United Nations CTOC/COP/WG.7/2020/3

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

Distr.: General
15 June 2020

Original: English

**Working Group on the Smuggling of Migrants**
Vienna, 8 and 9 September 2020
Item 3 of the provisional agenda*
**Successful strategies concerning the use of technology, including information and communications technology, to prevent and investigate the smuggling of migrants and to mount a robust response to the increasing use of cyberspace by criminal groups**

## Successful strategies concerning the use of technology, including information and communications technology, to prevent and investigate the smuggling of migrants and to mount a robust response to the increasing use of cyberspace by criminal groups

**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 the Smuggling of Migrants at its seventh meeting. It sets out a series of issues related to the current nexus between technology, including information technology, and the smuggling of migrants that the Working Group may wish to address in the course of its deliberations. It provides background information on a range of topics, including the use of modern applications to engage in the smuggling of migrants, as well as to detect, investigate, prosecute and counteract such smuggling, including in cyberspace, as well as challenges and promising practices in the utilization of technology, with due consideration to privacy and human rights safeguards and data protection policies. The paper also lists specific references, resources and tools that States may wish to review to further develop responses to such smuggling.

* CTOC/COP/WG.7/2020/1.

# 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) What are most significant uses of modern technology, including information and communications technology, that hinder crime prevention and criminal justice responses to migrant smuggling operations?

(b) What practical measures have States parties undertaken to adapt and respond to any increased and dynamic use of technology by smugglers?

(c) In curbing the misuse of technology, including in cyberspace, what good practices relating to multi-stakeholder and international cooperation have been identified by law enforcement agencies? How might law enforcement and criminal justice cooperation be improved to respond to such challenges?

(d) What have been the most effective and affordable technology solutions to enhance responses against the smuggling of migrants? What have been the most successful and tailored social media campaigns to create counter-narratives to raise awareness of the risks of migrant smuggling?

(e) How can the United Nations best support States parties' efforts to research, collect and disseminate good practices and effective strategies in the use of technology to counter the smuggling of migrants in times of crisis?

(f) What are the most relevant lessons learned in partnering with the private sector and civil society in the development and deployment of effective technology-based solutions to counter the smuggling of migrants?

(g) What types of privacy and human rights safeguards have States parties adopted in the use of technology in crime prevention and criminal justice responses, including in respect of migrant smuggling?

(h) How do States parties ensure respect for the privacy and human rights of migrants when investigating the misuse of information and communications technology and cyberspace by criminal groups engaging in migrant smuggling?

3. The Working Group might wish to consider the following possible actions by States parties in discussing successful strategies for addressing the smuggling of migrants through the use of technology and in building sustainable responses to the increasing misuse of technology by criminal groups, including in cyberspace:

- Significantly expand data collection and research on the scope, scale and nature of the misuse of technology to facilitate the smuggling of migrants, in particular the misuse of the Internet, social media applications and financial transactions in cyberspace.
- Identify and address gaps in legal systems to ensure the effective investigation and prosecution of technology-facilitated migrant smuggling, including, in particular, in harmonizing laws and enhancing international and cross-border cooperation.
- 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 this crime.
- Support strategies, policies and technology-based solutions that address the global scope of migrant smuggling, such as scalable, online prevention programming or data aggregation tools that facilitate automatized information analysis in support of prevention measures and investigations to counter such smuggling.
- Support the standardized and wider utilization of technological infrastructure by making use of existing technological innovation and ensure that new initiatives and strategic frameworks do not duplicate existing efforts related to technology.

- Build expertise and capacity among practitioners across sectors to allow for the maximum use of technology to prevent and combat the smuggling of migrants.
- Support law enforcement in establishing a presence in cyberspace, conducting pro-active operations, seizing appropriate electronic evidence and using available technology tools.
- Encourage and expand, where relevant and appropriate, effective partnerships and coalitions between various sectors and stakeholders, including international and regional organizations, the public sector, civil society, the private sector and academia, to enhance research, innovation and the development and use of technology.
- Incorporate a gender-sensitive perspective when developing strategies to address the nexus between technology and crime.
- Ensure that any use of technology by law enforcement is consistent with standards concerning human rights, fairness, accountability and transparency.
- Ensure that ethical considerations are fully addressed in the strategic deployment of technology, including large-scale surveillance systems, and that, in harnessing the growing application of machine learning and artificial intelligence to scale up law enforcement efforts, computerized intelligence and software are "debiased" throughout their programming and deployment stages.

# III. Overview of issues and related topics

4. Migrant smuggling is a highly profitable business, with criminal networks thriving on the high demand for smuggling services and the low risk of detection and punishment. The United Nations Office on Drugs and Crime (UNODC) has reported on known smuggling activities that have generated between $5.5 billion and $7 billion in 2016.[1] In 2017, the International Organization for Migration estimated that the smuggling business was worth approximately $10 billion per annum globally.[2] These economic returns are strongly influenced by the capacity of States of origin, transit and destination to prevent, detect and investigate such crime.

5. Against this backdrop, the scale, spread and rate of change brought about by digital technology, including information and communications technology, provides significant opportunities to curb organized crime while accelerating progress towards the achievement of the 2030 Agenda for Sustainable Development.[3] At the same time, unintended consequences of the increased accessibility of technology include its misappropriation by criminal syndicates.[4]

6. Despite growing attention paid by the international community to both addressing the misuse of the Internet and information technology for criminal purposes and leveraging its positive use to address crime, including by aiding investigations, enhancing prosecutions, raising awareness and providing services to those impacted, there are not enough data on the scale of the impact of technology on the crime of smuggling of migrants. The collection and dissemination of promising practices and strategies related to countering migrant smuggling through the use of technology seems to be limited and technology-based systems are not evenly deployed across countries, owing to, among other reasons, challenges concerning the availability of technology infrastructure. The Working Group may, accordingly, wish to consider what has gone wrong in the use of technology, what has worked in its positive use, and how to uniformly apply it, including through enhanced international cooperation.

[1] *Global Study on Smuggling of Migrants 2018* (United Nations publication, Sales No. E.18.IV.9).
[2] Data from the International Organization for Migration (IOM) Migration Data Portal.
[3] See United Nations, High-level Panel on Digital Cooperation, "The Secretary-General's High-level Panel on Digital Cooperation: follow-up process", 17 March 2020.
[4] United Nations Technology Innovation Labs, "Annual report 2019" (New York, 2018).

## 1. The use of technology to facilitate the smuggling of migrants

7. Information and communications technologies have become important and widely used tools for smugglers to transmit information about routes, services and fees. Technology is misused by criminals to facilitate payments, as well as the production and dissemination of fraudulent documentation, posing additional challenges to criminal justice systems in preventing and responding to the rapidly adapting modi operandi of criminals and an ever-changing smuggling criminal market (A/CONF.234/11, paras. 41–48). With regard to the use of technology by those utilizing the services of smugglers, social media platforms are used to maintain communication and exchange experiences between migrants on their journeys.

### Advertising

8. The use of social media platforms by smugglers has grown exponentially in recent times. Smugglers often post information and advertisements which promote routes, services and fees through social media pages that are accessible by migrants and used to exchange views and experiences. The information provided may include advertising images, detailed descriptions of services offered and payment modalities such as payment after delivery of the required visa. Communication with potential clients is directed to a range of different messaging applications, some of which may offer the advantages of anonymity and end-to-end encryption.[5]

9. Among the types of information provided, smugglers may sell various "travel packages", offering modes of transport ranging from air travel to sea transportation. To sell their services, smugglers often deceive migrants by channeling irregular migration movements towards or away from certain transit and destination countries, for example, by relying on the lack of awareness about which countries are members of the European Union. In some instances, social media pages were reported to have been utilized by smugglers pretending to work for non-governmental organizations or European Union agencies tasked with organizing safe passage to Europe by sea. Other smugglers were reported to have posed on social media as "legal advisers" supporting asylum applications for Afghan migrants.[6]

10. Law enforcement agencies in the European Union have reported challenges deriving from so-called "burner apps", which enable criminals to use hard-to-trace telephone numbers when advertising their services on social networks, as well as in communications with irregular migrants or with other members of the criminal networks, thus complicating the investigation of suspects.[7]

### Communication

11. Migrants were also reported to have made increasing use of social media, both at the pre-departure stage, for example, to get into contact with smugglers, and during their journeys to communicate and receive information on migration routes from smugglers. Migrants were also reported to have been provided with satellite phones on board of vessels or across smuggling routes to communicate with smugglers. Mobile technology and its development can also have implications for the relationship between smugglers and migrants. In several social media groups, for instance, migrants can verify the reliability of and share information on certain smuggling services, including with regard to safety, routes and fees. A common function of social media is thus to serve as "consumer forums" (see A/CONF.234/11).

---

[5] European Migration Network, "The use of social media in the fight against migrant smuggling" (October 2016).

[6] Office of the United Nations High Commissioner for Refugees, "From a refugee perspective: discourse of Arabic speaking and Afghan refugees and migrants on social media from March to December 2016" (April 2017).

[7] European Union Agency for Law Enforcement (Europol), European Migrant Smuggling Centre, "4th annual report 2019" (May 2020).

12. The use of social media by migrants differs by nationality, ethnicity and region of origin, and also depends on the availability of the Internet or smartphones, as well as the level of education of the migrant.[8] Displaced Syrians, for instance, were reported to have made extensive use of messaging applications and social media networks to communicate and share insights on their journeys. The use of such tools has also been documented in South Asia, for the selection of smugglers, and in Africa. In destination countries, smuggled migrants publish feedback about smugglers and their services, exposing cases in which smugglers failed, cheated or mistreated migrants. Migrants and refugees also comment on their experiences in the receiving countries, including by sharing information on administrative procedures to stay in the country of arrival.[9]

13. Overall, the use of social media in migrant smuggling has thus been described as having played a significant role in increasing not only the volume but also the effectiveness of smuggling operations, making the crime more difficult to investigate and prosecute, but also potentially safer for migrants. Counter-narratives on social media have been implemented through a number of information and awareness-raising campaigns in recent years to prevent potential migrants from engaging in hazardous journeys. However, those campaigns have often delivered mixed results.[10]

### Financing

14. Technologies are misused for financial payments effected through online payment systems. Payment transfers from destination countries to smugglers can be arranged through commercial money transfer agencies or through the use of money transfer apps. In some cases, money is deposited with an agency and protected by a security code. Once the migrant confirms his or her safe arrival in the intermediary or final destination, the money is released to the smuggler through disclosure of the security code.

15. Payments to smugglers can be made, including by family guarantors, in instalments. The use of cryptocurrencies may increase the ease with which smugglers are able to receive, hide and move money. Such currencies can aid money-laundering and help smugglers avoid investigation and apprehension by providing anonymity and reducing the need to carry large quantities of cash (see A/CONF.234/11).

### Fraudulent documentation

16. Various types of equipment are used to fraudulently create, alter or copy passports. Technology also plays a major role in making fraudulent travel or identity documents available to facilitate the smuggling of migrants.[11]

17. Because they provide users with anonymity and the possibility of real-time information exchange, messaging services are utilized to promote on a large scale fraudulent documents for unlawful entry under false identities. According to the European Union Agency for Law Enforcement (Europol), the online trade in fraudulent documents as enablers of crime will gain in importance for the organized facilitation of irregular migration.[12]

18. Criminals may send counterfeit identity documents via parcel services to facilitators or directly to migrants. Europol, for example, has detected dozens of social media group accounts containing the pictures of thousands of documents. Some of the groups had tens of thousands of followers. Many of the documents were reportedly stolen by organized groups of pickpockets in several European tourism hotspots.[13]

---

[8] European Migration Network, “The use of social media”.

[9] See *Global Study on Smuggling of Migrants 2018*, p. 44.

[10] European Migration Network, “The use of social media”.

[11] For more information on document abuse and counterfeit documents in the smuggling business, see CTOC/COP/WG.7/2019/3.

[12] Europol, “4th annual report 2019”.

[13] Ibid.

## 2. Using modern technology to prevent and address the smuggling of migrants

19. Article 10 of the Protocol against the Smuggling of Migrants by Land, Sea and Air, supplementing the United Nations Convention against Transnational Organized Crime, which entered into force on 28 January 2004, prescribes that States parties shall exchange among themselves, consistent with their respective domestic legal and administrative systems, relevant information on matters such as, inter alia, technological information useful to law enforcement, so as to enhance each other's ability to prevent, detect and investigate the smuggling of migrants and to prosecute those involved. Moreover, it is crucial to ensure adequate human rights safeguards in the application of technology throughout all investigative processes, including in search and seizure operations (see section IV below).

20. As countering the smuggling of migrants remains high on the political agenda of Member States, there is growing interest in finding effective ways to leverage and apply technology to disrupt migrant smuggling networks and mount robust responses to that crime. Indeed, beyond their criminal misuse, as in the case of trafficking in persons,[14] the positive impact of technologies can be harnessed to prevent, detect, intervene and ultimately thwart organized crime.

21. For example, technology is increasingly deployed at borders and offers the opportunity to address smuggling, provided that border forces are sufficiently trained and enabled to identify indicators of smuggling. Technology can also be utilized by law enforcement authorities to identify smugglers by means of machine learning, artificial intelligence and facial recognition systems, as well as data mining applications to identify suspicious transactions.

22. Furthermore, technology can facilitate the recording, storage, analysis and exchange of information relating to the smuggling of migrants. Electronic evidence such as flight bookings and bank records of cash withdrawals abroad assist in proving that transnational crime has occurred. Evidence that suspects have applied fake caller IDs or spyware can be used to rebut claims of innocent association and to prove criminal intent.

### Border control management

23. The use of modern technology to detect illegal border crossing has markedly benefited border surveillance aimed at preventing and countering migrant smuggling, as contemplated in article 11 of the Smuggling of Migrants Protocol, and its application is often highlighted as an effective and practical measure to facilitate the screening of passengers at airports. Several different technologies are reported to be used, for example, thermal imaging equipment and other types of human presence detectors. As with all law enforcement measures, their design and implementation must be done in a manner that respects international and domestic laws, including with regard to human rights.

#### *Automated detection equipment*

24. Advanced technologies in use include X-ray and fingerprint scanners, e-passport scanners and user interfaces, automated e-gates and biometric visas. Countries have highlighted a wide range of devices, including microscopes, lenses for decoding invisible security elements of photos and devices for checking documents, including authenticity control devices and document readers. Others have noted the advantage of automated identity checks, that is, those which allow the entry of passengers on the basis of recognition of biometric information, such as facial and iris recognition, to ensure that human errors caused by potentially tired or distracted border control staff can be avoided. They may also be cost-effective, as fewer staff members are required.

[14] See Inter-Agency Coordination Group Against Trafficking in Persons, "Human trafficking and technology: trends, challenges and opportunities", Issue brief, No. 7 (2017).

25. In the Schengen area, for example, Member States have noted the implementation of the Schengen Information System and the Visa Information System as practical tools and mechanisms to detect the smuggling of migrants across international borders. Other specific examples exist in relation to the checking of documents at entry points. International Criminal Police Organization (INTERPOL) databases and other image-archiving systems such as advanced passenger information systems are also in use to verify information at entry points. All of these systems provide a means for sharing and uploading common data elements relating to passengers seeking to travel. The information gathered is often utilized in dismantling smuggling networks.[15]

26. New kinds of technology-based solutions such as touchless fingerprint and facial scans are reported to be in development and will enable further automatization of border controls and increased security. Such solutions are expected to provide for so-called "biometrics on the move" environments for the benefit of airports and airlines, which are in turn expected to reduce passenger waiting times.[16]

*Artificial intelligence*

27. Globally, as in the case of other business applications, the computational power of artificial intelligence and machine learning is increasingly being explored to leverage responses against the smuggling of migrants. Artificial intelligence can help make predictions, recommendations or decisions independently, on a large scale and without human intervention by combining and analysing intelligence from multiple sources through programmed algorithms.

28. In the context of the smuggling of migrants, for instance, this includes strategies to deploy systems powered by artificial intelligence that can help to assess travellers at border crossings. The artificial intelligence approach leverages the ability to process and exchange a significant amount of data in a short amount of time to produce and rapidly share complete threat assessments. Examples of its recent application in border control include the use of algorithms trained to recognize patterns or behaviour using historical data on travellers obtained from different government agencies and other sources to provide real-time mathematical risk evaluations, and the deployment of high-resolution cameras and radars driven by artificial intelligence using custom software that distinguishes unusual vessel movements from ordinary, busy maritime traffic.[17]

*Imaging and Global Positioning System data*

29. Satellite imagery and Global Positioning System-based tracking systems have enabled the detection and identification of suspicious movements in and around borders. Forms of technical equipment that have been identified, sourced and deployed include X-ray vehicle scanners, thermal scanners and surveillance cameras used to detect smuggled migrants, including in vehicles or safe houses where migrants might be kept while in transit. Such technology and its progressive improvements, if supported by professional, well-trained personnel, can facilitate and foster enhanced border and migration management.[18]

30. Practices at the country and transnational levels include the use of integrated surveillance systems that are able to intercept and surveil vessels at sea at long range

[15] European Commission, European Migration Network, *Practical Measures to Reduce Irregular Migration* (October 2012).

[16] Frontex, "2019 in brief" (January 2020). Frontex, the European Border and Coast Guard Agency, collects and shares information on crime at the borders with national authorities and Europol, and has reported that it is setting up the central unit of the European Travel Information and Authorization System, a new system for granting authorization to travel into the European Union from countries from which no visa is required for entry, which will be used to verify visa applications.

[17] Paul Koscak, "Artificial intelligence turns the tide on securing northern border waterways", United States Customs and Border Protection, May 2020.

[18] IOM, Immigration and Border Management. Available at https://www.iom.int/.

and that are also capable of determining the number of persons on board. Such measures may also enable the easier identification of smugglers, who may, upon interception, attempt to hide among the smuggled migrants. Unmanned aircraft systems, including remotely piloted aircraft systems (RPAS), commonly known as drones, are increasingly used as aerial platforms for sensors such as optical cameras in the visible and infrared spectral ranges to provide long-range detection, recognition and identification capabilities. Additionally, RPAS can acquire a complete picture of vessel movements. As the RPAS industry appears to be in constant development, progressively abating the costs of such technology will enable its broader deployment.

**Investigative strategies and techniques**

31. There is great interest in finding ways for law enforcement authorities to holistically apply modern technology to disrupt smuggling networks and to enable them to take full advantage of evolving technologies such as artificial intelligence, machine learning and digital forensic capabilities to enhance crime prevention and control and the criminal investigation of smuggling cases.

*Artificial intelligence*

32. With regard to countering organized crime, relevant discussions are being conducted at the national level relating to the use of artificial intelligence to support the optimization of police resources in collecting digital evidence. Encouraged by advancements in artificial intelligence that have made robotics "smarter" and capable of replacing human beings in many functions and tasks, an increasing number of law enforcement authorities have adopted such technological advances in a variety of operations.

33. Promising uses of artificial intelligence and robotics that could be applied to investigative and law enforcement operations to counter the smuggling of migrants include the use of modern predictive policing and crime hotspot analytics to optimize law enforcement behaviour detection tools and forecast where and what types of crimes are likely to occur.[19]

34. Furthermore, artificial intelligence and machine learning are reported to provide an increasingly efficient tool to prevent and trace the laundering of revenue from illicit smuggling ventures. As in the case of algorithms that help online retailers target customers, artificial intelligence and machine learning can support more insightful and accurate due diligence policies by interpreting the signals that indicate criminal activity and analysing vastly greater quantities of data in a more reliable manner (A/CONF.234/11, paras. 41–48).

*Mobile technology and digital forensics*

35. Given the reliance of smugglers on mobile technology, including smartphones, a wealth of evidence may possibly be secured from such devices. Social media postings such as images, videos and information on contacts, associates and locations can be collected from social media accounts, and digital footprints, including the browser history on personal computers and Internet protocol addresses, can be acquired.[20]

36. Data stored on digital devices such as computers, smartphones, tablets, phones and any other devices that have digital memory capacity, external storage devices such as external hard drives and Universal Serial Bus flash drives, and network components and devices such as routers and servers could 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

[19] United Nations Interregional Crime and Justice Research Institute and International Criminal Police Organization, "Artificial intelligence and robotics for law enforcement" (2019).

[20] European Migration Network, "The use of social media".

and geotagging can also be used to determine the location at which a material event took place.[21]

### Technology in courts

37. Article 24 of the Organized Crime Convention obliges States parties to proactively protect witnesses in criminal cases, namely by providing evidentiary rules to 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 such as video links or other adequate means. Several practices exist whereby witnesses are allowed to give testimony from a remote location via video links or audio-conferencing systems. For instance, such practices enable smuggled migrants who have returned to their country of origin, or witnesses in different jurisdictions, to give evidence without having to be present in the country where the prosecution occurs.

38. In such cases, witnesses appear on screen in the courtroom, and a camera placed in the courtroom enables them to monitor the proceedings from their location. Such procedures, when enabled through national criminal law, are particularly advantageous for admitting testimonies from witnesses residing overseas, such as those with knowledge of migrant smuggling. The procedures can also be applied at various stages of the criminal proceedings, including detention hearings, initial appearances, preliminary hearings and sentencing. The successful application of such practices depends on the accessibility of the Internet and remote technology solutions.

39. The use and admissibility of video link technology usually depends on several factors, including the inability or unwillingness of the witness to travel, the relative cost of the technology, its online cybersecurity and reliability, the significance of the proposed evidence and the alternative ways available for admitting the evidence.

40. In many ways, the coronavirus disease (COVID-19) global pandemic has led to the enhanced and/or accelerated application of technologies and development of technology-based criminal justice strategies. For instance, as a consequence of the pandemic and the resulting lockdown measures and disruption of mobility globally, 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, making it easier to ensure continuity in criminal justice responses.[22]

41. Furthermore, the use of evidence obtained from social media and/or through the use of technology may support the testimonies of smuggled migrants in related criminal proceedings. Legal and technical requirements must be met to ensure the admissibility of digital evidence in a court of law, and such requirements vary greatly in practice at the national level.

42. Cybercrime investigators and digital forensics experts who handle and/or otherwise process digital evidence must adhere to national policies and best practice guidelines to ensure the admissibility of digital evidence in courts. Such policies set out the technical and legal requirements needed to ensure evidence admissibility. In addition to these requirements, the harmonization of cybercrime investigation and digital forensics practices across borders is essential for investigations, which often involve more than one jurisdiction.[23]

43. Considerations regarding the admissibility of digital forensic evidence thus require a thorough understanding of criminal, privacy and human rights law, data

[21] United Nations Office on Drugs and Crime (UNODC) Education for Justice initiative, University Module Series, “Module 4: introduction to digital forensics” and “Module 6: practical aspects of cybercrime investigations and digital forensics”.

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

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

protection policies and mutual legal assistance channels.[24] Requesting electronic evidence on migrant smuggling across borders necessitates guidelines to help identify steps at the national level to gather, preserve and share electronic evidence, with the overall aim being to ensure efficiency in mutual legal assistance practice. This may entail, inter alia, the mapping of the major communication service providers' relevant procedures and available points of contact, legal frameworks and practical requirements for law enforcement and mutual legal assistance cooperation.[25]

# IV. Challenges and considerations in designing technology-based strategies to prevent and counter migrant smuggling

44. Migrant smuggling facilitated by information and communications technology, in which perpetrators, smuggled migrants and technology platforms may all be in different countries, generates significant challenges concerning jurisdiction, evidence collection, extradition and mutual legal assistance.

45. The lack of cooperation or suboptimal cooperation among national institutions and other practical and legal challenges to international cooperation hinder the development and implementation of strategies to successfully tackle the misuse of technology by criminal networks.

46. Harnessing the positive potential of technology, including information technology, to promptly react to innovative approaches adopted by criminals requires the full utilization of resources and expertise available in very different sectors.

47. Lack of capacity, awareness and expertise among law enforcement authorities, prosecutors and the judiciary due to, among other factors, scarce resources and the complex and evolving nature of information and communications technology hinders the capacity of crime prevention and criminal justice systems to rapidly adapt to the modi operandi of smugglers and capitalize on the opportunities deriving from the use of modern technology to prevent and respond to the crime.

48. As the artificial intelligence and machine learning industry rapidly develops, challenges arise in unbiasing the programming of complex algorithms that might reinforce ethnic or gender stereotypes. This includes, for example, unbiasing artificial intelligence applied to facial analysis technologies, which might not only risk discriminating against ethnic or gender groups, but also produce distorted data and errors.[26]

49. The current level of research on, and collection and dissemination of, available, promising and effective technological solutions and strategies to counter the smuggling of migrants is not sufficient and could be usefully expanded to focus on the adaptability and broader use of successful practices in that regard.

50. The limited availability of technological tools and challenges in accessing often costly technological infrastructure make the obtaining, use and deployment of technology-based solutions fragmented and uneven across countries and regions.

51. The appropriate use of technology supports governments, the private sector and non-governmental organizations in preventing the smuggling of migrants within their respective areas of competence, and in assisting migrants. It is therefore vital to increase the effectiveness of criminal justice responses and to establish incentives for

[24] See the United Nations Convention against Transnational Organized Crime, art. 18, para. 1.

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

[26] For more information on bias in artificial intelligence, see James Manyika, Jake Silberg and Brittany Presten, "What do we do about the biases in AI?", *Harvard Business Review*, 25 October 2019.

and partnerships with online service providers aimed at improving the monitoring, detection and reporting of smuggling-related cases.

**Privacy, safeguards and data protection considerations**

52. Because the smuggling of migrants is global in nature, law enforcement efforts to counter such smuggling typically involve multiple jurisdictions. Particular attention needs to be paid to privacy and data protection considerations, in addition to broader human rights considerations, in addressing such smuggling. It is of fundamental importance that location tracking, data collection and surveillance technologies, including technologies developed by the private sector, all ensure consistency with human rights, fairness, accountability and transparency standards when these technologies are used by law enforcement authorities in any way.[27]

53. As artificial intelligence and robotics increasingly and significantly enhance the surveillance capabilities of law enforcement authorities, it becomes increasingly necessary to address privacy concerns associated with their use, such as when and where it is permissible.

54. The increased use of technology in other criminal justice sectors has already highlighted considerations regarding data privacy, ethics, transparency, accountability and informed consent, the latter becoming increasingly relevant in relation to the use of artificial intelligence by law enforcement.[28] Normative and legislative safeguards are often debated in relation to the use of information obtained by law enforcement on the suspects and/or accused persons and information on third parties, including the migrants, acquired during related investigations, as well as the admissibility of such information in court.

55. Examples of challenging issues in this regard include ensuring that sensitive data are securely stored and that access to the data is restricted to authorized persons only; ensuring that the sharing of data among relevant agencies and between countries is done in accordance with national and international legal frameworks and takes into account privacy and confidentiality standards; establishing consent protocols that are gender- and age-sensitive; assessing risks related to information released by law enforcement authorities that can be connected to the identities of migrants.[29]

56. Ensuring human rights safeguards in all investigatory stages involving suspects and accused persons is also a primary concern. This is particularly relevant with regard to search and seizure operations, for example, in decrypting or intercepting text messages, while recording audio calls, or in the analysis of computer data. Concerns may arise in relation to digital privacy 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 apps.[30]

57. In conclusion, technology-based tools can be useful for stepping up counter-smuggling efforts. However, caution should be exercised in the specific application of such tools to ensure their responsible and ethical use and to avoid unintended consequences. This is particularly important given that some of the technology being rapidly developed and deployed is relatively new and untested, and

[27] 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).

[28] Dunja Mijatović, "Safeguarding human rights in the era of artificial intelligence", Council of Europe, 3 July 2018.

[29] United Nations Inter-Agency Project on Human Trafficking, *Guide to Ethics and Human Rights in Counter-Trafficking: Ethical Standards for Counter-Trafficking Research and Programming* (Bangkok, 2008).

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

therefore, as in the case of its application in similar fields, should be monitored and evaluated with regard to its impact.

### International cooperation

58. The use of technology in international cooperation in criminal matters is the subject of ongoing debate. In 2016, the Conference of the Parties to the Organized Crime Convention, in its resolution 8/1, encouraged States parties to make the fullest and most effective use of available technology to facilitate cooperation between central authorities.

59. Within the framework of the Commission on Crime Prevention and Criminal Justice, an open-ended intergovernmental expert group has been mandated to conduct a comprehensive study of the problem of cybercrime and responses to it by Member States, the international community and the private sector, including the exchange of information on national legislation, best practices, technical assistance and international cooperation, with a view to examining options to strengthen existing and to propose new national and international legal or other responses to cybercrime.[31] In December 2019, the General Assembly adopted resolution 74/247, on countering the use of information and communications technologies for criminal purposes, in which the Assembly expressed appreciation for the work done by the intergovernmental expert group and requested it to continue its work. In the same resolution, the Assembly decided to establish an open-ended ad hoc intergovernmental committee of experts, representative of all regions, to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes.

60. Meeting the increasing need for enhanced international cooperation is greatly dependent upon the availability of resources, including technological resources such as networks for securely transmitting information, equipment for facilitating communication and case management systems for tracking incoming and outgoing requests. The provision of such resources should lead to, among other things, greater efficiency in handling mutual legal assistance requests involving electronic evidence, gained through, for example, the establishment of specialized units within central authorities.[32]

61. Overall, international cooperation contributes to the standardized application of successful strategies and technology-based solutions, and to the effective sharing of information with a view to their uniform use and application.

### Previous recommendations of the Working Group on the Smuggling of Migrants on related topics

62. The Working Group on the Smuggling of Migrants has, to date, formulated more than 170 recommendations advising States parties on the implementation of the Smuggling of Migrants Protocol.

63. The Working Group has not discussed or adopted any recommendations on the use of technology, including information and communications technology, to prevent and investigate the smuggling of migrants prior to the current session.

64. In examining practical action to address emerging technologies, the Working Group's past recommendations have emphasized the following: (a) States parties should consider ways to enhance cooperation at all levels to prevent and combat the crimes covered by the Smuggling of Migrants Protocol that are committed by means of new technologies, in particular the Internet; (b) such cooperation could include the more effective exchange of information and good practices relating to issues of criminalization, investigation and prosecution; and (c) States parties should develop public information campaigns, which could involve the media and Internet-based

[31] General Assembly resolution 65/230, para. 42.
[32] A/CONF.234/11, paras. 64–69.

social networks, in order to raise awareness about the adverse effects of the smuggling of migrants and to warn persons vulnerable to being smuggled, in particular young people and their families, about the dangers involved.

65. In the background paper prepared by the Secretariat containing an index of recommendations adopted by the Working Group on Smuggling of Migrants at its first five meetings (CTOC/COP/WG.7/2019/4), relevant guidance can be found under the following topics: border control and management; criminal justice system, investigations; information-sharing; intelligence-sharing; international cooperation, mutual legal assistance; and responders, private sector.

# V. Key tools and recommended resources

### Global Study on Smuggling of Migrants 2018

66. The *Global Study on Smuggling of Migrants 2018*, the first such study by UNODC, shows that migrant smuggling routes affect every part of the world. The study is based on an extensive review of existing data and literature and provides insight into trends, smuggling routes and the profiles of smugglers and those smuggled.

### Toolkit to Combat Smuggling of Migrants

67. The UNODC *Toolkit to Combat Smuggling of Migrants* provides guidance, showcases promising practices and recommends resources in various thematic areas to assist countries in implementing the Smuggling of Migrants Protocol. Among the tools comprising the *Toolkit*, tool 1 provides an overview of the crime of smuggling of migrants, tool 5 sets out the legislative framework for criminalizing the smuggling of migrants and tool 7 covers law enforcement and prosecution.

### Model Law against the Smuggling of Migrants

68. The aim of the UNODC *Model Law against the Smuggling of Migrants* is to assist States in implementing the Smuggling of Migrants Protocol by facilitating the review and amendment of existing legislation and adoption of new legislation using model provisions. Its chapters cover the criminalization of the smuggling of migrants, protection and assistance measures in respect of smuggled migrants, coordination and cooperation between agencies, cooperation in relation to the smuggling of migrants at sea, and processes related to the return of smuggled migrants.

### Smuggling of Migrants Knowledge Portal and case law database

69. In October 2016, UNODC launched, as a component of the UNODC knowledge management portal known as Sharing Electronic Resources and Laws on Crime (SHERLOC), the Smuggling of Migrants Knowledge 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 smuggling of migrants. The case law database is aimed at enabling judges, prosecutors, policymakers, the media, researchers and other interested parties to broaden their knowledge of how various States use their laws to combat the smuggling of migrants, with the ultimate goal of enhancing the global criminal justice response. The database is an essential tool for increasing the visibility of successful prosecutions, identifying global patterns and promoting awareness of the realities of that crime. The database currently consists of more than 800 cases involving the smuggling of migrants from 43 jurisdictions. The Knowledge Portal can be accessed online at https://sherloc.unodc.org/cld/en/v3/som/.

### Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto

70. The purpose of the *Legislative Guides for the Implementation of the United Nations Convention against Transnational Organized Crime and the Protocols Thereto* is to assist States in implementing the Organized Crime Convention and its Protocols. The publication can be found under the heading “Legislative guide” on the SHERLOC knowledge management portal.

### International Framework for Action to Implement the Smuggling of Migrants Protocol

71. The *International Framework for Action to Implement the Smuggling of Migrants Protocol* is a technical assistance tool to help States parties and non-State actors to identify and address gaps in their response to the smuggling of migrants in accordance with international standards. It draws on international instruments, political commitments, guidelines and best practices to propose a comprehensive approach to preventing and combating the smuggling of migrants. Part two of the *International Framework for Action* contains an overview, in the form of four tables, of the following topics: prosecution and investigation; protection and assistance; prevention; and cooperation and coordination.

### Education for Justice initiative, University Module Series on Trafficking in Persons and the Smuggling of Migrants and on Cybercrime

72. 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. Relevant modules on trafficking in persons and the smuggling of migrants and on cybercrime have been prepared.