU Commission, Press release published on 23/04/2022. 'Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment.'

103 Press release, 05/07/2022. 'Digital Services Package: Commission welcomes the adoption by the European Parliament of the EU's new rulebook for digital services.'

The Digital Services Act is in line with other European legislation, in particular with the Proposal for a Regulation laying down rules to prevent and combat child abuse (2022)[104] that, in turn, is consistent with the EU strategy for a more effective fight against child sexual abuse (2020)[105] and the comprehensive EU Strategy on the Rights of the Child 2021–2024[106]. What this means in practice is that online service providers will now be required to uncover and report any child sexual abuse material or related acts of which they become aware to the authorities. This is a relevant step to protect minors advertised for sexual exploitation on dedicated websites. However, the draft does not include any other human rights provisions.

Under the current EU Strategy on Combatting Trafficking in Human Beings, the European Commission will engage with relevant internet and technology businesses beyond the Digital Services Act and support similar engagement at the national level to address the use of online platforms to recruit and exploit trafficked persons. 'Cooperation with the private sector is therefore encouraged to harness innovation and expertise for the development of technology-based solutions to support prevention and combatting of trafficking in human beings. Prevention and awareness-raising activities on the safe use of the internet and social media, among others, could further contribute to mitigating the risk of child trafficking.'[107]

Vague age verification carried out on a voluntary basis by platform operators

Another point that is unclear is how age verification will be carried out in practice by online platforms. The Digital Services Act provides for 'targeted measures to protect the rights of the child, including age verification and parental control tools, tools aimed at helping minors signal abuse or obtain support, as appropriate' (Article 27). This point is also included in the EU strategy for a better internet for kids (2022, BIK+)[108], according to which the Commission will promote an EU code on age-appropriate design, which will build on the new DSA provisions and should comply in particular with the new EU General Data Protection Regulation (GDPR)[109]. The code will aim to protect the right to privacy and safety of children when using digital products and services. However, any participation in developing and implementing such codes on the part of online platform operators will be on a voluntary basis. Still according to the BIK+ strategy, the European Commission will '[…] will support methods to prove age in a privacy-preserving and secure manner, to be recognised EU-wide. The Commission will work with Member States (who in line with national legislation can choose to issue electronic IDs to the under-18s under the recent proposal on a European Digital Identity), relevant stakeholders and European standardisation organisations to strengthen effective age verification methods, as a priority. This work will encourage market solutions through a robust framework of certification and interoperability.'[110] How effective this plan will be remains to be seen.

104 Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final 2022/0155(COD), 11/05/2022.

105 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – EU strategy for a more effective fight against child sexual abuse.

106 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – EU strategy on the rights of the child, COM(2021) 142 final, 24/03/2021.

107 *EU Strategy on Combatting Trafficking in Human Beings 2021–2025,* p. 11.

108 COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – A digital decade for children and youth: the new European strategy for a better internet for kids (BIK+), COM(2022) 212 final, 11/5/2022.

109 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).

5.2 A BRIEF OVERVIEW OF THE GERMAN REGULATORY FRAMEWORK

Platform operators are not held accountable enough and age verification is either entirely lacking or insufficient: these two fundamental shortcomings have been unanimously criticised by all professionals interviewed as part of this study. 'You're a business. What are you doing to make sure children aren't being raped because of failings on your part? What are these websites doing to protect children?' (OSCE interview). Even on digital market places such as kaufmich.de and other platforms rated as *high-risk enablers* by the German Federal Criminal Police Office, there is no obligatory age verification. 'This must change' (German Federal Criminal Police Office interview). Another problematic phenomenon brought up by the German Federal Criminal Police Office is what is known as "pocket-money encounters" ("Taschengeldtreffen" in German), where young persons proactively offer sexual material and services online for money.[111] These practices occur not only on specialised sites but also on normal service platforms such as markt.de. Corrective measures by the legislator are needed, as highlighted by the Federal Criminal Police Office.

Other than the aforementioned points, the interviewed stakeholders could not name any loopholes in the German Criminal Code that could prevent or hinder the prosecution of trafficking in human beings that involve the use of technology. To date, existing legal provisions seem to adequately cover the support afforded to trafficked persons in this context, bar loopholes that have been known about for a long time and KOK has been calling for to be plugged for many years.[112] The means used to commit the crime as described in the criminal offence itself also cover digital aspects of trafficking in human beings. Furthermore, the use of the internet to facilitate offences has played only a minor role in previous investigations into trafficking in human beings as related offences continue to be mainly carried out offline and therefore require investigations in the real world (German Federal Criminal Police Office interview). From the point of view of law enforcement and judicial authorities, legislation should home in on specific information and communications technologies '[…] to ensure we have some interpretive leeway to include new technologies' (Berlin public prosecutor's office interview). Such a technology-neutral regulatory framework is also the approach recommended by the UN Committee on the Rights of the Child as regards criminal offences committed using new technologies, as mentioning any specific technological programmes or tools in legal documents can be counterproductive. Legal provisions should be worded as broadly as possible and make clear that national legislation covers any technical tool that can be used in any way to subject children to sexual violence and exploitation.[113]

110 *BIK+ 2022,* p. 10.

111 See German Federal Criminal Police Office, *Bundeslagebericht Menschenhandel 2020* ('2020 Situation Report on Trafficking in Human').

112 See KOK list of demands for the 2021 Bundestag elections.

113 See ECPAT International, 2019: *Explanatory Report to the Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.*

Cyberstalking: keeping up with technical developments through Section 238 of the German Criminal Code

One positive aspect to be mentioned is that the German legislator has amended the German Criminal Code to ensure cyberstalking is better covered by Section 238 Stalking[114], that came into force in 2021. The change was justified by technical developments and the resulting increase in cyberstalking: 'Without any specific IT knowledge, perpetrators can use what is known as stalking apps or stalkingware to gain unauthorised access to their targets' email or social media accounts or to data relating to their every movement, thus spying upon their social lives. However, unauthorised access to their prey's data is not the only method used by stalkers: in many cases, they assume their targets' identities on social media, for example, and publish harmful content or photos of them. These very specific modi operandi used in harassment-related offences must be covered by legislation in a more efficient way and with a higher level of legal certainty.'[115] Professionals working for specialised counselling centres, however, are only cautiously optimistic regarding the new version of the section on cyberstalking. If the 2016 reform of legislation on sex offences, which unfortunately has yielded no significant change in women's practical lives over the past five years, is anything to go by, legislative reform alone without supporting measures such as training for judicial staff and additional investigative capacities within the police forces is likely to be insufficient.[116]

6

CHALLENGES AND OBSTACLES

Due to the criminal nature of this issue, efforts to prevent and hinder trafficking in human beings and to support affected individuals are always lagging at least a step behind. As a specialised counselling centre put it aptly, 'Perpetrators have the advantage that they are not working legally, which means that they cross completely different boundaries and can try out new things. They are one critical step ahead and can therefore focus on how to reach their aim more easily' (specialised counselling centre interview). The rapid developments in trafficking in human beings brought about by advances in ICT pose new and urgent challenges for countries. As the UN warns, '[…] future success in eradicating human trafficking, in its many forms, will depend

114 Section 238 of the German Criminal Code (English version): https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p2263

115 Federal Ministry of Justice, legislative procedure, 17 August 2021. Gesetz zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings ('Act amending the German Criminal Code – combating stalking more effectively and improving legal coverage of cyberstalking', only available in German).

116 Bff Interview. For bff's comprehensive examination of the revised version of Section 238 of the German Criminal Code, see its *Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings* ('Position statement on the bill to amend the German Criminal Code – combating stalking more effectively and improving legal coverage of cyberstalking'), 2021. https://www.frauen-gegen-gewalt.de/de/stellungnahmen-1718/stellungnahme-zum-referentenentwurf-eines-gesetzes-zur-änderung-des-strafgesetzbuches-effektivere-bekämpfung-von-nachstellungen.html (only available in German). For more information regarding improving the protection of sexual self-determination, see: https://www.bundesregierung.de/breg-de/aktuelles/mehr-schutz-vor-sexueller-gewalt-393682 (only available in German); you will find a critical interim review here: https://www.deutschlandfunkkultur.de/reform-des-sexualstrafrechts-bilanz-nach-fuenf-jahren-100.html (only available in German).

on how countries and societies are prepared for, and equipped to, harness technology in their responses'. [117]

It should also be noted that ICT is rapidly and ever evolving, which means that cybercrime is too. Whilst some countries have only just begun to build targeted and structured capacities to carry out electronic investigations on the clear web, the first cases of sexual violence in the metaverse are already being reported.[118] Although typologies such as the one presented in Section 2 are useful to identify emerging phenomena, they cannot fully reflect their complexity, reducing them instead to a handful of categories and illustrative characteristics of offences. Due to the rigidity of their categories, these typologies are problematic, as acknowledged by the authors of Figure 1, who point out that future cybercrime classifications could bear less clear-cut delineations and be represented more as a gradual spectrum and/or be based on perpetrators' motives or intents.[119] Because cybercrime is the new normal, classifications must reflect reality in all its complexity whilst also allowing for future developments. The use of advanced technologies such as artificial intelligence, virtual reality or deep fakes has hardly been taken into account in current models and requires further examination.

Obstacles for law enforcement and judicial authorities from an EU perspective

The resulting new requirements for law enforcement and judicial authorities mainly concern two aspects. On the one hand, stakeholders need to be equipped with the necessary technical capacities at the national level to be able to tackle technological challenges and the digital *modus operandi* used by traffickers. On the other hand, systems must be interoperable in order to allow cross-sectoral collaboration.

According to the European Commission, over 80% of all offences committed nowadays have a digital component and even in the case of those committed offline, 'almost every law enforcement officer and prosecutor needs to know the basics of how to investigate crime online'.[120] Law enforcement authorities and public prosecutor's offices that are not specialised in a particular crime urgently need more resources and upskilling. They must have the necessary capabilities, skills and knowledge as regards available tools, services and technologies to keep up, and require the relevant operational know-how, as also pointed out by the European Commission.[121] Knowledge regarding investigative techniques used in special fields such as digital forensics applied to devices and data or using open-source solutions is also deemed insufficient '[…] due to a lack of awareness about what solutions have been developed and are available, differences in require-

117 Inter-Agency Coordination Group against Trafficking of Persons (ICAT). 'Trafficking and Technology: Trends, Challenges and Opportunities.' Issue Brief 7/2019.

118 Bracket Foundation, 2022: *Gaming and the Metaverse. The Alarming Rise of Online Sexual Exploitation and Abuse of Children Within the New Digital Frontier;* Definition of the metaverse: 'The metaverse […] is a virtual space in which users move around in the form of avatars and can have an impact on, and use, virtual artefacts, e.g. when they put on clothing, build or decorate a house, open a door, go out and meet other players and like-minded people there. Just like in the real world, it is possible to live, work, learn, do business, have conversations and build relationships in the metaverse. The term is a portmanteau of 'meta–' ('on a higher step', 'on a higher level') and 'universe'. Depending on the perspective and manifestation, the metaverse can be an expression of virtual reality but also of mixed reality, if some elements of reality, such as a text- of audio-based conversation or physically experienced sexuality are central factors.' (Gabler Wirtschaftslexikon. https://wirtschaftslexikon.gabler.de/definition/metaverse-123520, only available in German).

119 Cf. Forensic Sciences, 2022-2, pp. 393 et. seq.

120 *EU Strategy on Combatting Trafficking in Human Beings 2021–2025,* p. 31.

121 See Commission Communication 'Ensuring justice in the EU — a European judicial training strategy for 2021–2024', COM(2020) 713 final of 2/12/2020, which highlights the need to train professionals to tackle new challenges.

ments and levels of expertise, and a lack of support for further development and maintenance' on the part of authorities.[122]

It must be noted that these shortcomings have serious consequences: according to estimations by the Budapest Convention's Secretariat, only 1% of all cybercrimes are reported to law enforcement authorities and less than 1% of reported cases actually lead to an outcome in the justice system.[123] The clearance rate of just under 30% mentioned in the 2021 *Cybercrime Situation Report* published by the German Federal Criminal Police Office was well below the police crime statistics average.[124]

Even before traffickers started digitalising their modus operandi, cases often required international collaboration between authorities, institutions and other stakeholders, as criminal networks often operate across borders. Yet years after law enforcement and judicial structures were called for under all anti-trafficking instruments, they are not stable enough to adequately deal with the increasing demands in digital investigations. This is due to a lack of resources, coordination and communication. EU agencies such as Europol and Eurojust do help with capacity building as agreed and help coordinate the collaboration between national authorities, but detecting and prosecuting cases of digital trafficking in human beings requires the information systems to be compatible, in line with the current EU Strategy on Combatting Trafficking in Human Beings.

Challenges and obstacles in Germany

The 42 specialised counselling centres that are currently members of KOK offer support to trafficked persons in Germany, in Switzerland and in South Tyrol and carry out vital work to enforce the rights of trafficked persons, often stepping in when public structures fail. They draw their expertise from years of practical work on the ground with clients and collaboration with police forces and policymakers. And yet, they too face challenges due to the digitalisation of trafficking in human beings. They do admit to finding it difficult to adapt to keep in step with the digital realm, but also identify other obstacles in different areas of society that impact their anti-trafficking efforts. The observations were supplemented by information from law enforcement and judicial authorities and served as a basis to identify the key shortcomings and obstacles in Germany below.

Understanding the topic and developing new approaches: a process that has only just begun

'I think everything has only just begun in Germany. As you see, even we are still finding it difficult to grasp this issue despite our experience in this area. I think it must be given greater prominence.' 'We're quite clueless really. We know too little about online and digital aspects of trafficking in human beings.' These two quotes by specialised counselling centres pretty much sum up the situation faced by practitioners working for counselling centres in Germany, but also by police forces, as suggested by counselling centres based on their experience. Whilst specialised counselling centres tend to identify, and react to, new trends and forms of trafficking in human beings fairly quickly, e.g. by offering additional services for specific target groups such as

122 *EU Strategy on Combatting Trafficking in Human Beings 2021–2025,* p. 31.

123 Cf. Council of Europe, 2021, p. 12.

124 Cf. German Federal Criminal Police Office, *Bundeslagebild Cybercrime 2021* ('2021 Cybercrime Situation Report', only available in German).

women and children refugees, the impacts of technologies on trafficking in human beings have often been underestimated or seen as a separate topic in the context of the broad range of topics covered by specialised counselling centres. 'Until recently, I thought it was enough to send two counsellors to a training course so they knew about [technology-facilitated trafficking in human beings]. But I think that's not the right way to go about it. We must see this as a cross-cutting issue that all [counsellors] need to know about as it extends to all areas' (specialised counselling centre interview).

Lack of awareness on the part of society and authorities about digital violence

The various forms of digital psychological and sexual violence are a fairly recent phenomenon; there can be overlaps and they often have no clear-cut legal definition.[125] Whilst some of these forms of violence seem to have seeped into the consciousness of the media and, therefore, of the broader public, there is a lack of understanding for others. To illustrate this, the NGO bff gives the example of hate speech as one of the better-known forms of digital violence as compared with online stalking: 'Violence within relationships and sexual violence are much more of a social taboo than hate speech. In the case of hate speech, most people understand easily that it is wrong for a female journalist or academic to be threatened for doing her job, for example. But as soon as we're talking about an ex who feels wounded and starts stalking his ex-girlfriend, people find it more difficult to feel solidarity for the target, meaning that they excuse this type of behaviour' (bff interview).

In cases of trafficking in human beings in which perpetrators exert pressure on their targets online, specialised counselling centres have complained about a lack of awareness among authorities in their collaboration with police forces. They do not always take the threat seriously and when victims try to report being put under pressure online, the response often tends to be something along the lines of: 'Just switch your phone off, what's the problem? The [perpetrator] isn't even here, he can't do anything to you.' These issues are also addressed in a Council of Europe report (2021): 'In cases of online and technology-facilitated violence against women, being heard and believed by trained law-enforcement officers is a challenge in many countries. […] Most law-enforcement officers are not trained to recognise the different types of violence affecting women and girls online and many of them do not know how to handle these procedures. This lack of training affects women's ability to effectively file complaints.'[126] Or, as a specialised counselling centre puts it aptly: 'At the moment, it's more a question of whether the individuals happen to end up talking to the right person' (specialised counselling centre interview).

Difficulties related to the burden of proof and securing digital evidence

When affected individuals continue to be threatened by perpetrators after exploitation has ended and wish to report their ordeal to the police, experience has shown that they often cannot provide enough information for the police to see sufficient grounds for initial suspicion. If the traffickers are issuing no clear threats (such as physically standing on the doorstep) and if affected individuals are 'only' put under pressure online using fake profiles, police forces often cannot trace suspected online offences back to specific traffickers. The burden of proof lies with the targets, the problem being that they are not always aware of this and may fail to secure digital evidence (e.g. screenshots) before it is deleted by perpetrators, particularly since not all

125 Cf. Council of Europe, 2021, p. 11.

126 Council of Europe, 2021, p. 11.

trafficked persons have the IT skills to do so. They can rarely rely on adequate support from specialised counselling centres: 'I don't even know what law enforcement authorities need. What remains in the digital world once an account has been deleted?' (specialised counselling centre interview).

Securing digital evidence requires an awareness of the situation on the part of persons subjected to serious exploitation, but also a certain presence of mind. In some cases, affected women had taken photos of places and street names with their phone, for example, which they had kept and proved useful and relevant during criminal proceedings. However, specialised counselling centres point to a more serious aspect of the fact that the burden of digital proof lies with victims, namely in the case of uneducated or even illiterate targets who have a poor command of ICT. 'The less educated a woman is, the more dangerous her situation, as the evidence and her credibility down the line will suffer during criminal proceedings. Everything remains very vague' (specialised counselling centre interview). The crux is to be able to prove to the court that force has been used against the trafficked persons despite traffickers chiefly operating online, as in the call-centre example in Section 3. 'In cases of trafficking in human beings, the use of force often comes into play on a personal level, behind closed doors, with perpetrators exerting pressure on the women. It rarely happens over WhatsApp or voice messages. This is why I need personal evidence, i.e. the victim's testimony. We have already started doing more telecommunications surveillance, reading through chats and listening in on phone calls. The problem is that perpetrators obviously don't talk about these things over the phone', as explains the Berlin public prosecutor's office specialised in trafficking in human beings. This is why telecommunications data can indeed usually be used as evidence but cannot serve as a proof of the use of force. This is also illustrated by other examples from German-speaking countries where a criminal case could successfully be brought against traffickers because of law enforcement authorities' willingness to use audio recordings as well as social media messages and posts to reconstruct working hours and conditions, transport and logistics, daily income and the permanent control, threats and abuse the individual was subject to. In these cases, digital evidence supported the victim's testimony but could not have replaced it.[127] It should be noted that this is sometimes seen as an obstacle by law enforcement authorities and that the German Federal Criminal Police Office has been working on the use of evidence that does not depend on individuals in cases of trafficking in human beings with digital elements since 2018 as part of its "THB Liberi" project with partners.

Tackling image-based violence is not only a technological matter

A harrowing factor for women and minors advertised on specialised websites for the purpose of exploitation is the fact that even after the exploitative situation has ended, intimate images of them may still be circulating online. The same goes for affected individuals of whom perpetrators have posted naked images to exert pressure on them. To date, there is no good way of finding such images or to ensure they can no longer be found online. Some hash-value-based solutions do

127 See Chen, I./Tortosa, C.: 'The Use of Digital Evidence in Human Trafficking Investigations.' In: Anti-Trafficking Review, No. 14, 2020, pp. 122–124. https://doi.org/10.14197/atr.201220149

exist, but they will only detect known pictures.[128] There are also publicly available facial recognition software programmes such as PimEyes[129], but they raise many new ethical issues with regard to data protection, freedom of expression and digital surveillance.[130] 'All tools have their issues when used only automatically with no human oversight. [...] We will definitely need a solution to image-based violence that is reliable and complies with data privacy' (bff interview). Currently, specialised counselling centres are left with no other solution than to help their clients accept the situation: 'I must accept that these images are out there.' Yet technological approaches alone will not solve the problem and should not deflect our attention from the fact that these forms of violence must be addressed in a much broader context. 'If I were to prioritise, I would say that sufficient funding for specialised counselling centres and well-trained prosecution offices and police forces are a thousand times more important than developing a good reverse search engine, for example' (bff interview). In the end, the ultimate aim should be to prevent anyone having to experience these forms of violence. In order to do this, we will need more than effective software capable of finding intimate images online. What we need is to create a social environment in which perpetrators know that the law will definitely be enforced.[131] The Berlin public prosecutor's office believes action can often be taken if naked photos are published by perpetrators against the will of trafficked persons as this offence can at least be punished by way of fines on grounds of blackmail, threat or attempted coercion. 'Obviously, the penalties that can be handed down for blackmail, threat or coercion are far below those on grounds of serious trafficking in human beings or forced prostitution, but at least these concurrent offences are also taken into account during sentencing' (Berlin public prosecutor's office interview). But once again, the facts must be proved in order to bring charges against, and prosecute, the perpetrators.

Lack of IT skills and anxiety using social media on the part of specialised counselling centres

Specialised counselling centre staff usually include social workers, social scientists and psychology experts who have minimal IT skills, and most KOK counselling centres are small organisations that do not have an IT department and that only resort to external IT specialists when necessary. The lack of knowledge pertains to all technical and technological aspects, from basic awareness of IT security matters on the part of counsellors and their clients to knowing how to secure digital evidence. 'Perpetrators exploit gaps and this is something we have to keep in mind when using digital tools. In which situations should we be careful and protect ourselves using technical means and how?' (specialised counselling centre interview) Attacks on special-

128 A hash value is a digital code comprising figures and letters. In a nutshell, it can be seen as a sort of 'fingerprint' of a picture. Lists with known hash values are used to detect child sexual abuse material on web services run by Microsoft, Google, Facebook, Twitter, Adobe Inc. and other companies reporting any suspicions to competent authorities. The most well-known tool, which is also used in Germany, is PhotoDNA by Microsoft. 'The picture is converted into a black-and-white format, reduced in size and divided into smaller squares. Each of these pictures is scanned to find the strongest gradient. Taken together, the gradients of all pictures result in the *PhotoDNA*.' (https://www.wikiwand.com/de/PhotoDNA, only available in German).

129 PimEyes: https://pimeyes.com/en

130 For a critical assessment of tech tools used to combat trafficking in human beings, see also the Anti-Trafficking-Review No. 14, 2020 'Special Issue – Technology, Anti-Trafficking, and Speculative Futures'. https://www.antitraffickingreview.org/index.php/atrjournal/issue/view/22. Milivojevic, S., Moore, H. and Segrave, M., however, call for caution when it comes to facial recognition: 'Alongside the latest version of raid and rescue, we have also seen the rise in facial recognition flagged as a technology that can assist in the identification of victims of trafficking and slavery. Concerns about the limits and consequences of such technology are silenced by the overwhelmingly moral imperative to 'protect and rescue'. The power of this moralising discourse is such that it is untroubled by the absence of evidence to support this position (or indeed, the mounting evidence that casts doubt on the accuracy of this position).'

131 See also Thomas-Gabriel Rüdiger's *broken web theory,* especially his 'broken web phenomenon'. In: Jur@ im Netz, December 2017 (only available in German).

ised counselling centre computer systems do happen from time to time. Training to date has covered chiefly data protection, but more extensive training on IT security is needed and keenly sought: 'Actually, we need everything' (specialised counselling centre interview). bff, an NGO combatting gender-based violence against women, is one of the only stakeholders in this field to offer training courses as part of its project "Aktiv gegen digitale Gewalt" ("Action against Digital Violence"). It has proved so popular among its members that staff can 'hardly keep up with demand' (bff interview).

This lack of IT skills seems to be a generational issue. Older counsellors tend not to be technophiles and are usually more anxious when it comes to using digital media than younger colleagues or interns. Some specialised counselling centres do not have a social media account on grounds of data protection, others get younger counsellors to take care of this unpleasant task, figuring that these *digital natives* grew up with the internet and social media and are therefore automatically more competent. Although implementation in practice is challenging, most specialised counselling centres are aware of this challenge and know they have to do something about it: 'As a counselling centre, we have to do training and educate ourselves to get up to date. But we also need staff and time to really address this issue in depth. Do I want to have a Facebook account? What do I want to do with it? What am I aiming for? How do I want to use it? I you don't use it [in your private life] and aren't an expert, the first hurdle is to get started' (specialised counselling centre interview). In practice, employing counsellors of different generations seems to have been a solution to this issue.

A lack of awareness of technology risks on the part of affected individuals

'I'm always astounded to see how great clients are with apps and knowledgeable they are when it comes to technical matters, but also how carefree they are when they are using them. There is a lack of awareness and mindfulness' (specialised counselling centre interview). Many specialised counselling centres witness that social media are being used with little regard for privacy protection, including by clients living in shelters and under acute threat from traffickers. Some post pictures giving clues as to their surroundings and to their current location, e.g. iconic places in the city. Getting clients to understand the risks entailed and the need to better protect their privacy and the entire shelter's safety has been difficult. This is due, according to counsellors, to a key feature of the relationship between clients and counsellors, namely that building trust takes time. Clients cease to be so distrustful when they see that promises and agreements made with counsellors are indeed helpful. This is also true for any form of support in the digital space: 'The trick is to transfer this to the digital realm' (specialised counselling centre interview).

Social media use can also be unwittingly risky in other ways. One specialised counselling centre, for example, had a situation in which one of its clients decided to repost on her social media account a video depicting child abuse that she had been sent as a deterrent and is now being investigated on the grounds of spreading child pornography. Counsellors also now face new harrowing tasks when they have to watch brutal videos showing a murder or extreme physical violence to secure evidence of the threats a client is receiving from perpetrators.

New dilemmas in digital social work

More and more specialised counselling centres have begun offering services online or doing digital outreach work.[132] The digitalisation of social work requires new skills to be able to use and maintain the relevant technologies but also poses new dilemmas. A case study serves to illustrate this point. A specialised counselling centre is contacted by two 13-year-old girls. They reach out separately and ask for an anonymous online consultation. Grown-up men had been approaching them, in the one case on TikTok, in the other on Twitch, had showered them with compliments and tried to groom them to obtain naked pictures of them using what is sometimes known as the "loverboy" ploy. In one of the cases, the suspect was in Algeria. 'It was clear where this was going. But had we reported it, the girls would have simply disappeared into thin air. This has always been a dilemma in our outreach work. Building trust is very important when working with minors. If we contact the Youth Welfare Office or the police to get clients off the streets, things go awry. In most cases, we don't even know their full identity. If we were to report the case, the children and youngsters would just withdraw and avoid any contact with any outreach worker in future. This hinders any intervention. If the police or the Youth Welfare Office do intervene and bring the victims back home or to a shelter for young people, they usually don't stay for long and end up on the streets again. The authorities are aware of this dilemma. And we don't have enough experience with online consultations to know what to do, as we're not the only ones who are maintaining contact with the girls: the perpetrators are too' (specialised counselling centres interview).

Digital outreach work raises (at least) one other question, namely how to deal with geographic remits and accessibility of services. If a woman that was able to free herself from exploitation phones up as part of outreach work in the real world and asks to be picked up from a specific place, the counsellor will usually go. This work is usually organised at a regional level. Specialised counselling centres do not yet know how to handle situations in their online work when persons from other federal states in a crisis get in touch, for example. It is also unclear whether services will be accessible around the clock.

Relevance of competing issues

However important it is to examine the use of technology in trafficking in human beings, several of the interviewees noted that they are worried that policymakers may be tempted to focus on this subcategory of a broader and much more complex issue and fall prey to what could be seen as a new "fad": 'I'm a bit concerned that if digitalisation receives more attention, the part of our work done offline will suffer' (specialised counselling centre interview). One interviewee drew an analogy with child abuse material: after a number of highly mediatised cases, policymakers caught the bait, funded various projects and adopted measures without there actually being a real political will to promote child protection holistically. This also happened in the spring of 2022 with the topic of trafficking out of Ukraine. While policymakers and society focused on Ukrainians as a risk group, the precarious situation of other vulnerable people who were trafficked or at risk of being trafficked did not change. 'Since the beginning of the war in Ukraine, we've had to remind people that the other issues are still there' (specialised counselling centre interview).

132 Outcomes of an event held by KOK for its members, 06/09/2022.

The slow digitalisation of justice

The slow digitalisation of justice currently represents a considerable obstacle in tackling trafficking in human beings in Germany. In cross-border cases, the prosecution sends written requests for mutual assistance abroad by post. It takes an average of three months to get an answer and several months may have passed by the time charges are pressed, or even longer if additional investigations are necessary. The drawbacks for victims are obvious: 'If a woman is being threatened, three months is an eternity. It's a disgrace they have to wait so long.' For the judiciary, long proceedings can result in them losing their witness '[...] as in this case the woman can no longer be made to testify. It would be possible to accelerate things if we could easily make use of evidence from abroad, e.g. by printing out an email and adding it to the file' (Berlin public prosecutor's office interview). According to the Berlin public prosecutor's office, an electronic file would be a helpful first step, but there is still a long way to go before this is implemented due to the many reservations within the justice system: 'Digitalisation can offer new opportunities for data abuse. This is not the case when you have a "physical" file being passed around. Whilst I understand the concern, technology-facilitated investigations can really help us save time and in cases of trafficking in human beings, time is of the essence.' IT security structures in prosecution offices also make it more difficult to keep pace with technological developments. For example, staff at the Berlin public prosecutor's office cannot simply read USB sticks or data CDs on their own computer and this is probably no different elsewhere in the country. When prosecutors want to familiarise themselves with a new app or piece of software that is relevant for their proceedings, they can only do this with help from the IT department. 'The Prosecution Office is often a step behind perpetrators in this respect' (Berlin public prosecutor's office interview).

7

SELECTED EXAMPLES OF TECHNOLOGY-BASED SOLUTIONS

KOK specialised counselling centres have taken advantage of the pandemic to further digitalise their services, in addition to their normal website. They have bolstered their social media presence and more and more of them have offered online consultations, leading to better reach, improved accessibility for clients because their services have a low threshold and are available regardless of the person's location, and to faster response times on the part of counsellors. A number of specialised counselling centres have also started doing *digital outreach work.*[133] Other than that, no other particularly technical or innovative technological approaches could be identified.

133 Information from an online training course conducted by KOK for its member organisations on 06/09/2022; to see an example of how digital outreach work was implemented in youth welfare work, see https://www.digital-streetwork-bayern.de (only available in German).

The section below shall examine four approaches based on different technological solutions (website, machine learning, virtual reality and app). Technology-based tools are evolving ever more rapidly across the world. Whereas in 2009, only five tools were launched every year on average, since 2015 this has increased to 40.[134] The following examples are merely representative of the wide breadth of available options. This study does not aim to be comprehensive as we hope and expect that the future will bring a greater number of more effective and technically mature tools to tackle trafficking in human beings.

bff's guidelines on combatting digital violence against women

The organisation bff – Frauen gegen Gewalt has launched a special website, "Aktiv gegen digitale Gewalt" ("Action Against Digital Violence")[135] to address the most relevant and well-known forms of violence currently, e.g. cyberstalking, image-based sexual violence and identity theft. The website provides a definition and information about the corresponding criminal offences that could be prosecuted in the case of this particular form of violence as well as recommendations for affected individuals. It also offers a separate section on IT security and privacy with practical instructions on how to secure digital evidence.

Using a webcrawler to crack down on prostitution ads promoting minors: a tool used as part of the "THB Liberi" project by the German Federal Criminal Police Office

Ads for sexual services tend to use specific keywords hinting that the person offering the services could be a minor. This can yield a starting point for police investigations. To avoid having to manually search for such expressions and information, the German Federal Criminal Police Office and now 60 police stations in Germany use a "webcrawler". Simply put, a webcrawler is a computer programme that automatically searches publicly available websites for specific content. The webcrawler currently used by the German police forms part of the new approaches developed by the German Federal Criminal Police Office together with 8 police stations and the Austrian Federal Criminal Police Office since 2018 in the context of "THB Liberi", a project funded by the Internal Security Fund. "THB Liberi" aims to tackle the trafficking and exploitation of minors in Germany and Europe using an improved interdisciplinary approach promoting collaboration between countries, authorities and NGOs. The project has decided to focus on trafficking in human beings using the internet and more specifically the online recruitment of young people and teenagers.[136] The project has been extended to the period from 2023 to 2025 thanks to funding by the National Programme, with internet trafficking remaining its main focus.[137]

Virtual reality as a training ground for future professionals

The Berlin Psychological University has been developing the project ViContact 2.0 in collaboration with its partners, the University of Flensburg and the University Medical Center of Göttingen, since 2018. Now in its second project phase until 2024, it is creating a virtual environment to

134 OSCE, 2020: *Leveraging innovation to fight trafficking in human beings: a comprehensive analysis of technology tools*, p. 23.

135 bff: https://www.aktiv-gegen-digitale-gewalt.de/de/digitale-gewalt/bildbasierte-sexualisierte-gewalt/was-kann-ich-tun.html (only available in German).

136 Kramer, F. 2020: 'Mit THB Liberi organisierten Menschenhandel bekämpfen' ('Combatting organised trafficking in human beings using THB Liberi'). In: Die Polizei, 11-2020 (only available in German).

137 Written information provided by the German Federal Criminal Police Office, July 2022.

train future professionals to question suspected victims of sexual abuse. Its aim is to prepare teacher training students, teachers and people working in child protection to conduct initial discussions with a child suspected to have been subjected to sexual violence. Moreover, the idea is to develop a practical training resource to teach non-suggestive and supportive conversation practices with children.[138] The trainees talk to virtual avatars that look and chat like more or less ten-year-old children. The avatars have memorised content in the form of narrative answers which they reveal if questioned adequately (i.e. using supportive but also non-suggestive and open questioning methods). For the moment, human operators still have to manually code some aspects of the conversation in the background but an AI version is under development. After the talk, the trainees receive automatic personalised feedback. The project is currently in the evaluation phase.

The Police University in Rhineland-Palatinate[139], on the other hand, uses VR glasses as part of police officer training to help them identify potential cases of trafficking in human beings in prostitution locations. Using practice scenarios, trainees can practise what clues to look out for, e.g. during brothel checks. However, the VR scenarios are not AI-based, which means that there is no interaction with the women as they cannot react.

Profitability as a decision-making tool: the Pacific Links app PAXU for preventing labour exploitation

The Pacific Links Foundation, an NGO based in the US and combatting trafficking in human beings in Vietnam, has developed an app that compares alleged job offers and promised salaries abroad with the real costs of living in the country, calculates debt repayments and offers information on required documents with the aim to promote safe migration.[140] Instead of issuing warnings about the risks and danger of trafficking in human beings, the organisation has chosen to focus its work on a cost-benefit calculation, as labour migration is an economic decision. For the moment, the app is only available in English and Vietnamese. It is promoted in online communities on Facebook and in messenger groups.

Besides these technology-based solutions presented here as mere examples, there are a host of other digital or technology-facilitated tools used in anti-trafficking circles worldwide. The Organisation for Security and Cooperation in Europe (OSCE) has worked with the organisation 'Tech against Trafficking' and analysed 300 of these tools in a report published in June 2020.[141]

Technology-based solutions vs. the heart of the problem

Technologies are part of the problem and must therefore be part of the solution. However, they should not deflect attention from the discourse about the societal conditions making trafficking in human beings possible or even worse, e.g. migration policies, inequality, gender discrimination –

138 Tamm, A., Volbert, R., presentation on 10/05/2022: 'Das Projekt ViContact. Befragungen bei Verdacht auf sexuellen Missbrauch – Training in virtueller Umgebung' ('The ViContact project. Questioning in cases of suspected sexual abuse – training in a virtual environment', in German).

139 Rhineland-Palatinate Police University research. https://www.polizei.rlp.de/de/die-polizei/ueber-uns/dienststellen/hochschule-der-polizei-rheinland-pfalz/forschung/ (only available in German).

140 Pacific Links Foundation: PAXU. https://pacificlinks.org/paxu/#Courage

141 OSCE, 2020: *Leveraging innovation to fight trafficking in human beings: a comprehensive analysis of technology tools.*

all these factors must be examined separately from technologies.[142] There is no doubt that measures to combat trafficking in human beings should continue to involve researching and exploring ICT possibilities for prevention and law enforcement and especially to help affected individuals escape the exploitative situation they are in and to offer better protection and support. However, neither the internet nor ICT should be seen as a cause of these crimes or as a silver bullet. More critical research into the impact of technology-based and -facilitated approaches is needed.

Technology-based solutions to help combat trafficking in human beings and support trafficked persons also pose human rights-related risks: they can have a controlling effect on affected individuals, limit their freedom of movement and reduce their agency, the problem being that these rights may be seen as less important than the duty to 'save' them.[143] Using ICT in data-based anti-trafficking action also raises considerable questions with regard to data protection. Since 2012, KOK has worked on two complex issues, data protection and collection and their impact on trafficked persons, with several publications on this topic.[144]

8

RECOMMENDATIONS AND OUTLOOK

This study has examined what needs to be done as well as existing gaps and obstacles experienced by various stakeholders working in Germany to prevent and combat trafficking in human beings and to support affected individuals. A number of fundamental recommendations for policymakers, law enforcement authorities and specialised counselling centres can be derived from these observations.

Policymakers: extending the cybersecurity agenda to trafficking in human beings and introducing a uniform definition

In June 2022, the Federal Ministry of the Interior and Community published its cybersecurity agenda[145]. It included targets and measures for the 20th legislative term and presented the 'cross-sectoral strategic framework for the Government's action on cybersecurity'[146]. Its section on 'Combatting cybercrime and illegal content on the internet' does recommend a string of measures to combat sexual violence against children (including online child abuse material), but tech-

142 Cf. Milivojevic, S./Moore, H./Segrave, M.: 'Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology.' In: Anti-Trafficking Review, issue 14, 2020, pp. 16–32.

143 Cf. ibid.

144 German NGO Network against Trafficking in Human Beings, 2020: *Defining the Gap: Datenerhebung zu Menschenhandel und Ausbeutung in Deutschland – der zivilgesellschaftliche Ansatz des KOK* ('Defining the gap: data collection in the context of trafficking in human beings and exploitation in Germany - KOK's civil society approach', only available in German). https://www.kok-gegen-menschenhandel.de/datenschutz-datact; Uhl, B.: 'Data and responsibility - considerations on datafication, civil society and anti-trafficking action.' In: KOK, 2020: *Trafficking in Human beings - Reflection on Protection and Rights*, pp. 251–259.

145 Federal Ministry of the Interior and Community, June 2022: *Cybersicherheitsagenda* ('Cybersecurity Agenda', only available in German).

146 Federal Ministry of the Interior and Community: *IT- und Cybersicherheit* ('IT and cybersecurity'). https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-und-cybersicherheit/it-und-cybersicherheit-node.html (only available in German).

nology-based trafficking in human beings is not addressed either there or anywhere else in this document. If trafficking in human beings, which is increasingly being committed digitally, is to be comprehensively prevented and tackled, it must be included in the Government's next cybersecurity agenda.

Furthermore the definition[147] of cybercrime used by the Federal Ministry of the Interior and Community is different from that of the German Federal Criminal Police Office, which again differs from that of the Federal Office for Information Security.[148] As shown in Section 2, using different definitions of these criminal offences can hinder the efficacy of measures. A common definition is needed and should be at the base of all measures. Drafting definitions agreed by all stakeholders, especially regarding the digitalised elements of trafficking in human beings, should be done in collaboration with partners from the world of academia, criminal and judicial practice and NGOs.[149]

Policymakers: accelerating the digitalisation of public administration

In order to compete against technology-facilitated trafficking in human beings despite constant evolutions in criminal operations, the Government must accelerate the digitalisation of all public administrations and fully implement plans in this respect such as the Digital Strategy[150].

Policymakers: clarifying responsibilities for technology-facilitated trafficking in human beings and facilitate interdisciplinary collaboration

Although this study focuses on the perspective and experience of the specialised counselling centres, the author did also intend to interview policymakers regarding this issue. Trafficking in human beings and especially the digital dimension of the phenomenon are cross-cutting issues that affect different departments. The responsibilities still need some clarifying.

The Ministry of the Interior and Community has two potential points of contact: the CI 8 Cybercapabilities Department of the German Federal Criminal Police Office, which focuses, however, on online child sexual abuse material and sexual violence against children, and the ÖS II Department that deals with serious and organised crime. Although the latter is indeed responsible for trafficking in human beings, it does not (yet) have any expertise on technology-facilitated aspects of the issue. Discussions regarding potential overlap between these areas were launched in the autumn of 2022 with both departments as part of the German G7 presidency.

147 Federal Ministry of the Interior and Community: 'Definition of cybercrime: cybercrime is a global phenomenon that does not stop at national borders or closed doors. It can occur in any place where computers, smartphones and other IT devices are used, i.e. in businesses, administrations, universities, at home and on the go. 'Cybercrime' is the general term used to refer to criminal offences committed using modern information technology. It can take the form of fraud attempts that reach the potential victim by email instead of post. In a narrower sense, cybercrime refers to criminal offences targeting computer systems and networks, which can include cyber spying or cyber terrorism, among other things.' https://www.bmi.bund.de/DE/themen/sicherheit/kriminalitaetsbekaempfung-und-gefahrenabwehr/cyberkriminalitaet/cyberkriminalitaet-node.html (our translation).

148 Federal Office for Information Security: 'Cybercrime methods: Cybercrime is an umbrella term for all criminal acts that exploit modern information technology and electronic infrastructures. Criminals are coming up with new cybercrimes all the time. As our society becomes ever more digital, new IT applications are making their way into our everyday lives. These new applications inevitably come with some security risks. The most common types of cybercrime include malicious software (and all subtypes) and emotet, identity theft through doxing, spam and phishing, botnets and social engineering.' https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/methoden-der-cyber-kriminalitaet_node.html

149 Similar coordination processes took place during the preparation of the Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse published in 2017 under the leadership of ECPAT Germany.

150 *The Government's Digital Strategy*: https://digitalstrategie-deutschland.de/ueber-die-digitalstrategie/ (only available in German).

This is a promising approach and efforts should be continued. Overall, responsibilities should be more clearly defined and distributed and, where necessary, structures for interdisciplinary cooperation should be created. Failing that, this risks becoming an issue that is, in theory, seen by all as a cross-sectional topic but for which, in practice, nobody feels responsible.

Policymakers: making technology businesses accountable

Websites and platforms used by traffickers to recruit targets are rarely held accountable for their content in Germany. The Government should plug this legislative loophole by introducing accountability and liability mechanisms for tech businesses for any damage resulting from content published on their platform or the use of their platforms.[151]

Policymakers: taking into account IT infrastructure in funding for specialised counselling centres

The state has a duty of protection towards individuals affected by human trafficking and exploitation. If the state is unable to prevent an infringement of their rights, they are entitled to counselling and support. It is only possible for them to exercise this right if a support system with a stable source of funding is available. KOK has demanded secure, long-term funding for specialised counselling centres for many years.[152] Unlike what has been the case up to now, funding must also extend to establishing, maintaining and developing a safe IT infrastructure as well as corresponding staff training. This will improve the specialised counselling centres' impact in the digital environments in which perpetrators are also active in order to recruit potential targets. Stable and safe IT systems and trained counsellors also help protect the organisation as well as individual staff members against cyberattacks.

Law enforcement authorities: fostering awareness, IT skills and resources

The Federal Ministry of the Interior and Community's cybersecurity agenda provides for IT upskilling within various authorities in order to tackle cybercrime, focussing especially on the German Federal Criminal Police Office's Cybercrime Department and the Federal Police Force's investigation capacities in this area by increasing human resources and technical resources.[153] Technology-facilitated trafficking in human beings must urgently be included in this skills drive. In order to ensure trafficked persons can exercise their right to help and protection, law enforcement authorities in Germany must be more aware of and open to this issue; they must understand digital forms of violence and have operational capacities in place to carry out investigations and secure digital evidence. But to do this, they need more resources. This is true not only for cybercrime departments but also for departments specialised in trafficking in human beings, where technology-facilitated elements are only part of the offence. More and sometimes new interdisciplinary collaboration is also needed within the Interior Ministry.

151 This is what the Inter-Agency Coordination Group against Trafficking in Persons (ICAT) also calls for in its statement on the 'Use and abuse of technology' published on the World Day against Trafficking in Persons on 30 July 2022.

152 See KOK *List of demands for the 2021 Bundestag elections*, p. 5 (only available in German).

153 Federal Ministry of the Interior and Community, June 2022: *Cybersicherheitsagenda* ('Cybersecurity Agenda', only available in German).

Specialised counselling centres: increasing IT security and expanding ICT schemes

In view of the increasing presence and activities in digital environments, specialised counselling centres must improve their IT set-up. They need to train their staff in IT matters and secure stable funding in order to do so. The collaboration between some bff counselling centres and IT experts as part of the InterAktion project is a good example of a promising approach.[154]

Specialised counselling centres must also extend the protection schemes for clients, especially those living in shelters, to include elements concerning the use of ICT. There have been question marks over the use of smartphones in shelters for some time, but this issue is growing increasingly complex as technology evolves. The problem is no longer only teaching clients that they should not actively contact traffickers by telephone, text message or WhatsApp or how to prevent unwanted communication. Hidden spyware, GPS geolocalisation and other apps that can be used by traffickers to keep their targets within their reach and monitor them are now also an issue. Clients should therefore be encouraged to use social media and profiles mindfully. This creates a dilemma for specialised counselling centres, i.e. the need to strike a balance between security on the one hand and their clients' right to privacy and agency on the other. The outcomes of a British study (2021) analysing to what extent trafficked persons' access to smartphones is a crucial factor for their psychological wellbeing, mental health, autonomy and perceived safety could be helpful in this respect.[155]

154 bff press release: 'InterAktion: Modellprojekt gegen digitale Gewalt startet: Vernetzung von Beratung und IT' ('InterAktion: model project against digital violence begins, pairing counselling and IT', 23/03/2022, only available in German).

155 Unseen UK/BT, May 2021. *Evaluation report. Impact of mobile technology for survivors of modern slavery and human trafficking: A mixed method study.*

OUTLOOK

Trafficking in human beings is generally seen as the third main type of organised crime after drug and arms trafficking. But is tackling this issue also number 3 on the Government's priority list when it comes to dividing up resources to combat these crimes? This most certainly has not been the case to date. In areas where progress has been made in preventing and combatting trafficking in human beings, albeit slowly, developments in and increasing use of ICT by traffickers are now causing a new danger, namely that of lagging even further behind, which would be detrimental to victims.

The digitalisation of trafficking in human beings is here to stay. Germany must urgently accelerate the digitalisation of its public administration, bolster knowledge and capacity building and at long last step up and face the immense complexity of this crime by facilitating collaboration between departments, authorities and countries, including structurally. A certain number of international and German approaches are already going in the right direction, but stakeholders must act more quickly. A fast and coordinated reaction to acute situations on the part of the international community is indeed possible, as evidenced by the measures taken by the EU Anti-Trafficking Coordinator after the beginning of the war in Ukraine. It is to be hoped that countries will learn from this experience and that the knowledge gained will be applied to the work done to protect target groups and to combat all forms of exploitation related to trafficking in human beings anywhere on the spectrum, from online to offline crimes.

APPENDIX

LIST OF INTERVIEWS

No	Function	Institution	Date	Type
1	Detective Chief Superintendent	German Federal Criminal Police Office, SO41 Department	05/07/2022	Over the phone
2	Counsellor	Jadwiga Munich	06/07/2022	Over the phone
3	Counsellor	Dortmunder Mitternachtsmission	11/07/2022	Face to face
4	Official	Organisation for Security and Cooperation in Europe, Trafficking in Human Beings and Technology Department	12/07/2022	Zoom
5	Official	bff – Frauen gegen Gewalt e. V.	14/07/2022	Teams
6	Counsellor	IN VIA Berlin-Brandenburg	15/07/2022	Zoom
7	Counsellor	Fraueninformationszentrum – FIZ Stuttgart	18/07/2022	Teams
8	Prosecutor	Berlin public prosecutor's office, 255 Organised Crime Department	16/08/2022	Face to face
9	Counsellor	Fraueninformationszentrum – FIZ Stuttgart	24/08/2022	Over the phone
10	2 digital forensics analysts and consultants	Forensik.IT GmbH	01/09/2022	Face to face

REFERENCES

- Alec Muffet: *Real World Onion Sites*, 2022. https://github.com/alecmuffett/real-world-onion-sites/blob/master/master.csv
- Anti-Trafficking Review, No. 14, 2020: *Special Issue – Technology, Anti-Trafficking, and Speculative Futures.* https://www.antitraffickingreview.org/index.php/atrjournal/issue/view/22.
- ARD documentary: 'Illegale Prostitution – Das gefährliche Geschäft mit dem Sex' ('Illegal prostitution – the dangerous trade in sex'), 09/02/2022. https://www.ardmediathek.de/video/betrifft/illegale-prostitution-in-der-pandemie/swr/Y3JpZDovL3N3ci5kZS9hZXgvbzE2MTAxMzQ (only available in German)
- bff, 2021: *Stellungnahme zum Referentenentwurf eines Gesetzes zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings* ('Position statement on the bill to amend the German Criminal Code – combating stalking more effectively and improving legal coverage of cyberstalking'). https://www.frauen-gegen-gewalt.de/de/stellungnahmen-1718/stellungnahme-zum-referentenentwurf-eines-gesetzes-zur-änderung-des-strafgesetzbuches-effektivere-bekämpfung-von-nachstellungen.html (only available in German)
- bff, Press release 'InterAktion: Modellprojekt gegen digitale Gewalt startet: Vernetzung von Beratung und IT' ('InterAktion: model project against digital violence begins, pairing counselling and IT', 23/03/2022. https://www.frauen-gegen-gewalt.de/de/ueber-uns/presse/pressemitteilungen/pm/pressemitteilung-interaktion-modellprojekt-gegen-digitale-gewalt-startet-vernetzung-von-beratung-und-it.html?fbclid=IwAR1Icu7ggosp4blnVfw8eJihvqPYVa9GfpXAs5-M9P1f2At62BGKUu-3DoWA (only available in German)
- Federal Ministry of the Interior and Community, June 2022: *Cybersicherheitsagenda* ('Cybersecurity Agenda'). https://www.bmi.bund.de/SharedDocs/downloads/DE/veroeffentlichungen/themen/sicherheit/cybersicherheitsagenda-20-legislatur.html (only available in German)
- Bracket Foundation, 2022: *Gaming and the Metaverse. The Alarming Rise of Online Sexual Exploitation and Abuse of Children Within the New Digital Frontier.* https://static1.squarespace.com/static/5d7cd3b6974889646fce45c1/t/632f3344eacdbb108c8c356f/1664037701806/metaverse+%26+gaming.pdf
- Federal Office for Information Security: 'Cybercrime methods.' https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/methoden-der-cyber-kriminalitaet_node.html

- Federal Office for Information Security: *Blockchain & Kryptowährung* ('Blockchain and Cryptocurrencies'). https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Technologien_sicher_gestalten/Blockchain-Kryptowaehrung/blockchain-kryptowaehrung_node.html (only available in German)

- German Federal Criminal Police Office:
  - *Bundeslagebild Menschenhandel 2021* ('2021 Federal Situation Report on Trafficking in Human Beings'). https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Menschenhandel/menschenhandelBundeslagebild2021.html?nn=27956 (only available in German).
  - *Bundeslagebild Menschenhandel 2020* ('2020 Federal Situation Report on Trafficking in Human Beings'). https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Menschenhandel/menschenhandelBundeslagebild2020.html?nn=27956 (only available in German)
  - *Bundeslagebild Cybercrime 2021* ('2021 Cybercrime Situation Report') https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2021.html?nn=28110 (only available in German)

- Federal Ministry of Justice: legislative procedure, 17 August 2021. Gesetz zur Änderung des Strafgesetzbuches – effektivere Bekämpfung von Nachstellungen und bessere Erfassung des Cyberstalkings ('Act amending the German Criminal Code – combating stalking more effectively and improving legal coverage of cyberstalking'). https://www.bmj.de/SharedDocs/Gesetzgebungsverfahren/DE/Cyberstalking.html;jsessionid=A9191AD8E2915A07DA69F46A4CF1FE5D.1_cid334?nn=6704238 (only available in German)

- German Federal Government:
  - 'Mehr Schutz vor sexueller Gewalt, Mitteilung vom 10.11.2016' ('Better protection against sexual violence, announcement of 10/11/2016'). Https://www.bundesregierung.de/breg-de/aktuelles/mehr-schutz-vor-sexueller-gewalt-393682 (only available in German)
  - 'Digitalstrategie' ('Digital Strategy'). https://digitalstrategie-deutschland.de/ueber-die-digitalstrategie/ (only available in German)

- Bundesverband der Deutschen Wirtschaft (BVDW): Digital Services Act/Digital Markets Act. https://www.bvdw.org/themen/digitalpolitik/digital-services-actdigital-markets-act/#c10639 (only available in German)

- German NGO Network against Trafficking in Human Beings – KOK:
  - 2020: *Defining the Gap: Datenerhebung zu Menschenhandel und Ausbeutung in Deutschland – der zivilgesellschaftliche Ansatz des KOK* ('Defining the gap: data collection in the context of trafficking in human beings and exploitation in Germany - KOK's civil society approach'). https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/KOK_Datenbericht_Final_deu_2020_10_18.pdf (only available in German)

  - KOK case law database. Kleve Regional Court of 21 February 2017, case no. 190 KLs-203 Js 98/15-2/16.
  - KOK case law database. Aachen Regional Court, Judgment of 25 September 2019, case no. 62 KLs 4/19. Aggravated trafficking in human beings using the loverboy method, contact made via internet platforms.
  - List of demands for the 2021 Bundestag elections. https://www.kok-gegen-menschenhandel.de/fileadmin/user_upload/KOK_Forderungskatalog2021_final.pdf (only available in German)
  - datACT project website: https://www.kok-gegen-menschenhandel.de/datenschutz-datact (only available in German).

- Federal Agency for Civic Education: *Der Arabische Frühling und seine Folgen* ('The Arab Spring and its consequences'). https://www.bpb.de/shop/zeitschriften/izpb/238933/der-arabische-fruehling-und-seine-folgen/ (only available in German)

- Council of the Baltic Sea States, Task Force against Trafficking in Human Beings, 2019: *Human Trafficking Glossary*. https://cbss.org/publications/human-trafficking-glossary/

- German Bundestag:
  - Journal 19/16763, 19. Electoral Period, 20 January 2020. Response of the German Federal Government to a brief enquiry from Members of Parliament Ulla Jelpke, André Hahn, Gökay Akbulut, other Members of Parliament and DIE LINKE parliamentary group – Journal 19/16101 – Nutzung des Hawala-Systems durch organisierte Kriminalität und terroristische Gruppierungen ('Use of the hawala system by organised crime and terrorist organisations'). https://dserver.bundestag.de/btd/19/167/1916763.pdf (only available in German)
  - *Kurzinformation: Die Budapest-Konvention (Cybercrime-Convention) – Aktueller Stand der Verhandlungen zum Zweiten Zusatzprotokoll des Europarates* ('Overview of the Budapest Convention (Cybercrime Convention) – status quo of negotiations on the Council of Europe's Second Additional Protocol'). https://www.bundestag.de/resource/blob/897388/acdeb1ef515226e0308a2be9c022d328/WD-2-115-20-pdf-data.pdf (only available in German)

- Deutschlandfunk Kultur: 'Die Bilanz fällt ernüchternd aus' ('A sobering result'), 07/12/2021. https://www.deutschlandfunkkultur.de/reform-des-sexualstrafrechts-bilanz-nach-fuenf-jahren-100.html (only available in German)

- ECPAT Germany and International Justice Mission Deutschland: Interdisziplinäres Fachgespräch zur sexuellen Ausbeutung von Kindern per Livestream, Mai 2022 (Interdisciplinary Expert Seminar on Sexual Abuse of Children via Livestream, May 2022). https://ijm-deutschland.de/stop-streaming-exploitation

- ECPAT International:
  - 2018: *Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse.* https://ecpat.org/wp-content/uploads/2021/05/Terminology-guidelines-396922-EN-1.pdf

  - 2019: *Explanatory Report to the Guidelines regarding the implementation of the Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography.* https://ecpat.org/resource/opsc-explanatory-reports/

- Council of Europe:
  - 2011. *Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence, Council of Europe Treaty* Series No. 210. https://docentes.fd.unl.pt/docentes_docs/ma/TQB_MA_32409.pdf
  - 2021. *Protecting women and girls from violence in the digital age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women*. https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44
  - 2022. *Online and technology-facilitated trafficking in human beings.* https://rm.coe.int/online-and-technology-facilitated-trafficking-in-human-beings-full-rep/1680a73e49.
  - Cybercrime Convention Committee (T-CY), Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence. *Explanatory Report*, 17/11/2021. https://search.coe.int/cm/pages/result_details.aspx?objectid=0900001680a48e4b
  - *Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and the disclosure of electronic evidence*, 12/05/2022. https://rm.coe.int/1680a6f604

- European Commission:
  - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – A Digital Decade for children and youth: the new European strategy for a better internet for kids (BIK+), COM(2022) 212 final, 11/5/2022. https://digital-strategy.ec.europa.eu/en/library/digital-decade-children-and-youth-new-european-strategy-better-internet-kids-bik
  - Press release, 23/04/2022. 'Digital Services Act: Commission welcomes political agreement on rules ensuring a safe and accountable online environment.' https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2545; https://rm.coe.int/iris-special-2021-01en-dsa-package/1680a43e45
  - Press release, 05/07/2022. 'Digital Services Package: Commission welcomes the adoption by the European Parliament of the EU's new rulebook for digital services.'. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_4313
  - 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). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN.

  - *EU roadmap on the implementation of the strategy to tackle organised crime*, Roadmap – Ares(2021)1264557. https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12735-Fighting-organised-crime-EU-strategy-for-2021-25_en
  - 2019: *E-evidence – cross-border access to electronic evidence.* https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/e-evidence-cross-border-access-electronic-evidence_en
  - 2020: *Study on the economic, social and human costs of trafficking in human beings within the EU*. https://ec.europa.eu/anti- trafficking/sites/antitrafficking/files/study_on_the_economic_social_and_human_costs_of_trafficking_in_human_beings_within_the_eu.pdf
  - 2022: *A Common Anti-Trafficking Plan to address the risks of trafficking in human beings and support potential victims among those fleeing the war in Ukraine – Under the lead of the EU Anti-trafficking Coordinator.* https://home-affairs.ec.europa.eu/system/files/2022-05/Anti-Trafficking%20Plan_en.pdf
  - Commission Communication 'Ensuring justice in the EU — a European judicial training strategy for 2021-2024', COM(2020) 713 final of 2/12/2020.
  - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 'The EU Strategy on Combatting Trafficking in Human Beings 2021–2025', COM(2021) 171 final, 14/04/2022. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0171&from=EN
  - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – EU strategy for a more effective fight against child sexual abuse. https://db.eurocrim.org/db/de/doc/3511.pdf
  - COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT, THE COUNCIL, THE EUROPEAN ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS – EU strategy on the rights of the child, COM(2021) 142 final, 24/03/2021. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0142&from=en
  - Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021–2025, COM/2021/170 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0170&qid=1632306192409
  - REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL. Third report on the progress made in the fight against trafficking in human beings (2020) as required under Article 20 of Directive 2011/36/EU on preventing and combating trafficking in human beings and protecting its victims, COM(2020) 661 final of 20/10/2020. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020DC0661&from=EN

- European Parliament:
  - European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC (COM(2020)0825 – C9-0418/2020 – 2020/0361(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269_EN.html#title1

- European Parliament legislative resolution of 5 July 2022 on the proposal for a regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (COM(2020)0842 – C9-0419/2020 – 2020/0374(COD)). https://www.europarl.europa.eu/doceo/document/TA-9-2022-0270_EN.html
- Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('E-Commerce Directive'). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32000L0031&from=en
- DIRECTIVE 2011/36/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 05 April 2011 on preventing and combating trafficking in human beings and protecting its victims, and replacing Council Framework Decision 2002/629/JHA. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:101:0001:0011:EN:PDF
- *Council conclusions setting the EU's priorities for the fight against serious and organised crime for EMPACT 2022–2025*, Brussels, 12 May 2021 (OR. en), 8665/21, p. 6. https://data.consilium.europa.eu/doc/document/ST-8665-2021-INIT/en/pdf
- Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL laying down rules to prevent and combat child sexual abuse, COM(2022) 209 final, 2022/0155(COD), 11/05/2022. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0209&from=EN
- European Parliamentary Research Service, 2021: *Combating gender-based violence: Cyber violence.* https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf

– EUROPOL
  - 2022: *European Migrant Smuggling Center. 6th Annual Report.* https://www.europol.europa.eu/cms/sites/default/files/documents/EMSC%206%20th%20Annual%20Report.pdf
  - 2020: *The challenges of countering human trafficking in the digital era.* https://www.europol.europa.eu/cms/sites/default/files/documents/the_challenges_of_countering_human_trafficking_in_the_digital_era.pdf

– Fuß, M., 2020: *Forensische Linguistik – Sprachanalyse in Darknet-Foren zu sexuellem Missbrauch und Ausbeutung von Kindern* ('Forensic Linguistics – Linguistic analysis of dark web forums on sexual abuse and exploitation of children'). https://dpt-statisch.s3.eu-central-1.amazonaws.com/dpt-digital/dpt-25/medien/dateien/454/2020_Darknet_Sprachanalyse_ECPAT-kurz.pdf (only available in German)

– Initiative D21 / Kompetenzzentrum Technik-Diversity-Chancengleichheit, 2020: *Digital Gender Gap. Lagebild zu Gender(un)gleichheiten in der digitalisierten Welt.* ('Digital Gender Gap. Situation report on gender (in)eaquality in the digital realm'). https://www.kompetenzz.de/aktivitaeten/digital-gender-gap (only available in German)

– Inter-Agency Coordination Group against Trafficking in Persons (ICAT):
  - 'Statement: Use and Abuse of Technology, World Day against Trafficking in Persons', 30 June 2022. https://icat.un.org/sites/g/files/tmzbdl461/files/publications/icat_statement_wdat_2022.pdf
  - 'Trafficking and Technology: Trends, Challenges and Opportunities.' Issue Brief 7/2019. https://icat.un.org/sites/g/files/tmzbdl461/files/human_trafficking_and_technology_trends_challenges_and_opportunities_web.pdf

– UNCRC: General Comment No. 25 (2021) on children's rights in relation to the digital environment: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.

– G7 Leaders' Communiqué, 28 June 2022. https://www.consilium.europa.eu/media/57555/2022-06-28-leaders-communique-data.pdf

– Kramer, F., 2020: 'Mit THB Liberi organisierten Menschenhandel bekämpfen' ('Combatting organised trafficking in human beings using THB Liberi'). In: Die Polizei, 11-2020 (only available in German).

– Milivojevic, S., Moore, H., Segrave, M.: 'Freeing the Modern Slaves, One Click at a Time: Theorising human trafficking, modern slavery, and technology.' In: Anti-Trafficking Review, No. 14, 2020, pp. 16–32. https://www.antitraffickingreview.org/index.php/atrjournal/article/view/442/351

– Organization for Security and Co-operation in Europe (OSCE):
  - 2022: *Recommendations on enhancing efforts to identify and mitigate risks of trafficking in human beings online as a result of the humanitarian crisis in Ukraine.* https://www.osce.org/cthb/516423
  - Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings, 2022: *Policy Responses to Technology-Facilitated Trafficking in Human Beings: Analysis of Current Approaches and Considerations for Moving Forward.* https://www.osce.org/files/f/documents/0/d/514141.pdf
  - 2020: *Leveraging innovation to fight trafficking in human beings: a comprehensive analysis of technology tools.* https://www.osce.org/secretariat/455206

– Pacific Links Foundation: PAXU. https://pacificlinks.org/paxu/#Courage

– Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., Aiken, M. P.: 'Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies.' In: *Forensic Sciences* 2022(2), pp. 379–398.

– Polaris, 2018: *On-Ramps, Intersections, and Exit Routes: A Roadmap for Systems and Industries to Prevent and Disrupt Human Trafficking.* https://polarisproject.org/wp-content/uploads/2018/08/A-Roadmap-for-Systems-and-Industries-to-Prevent-and-Disrupt-Human-Trafficking.pdf

- Raets, S., Janssens, J., 2019. 'Trafficking and Technology: Exploring the Role of Digital Communication Technologies in the Belgian Human Trafficking Business.' In: European Journal on Criminal Policy and Research (2021) 27, pp. 15–238. https://link.springer.com/article/10.1007/s10610-019-09429-z

- Reid, R., Fox, B., 2020: *Human Trafficking and the Darknet: Technology, Innovation, and Evolving Criminal Justice Strategies.* https://link.springer.com/chapter/10.1007/978-3-030-41287-6_5

- Rüdiger, T., 2017: 'Das Broken-Web-Phänomen' ('The broken web phenomenon'). In: Jur@ im Netz. https://www.researchgate.net/publication/320490473_Das_Broken-Web-Phanomen_-_Jur_im_Netz

- Statista.de: Number of internet users in selected European countries in 2021: https://de.statista.com/statistik/daten/studie/184636/umfrage/internetreichweite-anteil-der-nutzer-in-europa/ (only available in German).

- Statista.de: Statistics on global internet usage: https://de.statista.com/themen/42/internet/#dossierKeyfigures (only available in German).

- Stop The Traffik, 2018: *Human Trafficking and the Darknet: Insights on supply and demand.* https://www.stopthetraffik.org/wp-content/uploads/2019/06/Human-Trafficking-and-the-Darknet-Insights-FINAL-1.pdf

- Tamm, A., Volbert, R., presentation on 10/05/2022: 'Das Projekt ViContact. Befragungen bei Verdacht auf sexuellen Missbrauch – Training in virtueller Umgebung' ('The ViContact project. Questioning in cases of suspected sexual abuse – training in a virtual environment, in German).

- Teschner, G.: 'Sex on Demand. Prostitution geht online, Menschenhandel und Ausbeutung auch?' ('Sex on Demand. Prostitution is going online – what about trafficking and exploitation?'), In: *Kriminalistik* 11/2021, p. 645 –648.

- UNICEF, 2022 – *Legislating for the digital age, Glossary.* https://www.childrenrights.de/content/user_upload/UNICEF__BMZ__GIZ__2022._Summary_Legislating_for_the_digital_age_.pdf

- United Nations Office on Drugs and Crime (UNODC), 2021: *The effects of the Covid19 pandemic on trafficking in persons and responses to the challenges.* https://www.unodc.org/documents/human-trafficking/2021/The_effects_of_the_COVID-19_pandemic_on_trafficking_in_persons.pdf

- Unseen UK/BT, May 2021. *Evaluation report. Impact of mobile technology for survivors of modern slavery and human trafficking: A mixed method study.* https://www.unseenuk.org/wp-content/uploads/2021/10/FINAL-Unseen-BT-Evaluation-report_Technology-report_17MAY.pdf

- Wall, D. S., 2017: 'Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing.' In: Brownsword, R., Scotford, E., Yeung, K. (eds): *The Oxford Handbook on the Law and Regulation of Technology*, unpaginated. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3005872

- WeProtect Global Alliance, 2021: *Framing Child Sexual Abuse and Exploitation Online as a Form of Human Trafficking: Opportunities, Challenges and Implications. Expert Roundtable Outcomes Briefing.* https://www.weprotect.org/wp-content/uploads/WeProtect-Global-Alliance-Trafficking-Roundtable-Outcomes-Briefing-2021.pdf

PUBLICATION DETAILS

TRAFFICKING IN HUMAN BEINGS 2.0 –
DIGITALISATION OF TRAFFICKING IN HUMAN BEINGS IN GERMANY
Developments and Courses of Action

Publisher:
German NGO Network against Trafficking in Human Beings – KOK
Lützowstr. 102–104 / Hof 1, Aufgang A
10785 Berlin
Phone: +49 (0)30/ 263 911 76
Fax: +49 (0)30/ 263 911 86
info@kok-buero.de
www.kok-gegen-menschenhandel.de/en

Author: Dr Dorothea Czarnecki
Graphic design and composition: Ricarda Löser
Translation and Editing: Fiona Scuiller / Rosy Skilton
Cover image: istockphoto.com/royyimzy
Legally responsible for content: Sophia Wirsching
Printed by: hinkelsteindruck, Berlin
Number of copies: 100 copies

Bank account details:
KOK
Evangelische Bank eG
IBAN: DE43 5206 0410 0003 9110 47
BIC: GENODEF1EK1

ISBN: 978-3-9821936-9-4

KOK is funded by:

Federal Ministry for
Family Affairs, Senior Citizens,
Women and Youth

KOK

German NGO Network against
Trafficking in Human Beings

Lützowstr. 102 – 104 I Hof 1, Aufgang A
10785 Berlin
Phone: +49 (0)30 / 263 911 76
Fax: +49 (0)30 / 263 911 86
info@kok-buero.de
www.kok-gegen-menschenhandel.de/en

9 783982 193694