United Nations CTOC/COP/WG.4/2021/2

Conference of the Parties to the United Nations Convention against Transnational Organized Crime

Distr.: General
23 July 2021

Original: English

Working Group on Trafficking in Persons
Vienna, 12 and 13 October 2021
Item 2 of the provisional agenda*
Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons

Successful strategies for addressing the use of technology to facilitate trafficking in persons and to prevent and investigate trafficking in persons

Background paper prepared by the Secretariat

I. Introduction

1. The present background paper was prepared by the Secretariat to facilitate discussion by the Working Group on Trafficking in Persons at its eleventh meeting. It sets out a series of issues related to the current nexus between technology, including information technology, and trafficking in persons. It provides background information on a range of related topics, including the use of modern applications to recruit, control and exploit victims, as well as to detect, investigate, prosecute and counteract trafficking in persons. It also notes challenges and promising practices in the utilization of technology and highlights the importance of respecting privacy, human rights safeguards and data protection policies. The background paper lists specific references, resources and tools that States may wish to review to further develop responses to such trafficking in persons.

II. Issues for discussion

2. Delegations may wish to consider the responses of their States to the following issues in preparing for the Working Group's deliberations:

(a) In the use of modern technology, including information and communications technology, what tools and strategies have been successful and promising so far in combating trafficking in persons? What have been the most effective and affordable technology solutions to enhance responses to combat trafficking in persons while respecting human rights?

(b) What practical measures have States parties undertaken to adapt and respond to any increased and evolving use of technology by traffickers? How can law

* CTOC/COP/WG.4/2021/1.

enforcement agencies strengthen their capacity to fight trafficking in persons in cyberspace, including the dark web?

(c) In curbing the misuse of technology, what good practices relating to multi-stakeholder partnerships have been identified by law enforcement agencies? How can States parties cooperate with social networks to better detect and investigate recruitment, control and exploitation of victims on those platforms?

(d) How can technology contribute to a more efficient and agile e-justice,[1] in particular with regard to international cooperation, joint investigations, mutual legal assistance, extraditions and the collection of digital evidence in cases of trafficking in persons? How have obstacles to the related use of technology been overcome?

(e) How do States parties ensure that human rights, in particular the right to privacy, are respected and fulfilled in the use of technology in crime prevention and criminal justice responses related to trafficking in persons? Are new legal and oversight frameworks needed to ensure that the use of technology in investigative operations is compliant with human rights requirements, in particular the right to privacy?

(f) How do States parties ensure that the use of new technologies, including information and communications technology, do not have an adverse effect on victims of trafficking?

(g) How can States parties better address demand for services stemming from trafficking in persons, including for sexual exploitation, and work on prevention strategies, in a context in which services and materials coming from victims of trafficking have become easily accessible in cyberspace?

(h) How can the United Nations, in particular the United Nations Office on Drugs and Crime (UNODC), best support States parties' efforts to research and disseminate good practices and effective strategies in the use of new technologies to prevent and counter trafficking in persons? How can UNODC further partnerships with various relevant stakeholders, and in which fields of technology can UNODC best strengthen the capacity of law enforcement agencies?

3. The Working Group might wish to consider recommending that States parties consider taking the following actions to address trafficking in persons through the use of technology and build sustainable responses to the misuse of technology by traffickers:

- Identify and address gaps in legal systems to ensure the effective investigation and prosecution of technology-facilitated trafficking in persons and ensure that legal frameworks keep pace with technological developments and, in particular, enable courts to receive electronic evidence.
- Ensure that appropriate legislation is in place to protect children from trafficking activities occurring online. Establish high standards of cybersecurity, privacy-by-design and safety-by-design in the digital services and products that children use, in order to minimize exposure of children to the risk of trafficking.[2]
- Incorporate a gender- and child-sensitive perspective into strategies being developed to address the nexus between technology and trafficking in persons.
- Strengthen the expertise and the capacity of law enforcement agencies in conducting efficient investigations and operations in cyberspace, seizing appropriate electronic evidence and using available technology tools, including on the dark web.

[1] The concept of "e-justice" refers to the enhanced application of technologies in criminal justice and the development of technology-based criminal justice strategies.

[2] Committee on the Rights of the Child, General comment No.25 (2021) on children's rights in relation to the digital environment, para 116.

- Enhance international and cross-border cooperation in criminal matters through the use of technology and innovative tools by practitioners and central authorities.[3]
- Support technology-based solutions that address the global scope of trafficking in persons, such as data aggregation and data scanning tools that facilitate automatized information analysis in support of investigations to counter this crime and that are in full compliance with human rights and privacy rights.
- Ensure that any use of technology by law enforcement authorities is consistent with human rights standards and is necessary, proportionate, legal, accountable and fair.
- Ensure that ethical considerations are fully addressed in the use of technology, including large-scale data gathering systems and ensure that, in harnessing the growing application of big data analysis, machine learning and artificial intelligence to scale up law enforcement efforts, computerized intelligence and software are "debiased" throughout their programming and deployment stages.
- Encourage and expand, where relevant and appropriate, effective partnerships and coalitions between various sectors and stakeholders, including the public sector, civil society, academia and the private sector, including technology companies, to enhance innovation, cooperation and the use of technology.
- Encourage technology companies to embrace more robust scanning practices and accelerate the development of methods for the detection of trafficking in persons activities online,[4] including the trafficking of children, while making sure that material stemming from online sexual exploitation is removed from online platforms to avoid re-victimization and continuing exploitation.
- Increase commitment and cooperation for developing policies, sharing intelligence and enhancing international cooperation at the national, regional and international levels to counter trafficking in persons enabled by information and communications technology.[5]
- Improve data collection and research on the scope and nature of the misuse of information and communications technology to enable trafficking in persons, in particular the misuse of social networks.
- Support the United Nations in the collection, analysis and broader dissemination of promising strategies and practices related to the use of modern technologies to address trafficking in persons.

III. Overview of issues and related topics

4. With the coronavirus disease (COVID-19) pandemic and its containment measures restricting movement and gatherings worldwide, people have increasingly turned to the Internet to carry out activities and engage in social life. Digital technology, including information and communications technology, has brought about positive developments in daily life which have been particularly magnified during the pandemic. Information and communications technology has become an indispensable element of our lives, for which COVID-19 has acted as a change accelerator.

5. At the same time, the consequences of the increased accessibility of technology include its misuse by criminal networks. Some trafficking in persons activities have

[3] See also A/CONF.234/16, para. 192 (j).
[4] United Nations, *Report of the Secretary-General: Roadmap for Digital Cooperation*, June 2020, p. 3.
[5] UNODC, *Darknet Cybercrime Threat to South-East Asia 2020*, foreword.

moved almost completely online, which reduces the risks for the perpetrators and at times offers greater profitability.[6]

6. Information and communications technology can, however, also be leveraged to combat organized crime and be of assistance to law enforcement authorities in multiple ways, such as in the detection, investigation and prosecution of trafficking in persons cases, the protection of victims and witnesses and the removal of harmful or exploitative materials online. Greater attention is being given to the need for law enforcement personnel to be trained in online investigation methods to counter trafficking in persons, the collection of digital evidence and the ethical concerns associated with the use of new technologies. Related investigations and surveillance methods as well as the use of technological tools by State actors, especially law enforcement agencies, should be closely monitored to ensure compliance with human rights and the right to privacy.

7. International cooperation, which is necessary in complex criminal activities spanning several jurisdictions, is often difficult to achieve in traditional investigations, but faces additional challenges in online cases, in which perpetrators, victims, clients and servers may all be in different parts of the world. The resulting difficulties are at least partially attributable to an often insufficient digital expertise of law enforcement authorities and a lack of use of technology-based systems in the countries concerned.

8. Effective partnerships connecting law enforcement authorities and State agencies with the private sector, including technological companies, as well as non-governmental organizations, academia and other relevant stakeholders, are crucial for effective strategies to counter trafficking in persons enabled by technology. Enhanced technology-enabled cooperation among all stakeholders would make anti-trafficking strategies more effective.

A. Use of technology to enable trafficking in persons

9. Trafficking in persons is a crime characterized by its adaptability because trafficking business models evolve to take advantage of the new opportunities offered by advances in technology. In article 3 of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime, trafficking in persons is defined as “the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation.” Technology intersects with trafficking in persons in every element of the definition above. Technology is used by traffickers at every step of the crime, from identifying future victims and recruiting them to laundering the proceeds of the exploitation.

1. Profiling and recruiting the victims

10. Technology has impacted on the recruitment of victims by traffickers in multiple ways. Traffickers can find a large volume of personal information about potential victims on the Internet, in particular on social media platforms such as Facebook, TikTok, Snapchat and Instagram, with publicly accessible details related to victims’ friends, family, location, work, holidays and tastes, revealing habits and vulnerabilities. Dating websites and applications, in particular, also allow for the geolocalization of victims. This may enable traffickers to thoroughly profile their victims before entering in contact with them and develop targeted grooming

[6] European Union Agency for Law Enforcement Cooperation (Europol), *European Union Serious and Organised Crime Threat Assessment: A Corrupting Influence – The Infiltration and Undermining of Europe’s Economy and Society by Organised Crime* (Luxembourg, Publications Office of the European Union, 2021), p.13.

strategies. Technology has enabled ready access to a wide range of personal information that was previously not easily accessible, if at all.

11. Information and communications technology also offers a mask of anonymity to traffickers, who can interact with potential victims on social networks and communication applications such as WhatsApp, as well as gaming chat rooms, in ways that are less conspicuous than if they had to meet them in person. This is particularly the case with child trafficking for sexual exploitation. Anonymity and confidentiality can be further secured by end-to-end encryption of the communications between traffickers and victims, thereby ensuring that no third parties can access communications. In addition, traffickers can hide behind different identities and names to interact with or deceive victims on those social networks. For example, in the UNODC *Global Report on Trafficking in Persons 2020*, a case is described in which a trafficker had two fake identities to interact with the victim – one to write abusive messages and the other to express compassion – thereby manipulating the person through coercion [7] – a case which demonstrates how traffickers misuse social media profiles for recruitment and control strategies.

12. The Internet gives access to a much broader pool of potential victims because traditional physical and geographical limitations do not exist, with the result that much less effort is required for their recruitment. Today, traffickers can recruit many victims in different countries simultaneously, which was unthinkable just a few years ago when the related technology did not exist. Further, for perpetrators, a key advantage in using multiple forms of information and communications technology is the potentially lower risk of immediate detection by law enforcement authorities. For those various reasons, among others, new technologies are increasingly used by traffickers to identify and recruit victims.

13. The UNODC *Global Report on Trafficking in Persons 2020*, in which 79 court cases worldwide containing an element of online technology are reviewed, characterizes two main ways that traffickers use the Internet to recruit victims: the "hunting" strategy, characterized by a proactive trafficker who pursues victims online, for example, on social media platforms, and the "fishing" strategy, more commonly used, which involves traffickers posting advertisements online, such as false job advertisements on legitimate employment portals, or creating fake employment agencies and waiting for potential victims to contact them.[8] The latter method may be used, for example, in cases of trafficking for labour exploitation, in which victims tend to play a more active role.[9]

14. New technologies are used in trafficking in persons cases for different types of exploitation. In the context of trafficking in persons for forced labour, victims can be recruited through deceptive job advertisements published on completely fake websites but also by posting fake advertisements on legitimate employment portals, job apps and social networking websites.[10] A case study in the Philippines[11] shows how unscrupulous recruiters, brokers and agents are also active on online job portals dedicated to migrant workers and social networks. While already operating in the traditional media and on billboards, traffickers, using the Internet, can reach a much wider audience, including in more remote locations. Some of the related websites feature the option of a live chat with a supposed recruiting manager, thus giving the

[7] UNODC, *Global Report on Trafficking in Persons 2020,* p.121.

[8] Ibid., p.127.

[9] Organization for Security and Cooperation in Europe (OSCE) Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings and Tech against Trafficking, *Leveraging Innovation to Fight Trafficking in Human Beings: A Comprehensive Analysis of Technology Tools, Taking Stock of Technology Tools* (Vienna, May 2020), p. 20.

[10] UNODC, Education for Justice initiative, "Module 14: technology facilitating trafficking in persons".

[11] Mark Latonero, Bronwyn Wex and Meredith Dank, *Technology and Labor Trafficking in a Network Society: General Overview, Emerging Innovations and Philippines Case Study,* (Los Angeles, University of Southern California, Annenberg Center on Communication Leadership and Policy, 2015).

trafficker immediate contact.[12] In addition, through advertisements, traffickers or exploitative employers request prospective employees to send sensitive personal information such as passport details, degrees or certificates, thus enhancing their power and control over the targeted workers. Such practices might increase an employee's vulnerability to situations of trafficking for forced labour.[13] The Organization for Security and Cooperation in Europe (OSCE) provides information about cases of trafficking for domestic servitude in which victims' details are sold online by the thousands to buyers, who can review their profiles.[14]

15. Information and communications technology have been used in cases of trafficking in persons for organ removal, in which traffickers have recruited victims by placing online advertisements promising highly paid employment in other countries. When the recruited victims have been transported abroad and the employment opportunities have failed to materialize, the victims have already incurred high costs. Traffickers would then offer the victims, as the only alternative for repaying the debt incurred under deception, the option of selling their organs.[15] The European Union Agency for Law Enforcement Cooperation (Europol) reports that the recruitment of female victims of trafficking in illegal surrogacy programmes and the sale of their newborns increasingly takes place online as well, as victims are lured with offers to purchase babies.[16] The traffickers particularly exploit the specific situations of vulnerability of these individuals, as there are documented cases of victims who are homeless, suffer from mental and physical disabilities, are single parents with children or are elderly.[17] Although some cases have been documented of online advertisements being used in connection with forced and sham marriages, the profiling and recruitment of victims with the use of information and communications technology is most commonly used in trafficking for sexual exploitation, including child sexual exploitation.[18] The COVID-19 pandemic has acted as a catalyst in that regard due to the increased use of the Internet, in particular social networks, especially their use by children, who have become exposed to risks of recruitment in trafficking cases, for example, through online video gaming sites.[19] Traffickers also frequently use the "lover boy" method to lure underage victims into sexual exploitation.[20]

2. Methods of control

16. The definition of the crime in the Trafficking in Persons Protocol states that "means" are used for a person to have control over another person for the purpose of exploitation, such as "the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits". In parallel with the increased use and presence of information and communications technology in our lives, traffickers have adapted their modus operandi and used technological tools to

---

[12] Europol Operations Directorate, "The challenges of countering human trafficking in the digital era", October 2020.

[13] *Technology and Labor Trafficking in a Network Society,* p.36.

[14] OSCE Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings and Tech against Trafficking, *Leveraging Innovation to Fight Trafficking in Human Beings: a Comprehensive Analysis of Technology Tools, Taking Stock of Technology Tools,* p. 15.

[15] Ibid., p. 18.

[16] *European Union Serious and Organised Crime Threat Assessment* (2021), p.73.

[17] Ibid., p.73.

[18] Online child sexual abuse does not always amount to child trafficking for sexual exploitation, and they constitute different crimes in many jurisdictions. However, online child sexual abuse can constitute child trafficking for sexual exploitation, and child sexual abuse material is often produced through trafficking. In addition, since the same technological tools and investigations are used by law enforcement agencies to combat both crimes, reference to both is therefore made in this paper, although the focus is on trafficking in persons.

[19] See also Committee on the Elimination of Discrimination against Women, General recommendation No. 38 (2020) on trafficking in women and girls in the context of global migration (CEDAW/C/GC/38), paras. 36–37.

[20] *European Union Serious and Organised Crime Threat Assessment* (2021), p.71.

gain and keep control over victims in various ways, consistent with the Protocol's definition the crime.

17. There have been reports of traffickers monitoring the phone records of their victims, either manually or by using spyware.[21] Location-tracking applications and use of global positioning systems in mobile phones can be used to know the victim's location, while cameras in smartphones and video calls in applications such as FaceTime, WhatsApp and Skype enable traffickers to see their victims and their surroundings. Technology gives traffickers the ability to control victims remotely sometimes without having ever met them face-to-face.

18. Technology also enables psychological methods of control by generating fear and despair in victims. For example, threats and deception may be used by traffickers as a method of control in cases where traffickers manage to obtain compromising information about the victim, such as nude photographs or the recording of sexual acts on video and then threaten to upload that content online or send it to relatives and/or friends of the victim through social networks. This is used, for example, in the "lover boy" method of recruitment, in which traffickers flirt and interact with individuals, ask them to send erotic pictures and then use those to coerce those individuals into sexual exploitation. Such methods of blackmail may be used both to coerce the victim into sexual exploitation and as a tool of deterrence to prevent the victim from complaining to law enforcement authorities or escaping.[22]

3. Exploitation

19. Technology acts as a force multiplier in cases of trafficking for sexual exploitation as it enables the recruitment, commercialization and exploitation of victims on a potentially massive scale. The use of websites to advertise the sexual services of victims to clients has become a fundamental feature of this exploitation,[23] and victims may be repeatedly exploited through live-streaming on multiple websites, their videos watched limitlessly and their services sold to many clients through the same advertisement on numerous platforms. In that regard, information and communications technology enables traffickers to maximize outreach and profits.[24]

20. The use of the dark web to advertise to obtain victims of trafficking for sexual exploitation seems so far to be limited. One reason for this is that to maximize profits, traffickers need to reach as large an audience as possible, which is better done on the clearnet, where the advertisement of sexual services derived from trafficking in persons can be hidden in the myriad of existing legal advertisements for sexual or other services. Darknets are more likely to be used for niche interests such as organ removal or online child sexual exploitation.[25]

21. In the case of trafficking for sexual exploitation, including online child sexual exploitation, information and communications technology is often used to archive, store and conceal materials, including on darknets, as they provide perpetrators with a greater degree of anonymity and enable them to better hide illegal material from investigators. Both the dark web and the clearnet are used to trade and sell material created through trafficking in persons to a global audience.

22. Although trafficking for sexual exploitation constitutes the majority of detected trafficking cases of exploitation online, the UNODC *Global Report on Trafficking in Persons 2020* relates that the Internet may be used for trafficking for forced

[21] UNODC, Education for Justice initiative, "Module 14: technology facilitating trafficking in persons".

[22] See also Europol Operations Directorate, "The challenges of countering human trafficking in the digital era", p.3.

[23] *European Union Serious and Organised Crime Threat Assessment* (2021), p.70.

[24] Europol Operations Directorate, "The challenges of countering human trafficking in the digital era".

[25] OSCE Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings and Tech against Trafficking, *Leveraging Innovation to Fight Trafficking in Human Beings: a Comprehensive Analysis of Technology Tools, Taking Stock of Technology Tools,* p. 15.

criminality and gives an account of a case in Denmark in which traffickers had recruited people to force them to commit data fraud and identity theft. They were given fake identities to procure and lease products by abusing credit card information on websites, fraudulently using digital signatures to file tax returns.[26]

4. Financial transactions

23. Technologies may be misused for financial payments effected through online payment systems. Payment transfers can be arranged through the use of money transfer applications.

24. The use of cryptocurrencies may increase the ease with which traffickers are able to use, receive, hide and move money. Use of cryptocurrencies can aid money-laundering and help criminals avoid investigation and being apprehended by providing anonymity and reducing the need to carry large quantities of cash.[27] For example, in a sex trafficking case prosecuted in the United States of America, the defendant had used bitcoins to purchase advertisement spaces on the website, backpage.com, to sell sex with several women he exploited after their recruitment on Facebook.[28] Cryptocurrencies also help avoid money-laundering compliance regulations and offer the opportunity to move cash across borders without alerting financial institutions.[29] However, the use of cryptocurrencies is considered to not yet constitute a large share of the financial transactions in online trafficking in persons cases.[30]

B. Using modern technology to prevent and address trafficking in persons

25. Technological information is useful to law enforcement authorities as it enhances the ability to prevent, detect and investigate trafficking in persons and to prosecute those involved. For example, technology can be utilized by law enforcement authorities to identify traffickers by means of artificial intelligence and data mining applications to identify suspicious transactions. Furthermore, technology can facilitate the recording, storage, analysis and exchange of information relating to trafficking in persons.

26. Beyond its criminal misuse to exploit persons in trafficking cases, technology does offer ways for law enforcement authorities to prevent, detect, intervene and combat organized crime. However, it is crucial to ensure adequate human rights and privacy rights safeguards in the application of technology throughout all investigative processes. It is essential to ensure that infiltration and prevention activities by law enforcement authorities are proportionate, legal, accountable and necessary. This requires solid legislative and human rights oversight frameworks.[31]

27. The examples given below describe existing or promising tools and show that technology can be used in a range of applications, although some vigilance is required with respect to monitoring their actual effectiveness and positive contributions. This paper does not aim to provide a comprehensive overview of all technological and data-driven approaches available to counter trafficking in persons but rather to offer examples of interesting and effective technological tools. The coalition of technology companies collaborating to combat trafficking in persons, Tech against Trafficking,

[26] *Global Report on Trafficking in Persons 2020,* p.122.
[27] See A/CONF.234/11.
[28] *United States of America v. Anthony Donte Collier*, 932 F.3d 1067 (8th Cir. 2019).
[29] See UNODC, Education for Justice initiative, “Module 14: technology facilitating trafficking in persons”.
[30] Europol Operations Directorate, “The challenges of countering human trafficking in the digital era”, p.4.
[31] UNODC, *Darknet Cybercrime Threat to South-East Asia 2020*, p.3.

provides more information and details on the hundreds of different technological tools created so far to combat diverse forms of exploitation.[32]

1. Smartphone applications

28. Among the different technological tools used against trafficking in persons, multiple and diverse applications have been created over the past decade to prevent and fight trafficking for forced labour. For instance, some applications are aimed at individual consumers, by encouraging, for example, ethical consumption by allowing consumers to select products free of involvement of trafficking in persons in their production through a ranking of providers and the provision of information on risks of trafficking, while some applications support migrant workers by providing information about the work of recruiting agencies, including whether they are suspected of human trafficking, and other applications enable employees to report trafficking in supply chains.[33] One such application and website, Contratados.org,[34] enables workers to find work, rate employers, get information on related topics such as COVID-19 and seek support.

29. While some scholars have underlined innovative approaches and results such as enhanced communication through horizontal peer networks, thus contributing to a more informed decision-making process[35], others have recommended caution when using and assessing applications fighting trafficking in persons for labour exploitation, citing, for example, obscure methodologies used to rank industries responsible for forced labour and the use of outdated, contradictory or incomplete information.[36] It has also been underlined that applications enabling employees to report forced labour in supply chains and their working conditions might harm the very workers they intend to protect by collecting and exposing personal data.[37] Finally, some criticize the fact that there has been a shift in the responsibility for detecting trafficking in persons and eradicating exploitation, from the State to individual consumers.[38] Such technological tools cannot address the structural and deep causes of trafficking for labour exploitation. Overall, while many of these applications have good potential, some seem to offer limited benefits and have a range of problems.[39]

2. Data analytics and blockchain

30. To better identify human trafficking risks, companies are also using blockchain technology, which allows tracking the production of goods from their source to the final destination, in order to increase transparency and aid in exercising due diligence.[40] For instance, data analytics may be used to monitor and identify trafficking for labour exploitation in global supply chains. The non-governmental organization Made in a Free World, for example, operates a software package called FRDM to support companies in analysing their supply chains for evidence of labour

[32] For further information, see www.techagainsttrafficking.org.

[33] See the detailed description of the functioning of these applications in Stephanie Limoncelli, "There's an app for that? Ethical consumption in the fight against trafficking for labour exploitation", *Anti-Trafficking Review*, issue 14, 2020, pp. 33–46.

[34] An interesting analysis of the functioning of the contratados.org website can be read in Annie Isabel Fukushima, "Witnessing in a time of homeland futurities", *Anti-Trafficking Review*, issue 14, 2020, pp. 67–81.

[35] *Technology and Labor Trafficking in a Network Society,* p. iv.

[36] "There's an app for that? Ethical consumption in the fight against trafficking for labour exploitation", *Anti-Trafficking Review*, issue 14, 2020.

[37] L. Berg, B. Farbenblum, and A. Kintominas, "Addressing exploitation in supply chains: Is technology a game changer for worker voice?", *Anti-Trafficking Review*, issue 14, 2020, p.63.

[38] "There's an app for that? Ethical consumption in the fight against trafficking for labour exploitation", *Anti-Trafficking Review*, issue 14, 2020.

[39] Ibid.

[40] Issue brief, No. 7 (2017), p.4.

trafficking and quantifying the risk of trafficking in suppliers and materials.[41] It does so through machine-learning "crawlers", the automated process of going through enormous amounts of websites to find information and save their content.

3. Hashes, data aggregation and information-sharing

31. Innovations in technological methods and techniques such as PhotoDNA and databases have contributed to improving forensic processes to advance investigations of cases of trafficking in persons for sexual exploitation, including child sexual exploitation.

32. PhotoDNA is a technological tool developed by Microsoft in 2009 and gifted to the National Center for Missing and Exploited Children (NCMEC) in the United States. NCMEC receives reports of suspected child sexual abuse material from technological companies such as Facebook, Instagram and Google, and, once an image is confirmed as child sexual abuse material, the "hash", a sequence of letters and numbers that constitute a unique digital fingerprint for that image, is created on the basis of an analysis of the details of the image. The hash is unique to the image. The hashes are then used by Internet service providers and social media companies which proactively use PhotoDNA on their servers to block known and verified child abuse content.

33. In 2020 alone, NCMEC received 21.7 million reports of images and videos depicting child sexual abuse through its CyberTipline,[42] and hashes (digital fingerprints) of images of exploitation were subsequently created. This was a 28 per cent increase in the number of reports compared with the previous year. The database, which is in constant expansion, serves as a central repository for child abuse material and as a reporting mechanism. With the use of PhotoDNA, other technology tools and open-source data, NCMEC aggregates information and analyses the geographical origin of the content in order to communicate it to law enforcement authorities. Data integration software aids the triage of those millions of reports and the extraction of information to identify and rescue child victims faster than human beings could.[43] In addition, the CyberTipline, through PhotoDNA, has a "cleaning" function, as NCMEC analysts inform the hosting providers of images, videos and other files related to child sexual abuse, including those stemming from child trafficking, in order to have them removed from the Internet and prevent further dissemination, in an effort to avoid revictimization. Furthermore, that data collection informs policies against child abuse and child trafficking and prevention efforts. The Internet Watch Foundation, a charity based in the United Kingdom of Great Britain and Northern Ireland which operates at the international level, recently established a task force to assess and generate hashes for similar materials.

34. This technology has been highly effective and offers a range of advantages. It does not analyse and understand the content of the Facebook profiles, Instagram photographs and platforms it goes through but is only capable of detecting the hashes that already exist in the database. As a result, this technology is used to block child sexual abuse material from being uploaded or downloaded without interfering with the privacy of customers. So far, the images which are used to form the hashset form the starting point of investigations and victim identification. Furthermore, they crucially help analysts and investigators to triage high-priority cases and new content versus lower-risk content, such as decades-old photographs. They have already assisted in the detection and reporting of millions of child sexual exploitation images, including content created through child trafficking. Finally, the hashset also minimizes the amount of exposure of analysts and investigators to real images and reduces risks of secondary traumatization.

---

[41] More information is available at https://app.frdm.co/. Also see the reference in *Technology and Labor Trafficking in a Network Society,* 2015, p. 3.

[42] Other countries also have similar reporting mechanisms and tiplines, such as the Cybertip.ca in Canada.

[43] See www.youtube.com/watch?v=h29rt8QV1Ko for a detailed explanation.

35. Similar other databases have been created to report child sexual abuse for investigation purposes through the use of unique hash values, such as the International Criminal Police Organization (INTERPOL) International Child Sexual Exploitation database.

36. The American non-governmental organization Polaris, which hosts the National Human Trafficking Resource Center, also applies analytics to the database of calls received on its national hotline. Through a special software, Polaris is able to use mapping techniques to project the potential geographic locations of calls to the national hotline referencing trafficking.[44] In 2020, Polaris partnered with PayPal, a major company operating an online payments system, to form a financial intelligence unit with the financial and substantive support of PayPal, to leverage intelligence from the hotline and other sources to interrupt cash flows stemming from trafficking in persons and enable prosecutions for financial crimes, including money-laundering.[45] Database analytics can therefore serve a wide spectrum of applications.

37. The Europol reporting website entitled "Stop Child Abuse – Trace an Object" is another interesting current application of technology to combat child sexual abuse, including child trafficking. It gives the public the opportunity to contribute to investigations by identifying objects taken from the background of photographs of sexually explicit material involving minors and other files linked to this crime. This is a tool of last resort used by Europol when other investigative techniques fail to identify such photographs. It seeks the help of the general public where other means have proved unsuccessful.

4. Artificial intelligence and facial recognition tools

38. Law enforcement authorities are increasingly interested in holistically applying technology to disrupt and investigate trafficking networks and take full advantage of new and evolving technologies such as artificial intelligence systems and digital forensic capabilities to enhance criminal investigations of trafficking cases. The potential of technology was recently highlighted at the Fourteenth United Nations Congress on Crime Prevention and Criminal Justice, held in Kyoto, the final report of which mentions that "cloud-based technology, big data and artificial intelligence could improve technical capabilities for more effective and coordinated policy responses to trafficking in persons at the national and international levels."[46]

39. The power of artificial intelligence and machine learning is increasingly being explored to leverage responses against organized crime, including trafficking in persons.[47] Artificial intelligence can help make predictions and conclusions on a large scale and without human intervention by combining and analysing intelligence from multiple sources using algorithms, such as machine-learning algorithms enabling facial recognition.

40. Furthermore, it is reported that artificial intelligence constitutes an increasingly efficient tool in preventing and tracing the laundering of revenue from illicit trafficking activities. As in the case of algorithms that help online retailers target customers, artificial intelligence and machine learning can support more insightful due diligence policies by interpreting the signals that indicate criminal activity and analysing vast amounts of data.[48]

41. However, at this point in time, artificial intelligence capability often seems to be deficient and unreliable. There have been, for example, multiple instances of artificial intelligence-powered facial recognition technology displaying racial or

[44] *Technology and Labor Trafficking in a Network Society,* p.3.
[45] For further information, see https://polarisproject.org/press-releases/paypal-polaris-join-forces-to-fight-human-trafficking/.
[46] A/CONF.234/16, para. 192 (g).
[47] See also CTOC/COP/WG.7/2020/3, para. 27.
[48] A/CONF.234/11, para. 62.

gender bias and inaccurately identifying targets.[49] Amazon's cloud-based software, Rekognition, in a test by the American Civil Liberties Union, wrongly associated 28 members of the United States Congress with individuals listed in a database of mugshots.[50] Facial recognition technology is already used by some law enforcement agencies to identify suspects much faster and in a variety of operations, but the consequences of racially- or gender-biased misidentification and other mistakes could be devastating for specific groups such as minorities, dark-skinned people, women and undocumented migrants. This technology thus needs to be used within a framework of strict safeguards and oversight, with human inputs and supervision to remove erroneous identifications, in part because, if misused, such technology could lead to abusive government surveillance, corporate manipulation and the end of privacy.[51]

5. Investigative strategies and techniques

42. Investigators have long undertaken operations in cyberspace, including complex joint operations and undercover investigations. In some instances, law enforcement authorities have used social media and online advertisement websites for sting operations to apprehend suspects.[52] Operations and surveillance are conducted in both the clearnet and darknets, for which law enforcement personnel monitor illegal activities using web crawling, by visiting vast quantities of websites and saving their content, and data-scraping technologies, by extracting relevant information from that content for data analysis.[53] However, due to the large degree of anonymity offered by the dark web, it is challenging to associate identified activities with specific jurisdictions and geographical boundaries. The identification of countries where criminals operate from is sometimes done at a later stage in the criminal proceedings, during the investigation and prosecution of specific cases.[54]

43. Technology-based tools can constitute innovative elements of special investigative techniques and useful entry points for addressing crime-related threats such as trafficking in persons. However, caution is needed in their application to ensure responsible and ethical use and avoid unintended consequences. This is particularly important given that many present and future technologies can have serious implications for personal privacy and civil liberties. The widespread use of biometrics and data collection systems can have a destructive effect on privacy if proper control and oversight are insufficient or lacking.[55] Only highly trained and specialized officers should therefore conduct law enforcement operations, in particular on the dark web, operating in full compliance with human rights and the right to privacy.[56]

6. Digital forensics

44. A wealth of evidence may be secured by investigators from smartphones, computers, tablets, external hard drives and any device with a digital memory. Social media postings such as images, videos and information on contacts and locations can be collected, and digital footprints, including the browser history on personal computers and Internet protocol addresses, can be acquired.[57] Network components

[49] See, for example, Joy Buolamwini and Timnit Gebru, "Gender shades: intersectional accuracy disparities in commercial gender classification", in *Proceedings of Machine Learning Research* (2018), and James Manyika, Jake Silberg and Brittany Presten, "What do we do about the biases in AI?", *Harvard Business Review*, 25 October 2019.

[50] American Civil Liberties Union, "Amazon's face recognition falsely matched 28 members of Congress with mugshots", report, 26 July 2018.

[51] CTOC/COP/WG.3/2020/3, paras. 62–63.

[52] See UNODC, *Evidential Issues in Trafficking in Persons Cases: Case Digest* (Vienna, 2017), p. 131.

[53] UNODC, *Darknet Cybercrime Threat to South-East Asia 2020,* p.19.

[54] Ibid., p.15.

[55] See A/CONF.234/11.

[56] Ibid., p.3.

[57] European Migration Network, "The use of social media in the fight against migrant smuggling".

and devices such as routers and servers may be obtained to extract content and/or metadata, including in relation to the identity and location of users, transactions and the senders and receivers of telecommunications and electronic communications. Metadata may assist law enforcement authorities in providing the dates on which images were captured and crimes were committed. Data on images and geo-tagging can also be used to determine the location at which a material event took place.[58]

7. Technology in criminal justice proceedings

45. The COVID-19 pandemic has had a profound impact on the way in which criminal justice systems operate. It has acted as a change accelerator in many regards and led to the enhanced application of technologies and the development of technology-based criminal justice strategies.

46. The Working Group on International Cooperation, for example, has highlighted the ongoing digitization of judicial cooperation efforts and encouraged States to make use of technology in international cooperation to address challenges linked to the COVID-19 pandemic, including the more frequent use of videoconferencing in mutual legal assistance and the use and acceptance of electronic signatures. The Working Group noted that the increase in the electronic transmission of international cooperation requests due to the pandemic has demonstrated that such requests can be sent and answered in a safe, timely, agile and valid manner using electronic means.[59]

47. Furthermore, as a response to the pandemic and the resulting mobility restrictions, certain procedures that required a physical presence in courts can now be conducted online. In addition, new technology has been deployed to keep the criminal justice system functioning, including video platforms that enable parties in a criminal hearing to take part remotely and judges to hold secure hearings.[60] This makes it easier to ensure continuity in criminal justice responses and improves access to justice, although concerns about the security of the information exchanged by these means have been raised, as well as the need to bring national legislation in line with these developments.[61]

48. Under article 24 of the Organized Crime Convention, States parties are obligated to proactively protect witnesses in criminal cases, namely by establishing evidentiary rules which permit witness testimony to be given in a manner that ensures the safety of witnesses, for example, permitting testimony to be given through the use of communications technology. Several practices exist whereby witnesses give testimony remotely, via video links or audioconferencing systems. These practices proved particularly useful during the COVID-19 pandemic. The procedures can be applied at various stages of the criminal proceedings, including detention hearings, initial appearances, preliminary hearings and sentencing.[62]

49. Moreover, the use of online evidence and digital footprints, as mentioned above, may support testimonies in criminal proceedings. Legal and technical requirements must be met to ensure the admissibility of such digital evidence in a court of law, and requirements may vary in practice at the national level.[63]

50. Some encouraging practices have, however, been identified in recent times. For example, in a 2018 trafficking in persons court case in Austria in which 20 women from the Bolivarian Republic of Venezuela were trafficked through the use of Instagram, WhatsApp and Facebook, digital evidence of their interactions with the traffickers was used in the successful prosecution and conviction of the six

[58] UNODC Education for Justice initiative, “Module 4: introduction to digital forensics” and “Module 6: practical aspects of cybercrime investigations and digital forensics”.

[59] CTOC/COP/WG.3/2021/3, para. 3 (b) and (g).

[60] United Kingdom of Great Britain and Northern Ireland, “New tech will help keep the criminal justice system moving during COVID-19 pandemic”, press release, 30 April 2020.

[61] CTOC/COP/WG.3/2021/3, paras 22–23.

[62] CTOC/COP/WG.7/2020/3, para. 37.

[63] See UNODC, Education for Justice initiative, “Module 6: practical aspects of cybercrime investigations and digital forensics”.

perpetrators.[64] In that case, digital evidence enabled law enforcement officials to document victims' working hours, working conditions, threats against them, the logistics of their transport, their daily income and the constant control and abuse exerted over them. Albeit vast, the amount of digital evidence gathered was used only to support the victims' testimonies and could not replace them.

8. Technology for victims of trafficking in persons

51. A wide range of technology-based tools to identify or support victims have been developed, such as applications that allow outreach workers to interview potential victims in different languages or e-learning platforms to teach survivors new job skills. In the context of labour exploitation, in addition to the applications mentioned above, technology solutions based on online surveys and voice-operated applications are used to engage workers broadly to request information about possible exploitative practices in supply chains.[65] Through a partnership with IBM and the Colombian non-governmental organization Pasos Libres, UNODC has organized six "datajams against exploitation" in recent years, in which students compete online to develop technology-based solutions to identify and protect victims of trafficking in persons and support prosecution of the crime.

9. Challenges and human rights considerations

52. Considerations regarding the admissibility of digital forensic evidence require a thorough understanding of criminal, privacy and human rights law, data protection policies and mutual legal assistance channels. In the course of criminal investigations, it is essential that location tracking, data collection and surveillance technologies ensure consistency with human rights, fairness, accountability and transparency standards.[66] Sensitive and personal data should be securely stored and access to it restricted to authorized persons only. Furthermore, cross-border data-sharing among agencies should be in line with national and international legal frameworks, taking into account privacy and confidentiality standards.[67] In addition, the digital privacy of suspects and accused persons and the adequate existence of safeguards and standards for law enforcement authorities in the obtaining of smartphones or computer passwords and in the decryption of private sector messaging applications should be ensured and monitored.[68]

53. The exchange of electronic evidence across borders necessitates expertise to gather, preserve and share it. In addition, the harmonization of cybercrime investigation and digital forensics practices across borders is crucial for such investigations, involving multiple jurisdictions.[69] Therefore, while the use of digital evidence is still limited, it could be critical in numerous criminal proceedings related to trafficking in persons but requires solid capacity strengthening of all the relevant actors as well as legislative changes in some jurisdictions.

---

[64] See details regarding the use of digital evidence in this trafficking case in Isabella Chen and Celeste Tortosa, "The use of digital evidence in human trafficking investigations", *Anti-Trafficking Review*, issue 14, 2020, pp. 122–124.

[65] Issue brief, No. 7 (2017), p. 4.

[66] See also Office of the United Nations High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework* (Geneva, 2011).

[67] Lisa Rende Taylor and Mark Latonero, *Updated Guide to Ethics and Human Rights in Counter-Trafficking: Ethical Standards for Counter-Trafficking Research and Programming* (Bangkok, 2018).

[68] See Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, "Encryption and anonymity follow-up report", research paper, June 2018.

[69] See UNODC, Counter-Terrorism Committee Executive Directorate and International Association of Prosecutors, *Practical Guide for Requesting Electronic Evidence across Borders*, (Vienna, 2019).

C. Previous recommendations of the Working Group on related topics

54. The Working Group on Trafficking in Persons has, to date, formulated more than 250 recommendations advising States parties on the implementation of the Protocol.

55. Prior to the current session, the Working Group has adopted very few recommendations specifically on the use of technology, including information and communications technology, to prevent and investigate trafficking in persons.

56. In examining practical action to address emerging technologies, the Working Group's past recommendations have emphasized that States parties should do the following:

(a) Use new technologies to raise awareness of trafficking in persons through activities such as virtual teaching, thus reaching a wider audience and increasing the possibility of exchanges of good practices;[70]

(b) Consider the possibility of implementing measures to prohibit the dissemination, through any means of communication, of advertisements and publications that promote the exploitation of persons, in particular children, especially sexual exploitation, in order to prevent trafficking in persons and combat sociocultural patterns that sustain gender inequality and discrimination against women;[71]

(c) Take into consideration new methods of recruiting victims of trafficking in persons and take measures to develop targeted awareness-raising campaigns and specialized training for law enforcement and criminal justice practitioners on issues such as the use of the Internet by traffickers, in particular to recruit children;[72]

(d) Consider the role of modern technology and data in preventing and combating trafficking in persons, including during the reflection and recovery periods, and, at a future meeting of the Working Group, the issue of how States identify victims and use confiscated proceeds of offences involving trafficking in persons should be considered.[73]

57. In the compendium prepared by the Secretariat[74] containing an index of recommendations adopted by the Working Group on Trafficking in Persons at its first 10 meetings, relevant guidance can be found on the following topics: criminal justice system, investigations, information-sharing, intelligence-sharing, international cooperation, mutual legal assistance and the private sector.

IV. Key tools and recommended resources

Global Report on Trafficking in Persons 2020

58. The UNODC *Global Report on Trafficking in Persons 2020*, in particular its chapter V (Traffickers' use of the Internet), describes the different steps of the trafficking in persons process happening online.

Issue brief 7 (2019) on human trafficking and technology: trends, challenges and opportunities of the Inter-Agency Coordination Group against Trafficking in Persons

59. In 2019, the Inter-Agency Coordination Group against Trafficking in Persons released an issue brief highlighting how traffickers misuse technology and how this impacts victims. The issue brief describes how technology can be used to fight

[70] CTOC/COP/WG.4/2011/8, para. 38.
[71] Ibid., para 41.
[72] CTOC/COP/WG.4/2013/5, para. 33.
[73] CTOC/COP/WG.4/2018/3, para. 7.
[74] UNODC, *Trafficking in Persons: Compendium and Thematic Index of Recommendations, Resolutions and Decisions* (Vienna, 2021).

trafficking in persons while giving attention to ethical considerations and data protection.

Trafficking in Persons Knowledge Portal and case law database

60. The Trafficking in Persons Knowledge Portal is a core component of the UNODC knowledge management portal known as the Sharing Electronic Resources and Laws on Crime (SHERLOC) portal. The portal includes a case law database, a database of legislation and an annotated bibliography providing information on key articles and publications on the crime.

Practical Guide for Requesting Electronic Evidence across Borders

61. UNODC, the Counter-Terrorism Committee Executive Directorate and the International Association of Prosecutors released in 2019 the *Practical Guide for Requesting Electronic Evidence across Borders* to help practitioners understand, for example, how to preserve electronic evidence or draft a compliant mutual legal assistance request for electronic evidence. The *Practical Guide* assists States in procedures to request or handle electronic evidence.

Leveraging innovation to fight trafficking in human beings: a comprehensive analysis of technology tools

62. The OSCE Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings, together with Tech against Trafficking, in 2020 published a study, *Leveraging Innovation to Fight Trafficking in Human Beings: A Comprehensive Analysis of Technology Tools, Taking Stock of Technology Tools*, describing initiatives developed to combat trafficking in persons and how stakeholders can fully make use of them.

Education for Justice initiative, university module series on trafficking in persons and cybercrime

63. Under the Education for Justice (E4J) initiative, UNODC has developed a series of university learning modules and other tools to assist academics in teaching university students about some of today's most significant threats, including trafficking in persons and cybercrime.