United Nations A/HRC/54/22/Add.5

General Assembly

Distr.: General
11 September 2023

English only

Human Rights Council
Fifty-fourth session
11 September–6 October 2023
Agenda item 3
Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development

New technologies and enforced disappearances

Report of the Working Group on Enforced or Involuntary Disappearances*

Summary

In the present report, the Working Group on Enforced or Involuntary Disappearances examines how new technologies are being used against relatives of disappeared persons, their representatives and human rights defenders; can be effectively applied to facilitate the search for disappeared persons; and can be used to obtain and secure evidence of the commission of enforced disappearance.

The Working Group makes several recommendations to States, corporations, civil society organizations, national human rights institutions, academic institutions, donors, international courts and other human rights mechanisms and the Office of the United Nations High Commissioner for Human Rights.

* The present document is being issued without formal editing.

I. Introduction

1. During its 125th session, the Working Group on Enforced or Involuntary Disappearances announced its intention to conduct a thematic study on new technologies and enforced disappearance.

2. To gather relevant information, expert meetings were held on 9 February and 11 May 2022, during the 126th and 127th sessions of the Working Group, respectively. On 17 October 2022, the Working Group circulated a call for inputs.[1] As at 2 August 2023, 29 written submissions had been received from States (5); national human rights institutions (1); civil society organizations, including associations of relatives of disappeared persons (16); and experts or scholars (7).

3. For the purposes of the study, the expression "new technologies" is used in a broad sense, as to refer to technological innovations occurred mostly over the past 20 years, including hardware and software information and communications technology (ICT), encompassing satellite imagery, geographic information science and remote sensing, digital social networks and online datasets, the use of artificial intelligence and development of machine-learning, as well as digital forensic and biodata.

4. New technologies, which today are, for the most part, easily accessible to the general public and cost-efficient, have an ambivalent relationship with human rights-related issues. On the one hand, repressive Governments, as well as other actors such as criminal networks and armed groups, can use new technologies against, among others, human rights defenders and relatives of disappeared persons to curb their fundamental rights, including through surveillance, monitoring, intrusion, disinformation campaigns, online harassment and cyberattacks. Other stakeholders, such as technology corporations, can also play a crucial role through the development of hardware and software used to hamper the activity of human rights defenders and relatives of disappeared persons. On the other hand, new technologies are indispensable in documenting and investigating human rights violations, obtaining and preserving evidence, and promoting accountability, including in cases of enforced disappearance.

5. This study analyses how new technologies are being used against relatives of disappeared persons, their representatives, human rights defenders and civil society organizations and which protective strategies are – or can be put – in place; can be effectively applied to facilitate the search for disappeared persons, ensuring that their fate and whereabouts are established promptly and in a reliable and secure manner; and can be used to obtain evidence of the commission of enforced disappearance, bearing in mind that this international crime is by its own nature shrouded in secrecy and, as such, poses formidable evidentiary obstacles to identify and bring to justice perpetrators.

6. The study is complemented by annexes, containing a glossary; a non-comprehensive mapping of publicly available tools, contacts and resources that may assist in putting in place protective strategies vis-à-vis online threats, facilitate the search for disappeared persons and the corresponding criminal investigations. The Working Group also aims at developing in the near future the presentation of a hypothetical case study illustrating the step-by-step process to investigate a case of enforced disappearance through the use of new technologies, with the objective of showing the implications, both in terms of advantages and existing obstacles.

7. Especially with regard to the search for the disappeared and the documentation of the crime and the promotion of accountability, new technologies offer cost-effective solutions that are likely to have a relevant impact. However, alone, they are incapable of solving all the existing problems and therefore traditional approaches and techniques to documenting, monitoring and reporting should not be abandoned and cannot be entirely replaced by digital material and new technologies. Instead, complementarity between the two strategies should be pursued and promoted.

[1] The call for inputs and the contributions received (excluding those for which confidentiality was requested) are available from www.ohchr.org/en/calls-for-input/2023/call-inputs-thematic-study-working-group-enforced-or-involuntary.

II. Use of new technologies to facilitate or conceal the commission of enforced disappearance, or as a means of reprisal or intimidation

8. The experience of the Working Group and the submissions received show that new technologies, and in particular ICT, are frequently used to facilitate or conceal the commission of enforced disappearance, to hinder the work of human rights defenders and relatives of disappeared persons, and to intimidate or harass them. On occasion, legislation related to technology (especially to the use of social media and cybercrime) is speciously used for the same purposes and for prosecuting human rights defenders and relatives of disappeared persons who employ such means to report enforced disappearances or to denounce abuses.

9. The Working Group received information on enforced disappearances perpetrated where the State had disrupted Internet access and mobile data, either through blanket interventions or more targeted approaches, including by throttling bandwidth and blocking specific media platforms.[2] Albeit the lack of a comprehensive study analysing the concurrence of Internet shutdowns or restrictions and disruptions of access to mobile data with the increase in the number of enforced disappearances, reports received by the Working Group appear to indicate that the limitation of access to the Internet – or its complete shutdown – have been instrumental to the concealment of gross human rights violations, including enforced disappearance.

10. Restrictions on Internet access have an impact on the enjoyment of various human rights and shall be permissible only under specific circumstances and with due guarantees in place.[3] Oftentimes, after Internet connectivity, including the use of media platforms, is restored, the Working Group receives reports of enforced disappearance or harassment against human rights defenders and relatives of disappeared persons perpetrated during the shutdown. In these cases, shutdowns or similar disruptions concretely prevent human rights monitoring and the documentation and rapid report of the crimes at stake and hinder investigations and search activities, ultimately jeopardising the right to know the truth and favouring impunity.

11. The Working Group received an increasing number of communications referring to enforced disappearances allegedly perpetrated to "silence" someone active on social media, for instance persons who have reported abuses perpetrated by the State, commemorated events, or pertain to minorities. Persons subjected to enforced disappearance under these circumstances include human rights defenders, journalists, bloggers, You-tubers, activists, political opponents and religious leaders.[4]

12. A practice detected by the Working Group that seems to amount to a modus operandi common to security forces across the world is that of confiscating all electronic devices of persons later subjected to enforced disappearance and, frequently, of the relatives or any other person present at the moment of deprivation of liberty. Instances where electronic devices of bystanders or potential witnesses to an enforced disappearance were destroyed by security forces, allegedly to erase all evidence of the crime, are also recurrent.

13. In connection with the circumstances described in the paragraphs above, the Working Group recorded a growing number of cases where human rights defenders, including relatives of disappeared persons, have been charged and prosecuted under domestic legislation on cybersecurity. These instances include cases where the persons concerned had published information on enforced disappearance in their accounts and social media or criticised the Government for its alleged involvement or for the impunity in cases of enforced disappearances.[5] In other cases, fake accounts were used to later accuse the person concerned of spreading hate or false information, or jeopardizing national security.[6]

[2] EGY 4/2011; IRN 37/2021; KAZ 1/2022.
[3] A/HRC/50/55. See also A/HRC/RES/44/20; A/HRC/RES/38/7; A/71/373; A/HRC/32/38; and A/HRC/47/24/Add.2.
[4] IRN 27/2012; ARE 1/2017; VNM 4/2020.
[5] EGY 7/2018; NIC 3/2020; NIC 6/2022; ZMB 1/2021.
[6] BGD 1/2022.

14. In addition, international human rights mechanisms have been seized of cases where the use – or even the mere downloading – of a specific application (such as, for example, the messaging application ByLock) was considered by domestic authorities as the sole decisive evidence justifying mass arrests of human rights defenders and political opponents, in some cases leading to their subsequent enforced disappearance or death in custody.[7] These cases are especially troublesome, due to, among others, the lack of clarity on the legal grounds invoked. Another issue of concern relates to the technologies and techniques used by domestic authorities to gather access to the servers, obtain IP addresses and the contents of users' exchanges, which might encompass hacking and infiltrating and stealing the data from the servers. For instance, in the case of ByLock, the server was located in a different State from where the arrests were conducted and prosecutions took place.[8]

15. According to the information received by the Working Group, social media have also been used to conduct smearing campaigns and threaten human rights defenders, including relatives of disappeared persons. The reported attacks on social media against relatives of disappeared persons have often been characterised by gender stereotyping and discrimination[9] and digitally-enabled tools (including troll farms, botnets and fake accounts) have been used to conduct targeted defamation or disinformation campaigns, to stigmatise the disappeared persons or their families, and to enable online harassment, including sexual harassment, and hate speech.

16. Instances of cyberattacks conducted against human rights defenders, including relatives of disappeared persons, encompass sabotage via phishing, malware and ransomware, espionage and supply of disinformation, as well as tainted leaks and doxxing. Often, those targeted are maliciously depicted or labelled as spies, foreign agents, terrorists or smugglers and this, in turn, exposes their accounts to special monitoring, suspension or hate campaigns, in a scenario that is characterised by under-reporting and policy and legal gaps and challenges in holding those responsible accountable, including because of the involvement of different jurisdictions.[10] The Working Group learned with concern about a case where a human rights defender investigating an enforced disappearance was approached through her social media by someone using a false identity, who took advantage of these exchanges to send her links to files containing a malware, thus compromising the security and hindering the privacy of her data.[11]

17. Furthermore, the Working Group has been informed that websites set up by relatives of disappeared persons or their associations, either to honour and preserve the memory of their loved ones or on the issue of enforced disappearance in general, have been subjected to cyber-attacks, which amount to grave and unjustified interferences, a form of re-victimisation and violations of the dignity and reputation of the disappeared persons and their relatives. To the knowledge of the Working Group, these attacks and hindrances – that may be conducted by private actors engaged by the State and non-State actors[12] – are rarely subjected to thorough and effective investigations and remain unpunished, thus facilitating the repetition of similar offences.

18. The Working Group learned about equally recurrent cases where technologies, especially ITCs, were used to spy on relatives of disappeared persons, their representatives or associations and human rights defenders. An especially worrisome development is that of the domestic or transnational use of spyware programmes, such as Candiru, Pegasus or Predator, to maliciously monitor the activities of, among others, human rights defenders, journalists, activists and lawyers, including by determining their location, accessing contact lists to uncover other people, planting incriminating evidence and blackmailing those concerned

[7] European Court of Human Rights (ECtHR), Case Akgün v. Turkey, judgment of 20 July 2021; and Human Rights Committee, Case Açikkollu v. Türkiye, Communication No. 3730/2020, views of 25 October 2022.

[8] Working Group on Arbitrary Detention, Opinion No. 42/2018 of 21 August 2018, para. 33.

[9] A/HRC/50/25 and A/HRC/38/47.

[10] Attempts to overcome some of the mentioned obstacles, within the Council of Europe, are the 2001 Convention on Cyber-crime and the 2022 Second Additional Protocol to the Convention on Cyber-crime on enhanced cooperation and disclosure of electronic evidence (not yet in force).

[11] Amnesty International, Pakistan, les défenseurs des droits humains sont la cible d'une campagne de cyberattaques et de surveillance, 15 May 2018.

[12] On the potential involvement of mercenaries (encompassing business entities, advance persistent threat groups, cyber-militias, individuals and cyber-criminals) in cyber-attacks, see A/76/151.

with personal information.[13] Spyware has been used to surveil relatives of disappeared persons, including, for instance, the wife and fiancée of Jamal Khashoggi,[14] or Mr. Paul Rusesabagina's daughter;[15] or human rights defenders involved in the support of relatives of disappeared persons;[16] or the members of an independent commission mandated to investigate the enforced disappearance of 43 students in Ayotzinapa, Mexico.[17] The pervasiveness of spyware projects a chilling effect on civil society organizations and human rights defenders, including relatives of disappeared persons.[18]

19. Relatives of disappeared persons often live in fear of reprisals, and this often prevents them from reporting abuses, including through the Working Group's humanitarian procedure. Spyware magnifies the risk by allowing unrestricted access to their devices and data. The information gathered through spyware can be used to commit further abuses against relatives of disappeared persons, blackmail them into silence or cause further harm. Data obtained through spyware can also help locating individuals to forcibly disappear them.

20. Spyware programmes can be acquired by Governments, mostly in a context that, in general, lacks independent oversight and sufficient regulation, especially with regard to import, export and use of such a technology. The Working Group learned with interest about the applicable legislation of certain States and existing regional regulations and international arrangements[19] that are aimed at subjecting the sale and transfer of technologies to stricter control. While these are good practices, the applicable legal framework remains weak and fragmented and a thorough and independent scrutiny of the impact of these technologies on human rights should become the rule prior to their sale, transfer and use.[20]

21. Instances where those – be they States, corporations or individuals – responsible for the misuse of surveillance technologies or abuses in their sale and transfer have been held to account are extremely rare.[21] Until regulatory gaps are addressed in a comprehensive manner and corporations fully comply with their obligations under international law as spelled out pursuant to the Guiding Principles on Business and Human Rights, a moratorium on the sale, transfer and use of spyware should be enforced.[22]

22. The Working Group also observed with concern the uncontrolled proliferation of mass surveillance, facial-recognition and similar programmes.[23] By nature, these systems subject

[13] United Nations High Commissioner for Human Rights, Statement on the Use of Spyware to Surveil Journalists and Human Rights Defenders, 19 July 2021; and www.oas.org/en/iachr/jsForm/?File=/en/iachr/media_center/preleases/2022/022.asp. On digital surveillance of journalists, see A/HRC/50/29. Also A/HRC/52/39, paras. 44-50.

[14] A/HRC/4/CRP.1, paras. 68-71.

[15] See www.theguardian.com/news/2021/jul/19/hotel-rwanda-activist-daughter-pegasus-surveillance.

[16] See www.ohchr.org/es/press-releases/2017/07/mexico-un-experts-call-independent-and-impartial-investigation-use-spyware.

[17] The Citizen Lab, Reckless II, Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware, 2017.

[18] A/HRC/51/17 and A/HRC/41/35.

[19] See the 1995 Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-use Goods and Technologies, as amended in 2013; and the Regulation (EU) No. 2021/821 of 20 May 2021 setting up a regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items. See also Japan Foreign Exchange and Foreign Trade Act No. 228 of 1949, as amended in 2005; and Draft U.S. Government Guidance for the Export of Surveillance Technology, Bureau of Democracy, Human Rights, and Labor, U.S. Department of State, 4 September 2019. For a draft on proposed State commitments on international trade in spyware, see A/HRC/52/39, annex.

[20] An initiative in this sense, called "Export Controls and Human Rights Initiative", was launched on 10 December 2021 by Australia, Denmark, Norway and the United States of America.

[21] Notable exceptions are that of the Chamber of the Paris Court of Appeal which, in November 2022, confirmed the indictment of a surveillance company and its executives, due to the fact that the sale of surveillance software to authoritarian regimes resulted, among others, in the disappearance of dissidents; as well as the decision issued on 9 January 2023 by the United States' Supreme Court that allowed the proceedings against the NSO's Group based on a law suit lodged by WhatsApp to continue. See https://www.fidh.org/en/impacts/Surveillance-torture-Libya-Paris-Court-Appeal-indictment-AMESYS; and https://dockets.justia.com/docket/california/candce/3:2019cv07123/350613.

[22] Spyware scandal: UN experts call for a moratorium on sale of 'life threatening' surveillance tech, 2021.

[23] On the unique challenges concerning the use of personal and non-personal data in the context of artificial intelligence, see A/HRC/46/37; and on big data analysis and computational techniques based on artificial intelligence, see A/73/438. See also A/HRC/37/62 on surveillance and the right to privacy; A/HRC/41/43 on the disproportionate impact of artificial intelligence and automation on women; A/HRC/41/35 on private surveillance technologies and human rights; A/74/159 on investigations of digital technologies used for surveillance; and A/HRC/34/60 on governmental surveillance activities.

a significant number of individuals to indiscriminate monitoring, systematically interfering with their human rights. The processing of biometric data, images and information gathered through these means by video-cameras in public spaces has been used to single out certain individuals, including in the context of social protests,[24] who have subsequently been arrested and, in certain cases, forcibly disappeared. Centralised data systems operated through mobile applications used by governmental officials have been allegedly used to perform similar operations of mass surveillance, leading to the targeting of certain individuals considered to be 'suspicious' (including human rights defenders and persons belonging to ethnic or religious minorities) and to their subsequent enforced disappearance.

23. According to the information received by the Working Group, the above-mentioned surveillance technologies, as well as artificial intelligence solutions, drones, thermal imaging sensors, night-vision googles, biometric identification systems, aerial surveillance towers and specialised sensors for detecting mobile phone emissions and tracking devices, have increasingly been used at borders by States and regional agencies to automate processes of identifying and tracking the movement of migrants, refugees and asylum seekers, including in pushback operations, leading – or in some instances amounting – to enforced disappearances.[25] The Working Group learned also about the failure to use data gathered through the said technologies with Search and Rescue teams and authorities, thus failing to prevent migrants in distress from going missing or dying. The Working Group expresses deep concern vis-à-vis such a vicious use of new technologies and notes that the applicable international legal framework – especially concerning the use of artificial intelligence – is flawed and should be urgently strengthened.[26]

24. Cyberattacks on databases containing sensitive information about disappeared persons and their relatives have also occurred. For instance, on 18 January 2022, personal data and other confidential information concerning more than 515,000 people worldwide, stored in the systems of the Central Tracing Agency of the International Committee of the Red Cross were accessed.[27] Among others, platforms containing data on missing and disappeared people, as well as their relatives (including the "Family Links Answers" application and website and the platform "Trace the Face") were compromised. The investigation on the attack showed that it was a very sophisticated one, conducted with the objective of data extraction.

25. Instances as the one here described confirm the urgent need to develop more secure means that can ensure the exclusively humanitarian use of data[28] and safe channels of communication for human rights defenders, civil society organizations , humanitarian actors, human rights bodies and relatives of disappeared persons.[29] In the meantime, the use of available free applications that allow the secure collection, storage and analysis of data is a first mitigation measure to be put in place.[30] The development of open source and easily accessible tools to perform reliable forensic analysis of devices that may have been compromised has also been mentioned as a relevant action to mitigate some of the risks described in this section.[31] Moreover, many of the contributions received by the Working Group emphasized the importance of providing adequate training to members of civil society organizations and relatives of disappeared persons to increase their awareness of risks related to new technologies and mitigate them, including through disseminating information on digital hygiene, data sensitivity, harm, and minimisation. These programmes should allow

[24] A/HRC/44/24.
[25] A/HRC/36/39/Add.2 and A/HRC/47/30. Committee on Enforced Disappearances, draft general comment on enforced disappearances in the context of migration, March 2023, paras. 22, 33 and 44 and footnote 21.
[26] Efforts are ongoing at the EU level to adopt an Artificial Intelligence Act.
[27] See https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000-people.
[28] For instance, the protocol known as SCION developed at the Zurich Polytechnic.
[29] To tackle some of these challenges, ICRC is opening a delegation for cyberspace. The Central Tracing Agency also counts on a digitalisation programme, in the context of which a Missing Persons Digital Matching Programme and an Integrated Online Tracing and Pre-case project have been launched. More in general, see the issue of the ICRC Review (2021) on digital technologies and war.
[30] For some of these applications, see Annex I.
[31] Among others, Amnesty International, Forensic Methodology Report: How to Catch NSO Group's Pegasus, 2021.

civil society organizations to integrate security methods in their work and acquire in-house capacity to diagnose existing risks and recover from threats or attacks.

III. Use of new technologies to facilitate the search for disappeared persons

26. Technological innovations have proved crucial in documenting and raising awareness on the perpetration of gross human rights violations. Data gathered for the purposes of searching for the disappeared can be essential also in the context of criminal investigations, although this aspect is examined more in-depth in section IV. As set forth in Principle 13 of the 2019 Guiding Principles for the Search for Disappeared Persons, the search for the disappeared person and the criminal investigation of those responsible for the crime should be linked and mutually reinforcing.[32]

27. One of the submissions received by the Working Group stressed that, as of today, most technologies used for the search for disappeared persons and the corresponding investigations rely on a binary understanding and classification of gender that ignore non-normative experiences and expressions. Data gathered and processed unreflectively, and lacking a broader understanding of sex-gender spectrums, ignore crucial social and cultural systems and hinder search activities and investigations. An integrated approach to information processing, should incorporate the exhaustive search for details about the person (pre/peri/post disappearance) with a gendered lens and the use of this information across the entire process. The Working Group considers that this will be taken into account when designing data collection tools and technologies for the search for disappeared persons and investigations.[33]

28. It has been brought to the consideration of the Working Group that some of the technologies mentioned in the previous section – spyware, surveillance and facial recognition programmes, and technologies currently employed at borders for migration control – which have been used against human rights defenders and relatives of disappeared persons, including being instrumental to the perpetration of enforced disappearances, could conversely be applied to facilitate the search for disappeared persons and the identification of perpetrators. The Working Group observes that it could indeed be worth exploring this aspect of such technologies, bearing in mind that they shall always be used guaranteeing the respect of fundamental human rights and that, in this realm, the criteria and requirements for corporations to grant access to data – to law enforcement personnel and to third parties – could be re-assessed.

29. The use of open-source intelligence, which relies upon technology to gather and analyse data that are publicly available (e.g. on social media, satellite imagery or mapping tools), can play a crucial role both in the search for disappeared persons and in identifying and securing evidence that allows to identify perpetrators of the crime. It will therefore be mentioned both in this and the following section of the study. For a more exhaustive analysis of all the pertinent aspects, an essential reference is the 2022 Berkeley Protocol on Digital Open Source Investigations ("the Berkeley Protocol"), which contains a practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law.[34] The Working Group considers that the Berkeley Protocol should be taken into account by all stakeholders involved in the search for disappeared persons and in the investigation of enforced disappearance.

30. With regard to technologies that are mostly used to search for disappeared persons, the Working Group notes that many of them have been conceived and are used essentially to search for mortal remains. Albeit the Working Group acknowledges the importance of these techniques and in the following paragraphs analyses some remarkable achievements in this regard, it is worth recalling that the search should be conducted under the presumption that

[32] A/HRC/45/13/Add.3, para. 56.

[33] This applies to semantic, thematic and content data analysis, localization efforts with the use of drones, pattern recognition technologies, forensic facial reconstruction technologies and digital visualization processes.

[34] www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.

the disappeared person is alive.[35] The Working Group considers that more efforts and resources – technical, financial and human – should be devoted to the development of technologies that focus on the early stages of an enforced disappearance and in proactively searching for the disappeared person alive, including through the early tracking of digital traces of the disappeared. Bearing in mind this clarification, a subject that has already been thoroughly analysed and is relevant also for the search for disappeared persons is how new technologies – and in particular digital technologies – can contribute to the discovery and management of mass graves.[36]

31. A technology that has already been in use for some years is that of Light Detection and Ranging (LiDAR), which is a remote sensing method used to examine the surface of the Earth. In the past, in search operations for disappeared persons, it has been mostly used to conduct mapping and to locate burial sites and mass graves.[37] The progresses in the mapping capabilities of LiDAR make it suitable also for search and rescue operations, as it can assist in identifying a human form on any given terrain and in detecting the most effective way to reach the person concerned. LiDAR units are mounted on drones or small airplanes and flown over the areas to be mapped.[38]

32. During its visit to Uruguay, the Working Group learned that it took months for the institution in charge of the search for disappeared persons to get hold of a LiDAR unit, eventually borrowed from Argentina. Once obtained, a number of bureaucratic obstacles were encountered before it could be used. It later emerged that LiDAR units existed in Uruguay and could have been made available by the army (which owns them) at a much earlier stage, thus facilitating the search operations and their effectiveness.[39] This example suggests that institutions in charge of the search for disappeared persons in any country should have this technology at their disposal and adequate rules should be in place to avoid undue hindrances to its use. Similar considerations apply to the use of sound, navigation and ranging (known as SONAR) scanners, drones and ground penetrating radars.

33. Besides aerial images, satellite imagery with a significant spatial resolution is today accessible also beyond the domain of Governments and it can facilitate the search for disappeared persons. For instance, it has been used to document the establishment of official or secret places of detention, locate torture sites,[40] and to identify mass graves or burial sites.[41] The passing of time may pose obstacles to the use of this technology in the search for disappeared persons, but the employment of reverse image search tools, photogrammetry, and cartographic regression can mitigate some of the challenges.

34. The Working Group learned about the use of geospatial analysis, in combination with spatial statistics and remote sensing to identify potential search areas for mass graves in Baja California, Mexico.[42] Researchers used spatial clustering and clandestine space and integrated them into a spatial model within a Web application, with the aim to reduce the

[35] See Principle 1 of the 2019 Guiding Principles for the Search for Disappeared Persons.
[36] A/75/384.
[37] See www.coloniadignidad.cl/actualidad/noticias/la-tecnologia-lidar-en-la-busqueda-de-personas-detenidas-desaparecidas-en-las-ultimas-dictaduras-de-argentina-y-chile/. See also Corcoran A., Mundorff A.Z., White D.A. and Emch W.L., A Novel Application of Terrestrial LIDAR to Characterise Elevation Change at Human Grave Surfaces in Support of Narrowing Down Possible Unmarked Grave Locations, 289 Forensic Science International, 2018, pp. 320-328.
[38] It is used for instance by Frontex during its operations, see PowerPoint Presentation (europa.eu). See also Artificial Intelligence-based capabilities for the European Border and Coast Guard (europa.eu) more in general for Frontex artificial intelligence capabilities.
[39] A/HRC/54/22/Add.1, para. 21.
[40] Amnesty International, Cameroon's Secret Torture Chambers, 2017; and Humanitarian Research Lab, Extrajudicial Detentions and Enforced Disappearances in Kherson Oblast, 2022.
[41] Seewww.icrc.org/en/document/joint-statement-tripartite-commission and www.icrc.org/en/document/gulf-war-9-human-remains-identified-and-returned-their-families-after-30-years.
[42] The technique employed relied upon the consideration of the spatial distribution of hidden graves, the spatial visibility and accessibility of specific areas, and the accumulation of nitrogen identified through satellite images. For a full reconstruction, see Finding clandestine graves: using geospatial analysis to search for missing persons in Baja California, Mexico – Citizen Evidence Lab – Amnesty International; and Silván-Cárdenas J., Alegre-Mondragón A., Ruiz-Reyes J., 'Geospatial Analysis of Clandestine Graves in Baja California: New Approaches for the Search of Missing Persons in Mexico', in Tapia-McClung R., Sánchez-Siordia O., González-Zuccolotto K., Carlos-Martínez H. (eds), Advances in Geospatial Data Science, Springer, 2022, pp. 29-40.

areas with the highest probability of finding more clandestine graves, based on the original information of 52 burial sites located by the attorney general. This led to a substantial reduction (<10%) of the search areas, producing a model that ensures that search areas are within practical distances from urban settlements. This methodology brought encouraging results and is worth further consideration and analysis.

35. Technologies are crucial also in terms of forensic sciences and proved instrumental in determining the fate and whereabouts of disappeared persons, including through the use of biometric data and the setting up of genetic databases.[43] Interoperability of such databases remains a challenge, both within States (especially federal ones) and internationally. The Working Group learned about global databases[44] aimed at supporting DNA kinship matching and considers that these efforts should be further pursued. According to the information received, forensic bioinformatics play an increasingly significant role in the verification of DNA analysis, thus contributing to the realisation of the right to know the truth.

36. The issue of secure data collection and exchange – crucial to facilitate the search for disappeared persons – is proving especially challenging in cases involving migrants. On the one hand, there is a generalised reluctance in sharing data on those disappeared, out of fear that, in the absence of adequate protection, the collected information may be used against the persons concerned or their families. On the other hand, there may be several databases, often located in different countries, that contain relevant information, but they do not offer inter-operativity, including because they do not follow harmonised criteria with regard to the data collected, eventually frustrating the search attempts. Similar problems arise where mortal remains that may belong to a disappeared person are located in a State, but databases containing genetic data necessary to perform a reliable identification are scattered across different countries.

37. In this area, additional technical, financial and human resources are needed, with a view at, among others, developing technologies to overcome these obstacles in a secure manner.[45] Initiatives directed at enhancing biometric and genetic inter-force identification, especially at borders, should be guided by this spirit, bearing in mind that alleged security considerations cannot prevail over the guarantee of fundamental human rights, including the right to know the truth in connection with possible enforced disappearances.

38. The Working Group received information on cases where, through the footage of CCTV in the place where the disappeared person was allegedly taken, relatives or their representatives tracked the number plate of the vehicle used and its subsequent itinerary. Crossing this information with the call-logs and mobile data of the disappeared, they gathered relevant indications about the possible whereabouts of the person. In certain cases, similar information was obtained through user-generated content (e.g. photos or videos uploaded on social media). These steps have been oftentimes left to the initiative of relatives of disappeared persons, their representatives or other members of civil society, frequently exposing them at risks, while authorities do not seem to have developed a systematic practice.

39. Relatives of disappeared persons frequently use social media or messaging applications to proactively search for their loved ones.[46] Whilst this can facilitate establishing the fate and whereabouts of disappeared persons, there are concerns on whether such highly sensitive data are adequately and securely stored and protected, also bearing in mind the instances of cyberattacks, data breaches and hacking referred to above. It has been submitted to the Working Group that, even where rigorous data protection regulations exist, they could be amended to include clauses dealing specifically with the issue of enforced disappearance, for

[43] Argentine Forensic Anthropology Team, Forensic Guide to the Investigation, Recovery of Human Skeletal Remains, 2020.

[44] I-Familia, managed by INTERPOL.

[45] ICRC, Core Dataset for the Search for Missing Migrants, 2021; and Laczko F., Singleton A., Black J. (eds.), Fatal Journeys Vol. 3: Improving Data on Missing Migrants, International Organization for Migration, 2017.

[46] E.g., in the application Telegram more than 200 pictures of persons reported missing in Ukraine – some of which victims of enforced disappearance – are published daily. Neuville M., Les réseaux sociaux, principaux alliés dans la recherche des personnes disparues, 2022. In other contexts, TikTok is used to report abuses, including enforced disappearance.

instance foreseeing procedures of "quick freeze" allowing data preservation upon request of a person who feels in danger.

40. Some technologies may not be applicable to, or relevant for, cases where the person disappeared prior to the existence of smartphones or the Internet. Enforced disappearance is a permanent crime and a continuous violation of multiple human rights[47] and thus the search is a continuous obligation.[48] It is therefore essential to further invest in the development of technologies that can be instrumental also in clarifying cases where the disappearance commenced decades ago. New technologies can bring significant results in this regard, but traditional human-centred techniques must also be maintained and used together with the former.

41. The effective search for disappeared persons often requires going through, and cross-check multiple archives that may be composed of hundreds of thousands of pages and terabytes of files. Technologies can facilitate the task and boost the effectiveness of the consultation of archives.[49] The Working Group learned about the existence of a programme called Angelus,[50] developed in Mexico by mathematicians in collaboration with the National Search Commission and that relies upon the use of a network of algorithms, artificial intelligence and machine-learning. This programme represents a good practice, as it allows to process and cross a huge quantity of data and to detect the existence of patterns, contexts and connections that can facilitate the search for disappeared persons.

42. Data mining, performed either manually or through different technologies based on algorithms, holds great potential with regard to gathering information that may prove of crucial importance both for the search for disappeared persons and the promotion of accountability. An example are the remarkable results obtained both in terms of establishing the fate and whereabouts of disappeared persons and identifying perpetrators, based on the information retrieved from the Historic Archive of the Guatemalan National Police, which was discovered in 2005.

43. This instance is emblematic of how technology and the application of adequate techniques, including statistical methods, in terms of multi-stage random sample of documents, data model and coding frame, is instrumental in preserving, digitalising and inspecting a huge quantity of data, in the impossibility to systematically examine each individual document.[51] Computational access, optical character recognition, handwriting recognition, as well as facial and voice recognition to analyse audio-visual material,[52] are crucial tools in this domain. Moreover, the example shows the pivotal role played by international cooperation, be it in the context of civil society organizations, academia,[53] or at the intergovernmental level.[54] Similar considerations apply also to massive amounts of data uploaded in social media, or the documentary by-product of truth-seeking initiatives, that may contain evidence of international crimes, including enforced disappearance, and require adequate and well-regulated long-term preservation and processing. Forensic tools, including through the comparison of databases created by different stakeholders, are essential to ensure validation, identification, analysis, interpretation, documentation and presentation of digital information derived from digital sources and archives.

[47] Article 17 of the Declaration on the Protection of All Persons from Enforced Disappearances; General Comment on Enforced Disappearance as a Continuous Crime; and article 8 of the International Convention on the Protection of All Persons from Enforced Disappearance.

[48] Principle 7 of the 2019 Guiding Principles for the Search for Disappeared Persons.

[49] On how technologies can be instrumental in advancing transitional justice (through documentation, digitalisation and memorialisation), see the special issue of 2019 of the International Journal of Transitional Justice.

[50] Santiago V., Angelus: el algoritmo que escarba en la Guerra Sucia, 2022.

[51] https://hrdag.org/guatemalan-national-police-archive-project/.

[52] Donida Labati R. et al., Automatic Face Recognition for Forensic Identification of Persons Deceased in Humanitarian Emergencies, 2021.

[53] The Human Rights Data Analysis Group designed the strategy and implemented the techniques that enabled the remarkable outcomes mentioned. The University of Texas, through a collaborative project, set up and hosts the digital archive.

[54] A notable example of inter-State cooperation intended to build forensic and documentation capacities is the Condor Document Archives project by the Southern Common Market (MERCOSUR). The United Nations has supported several initiatives on data identification and collection worldwide (A/HRC/36/50/Add.1, paras. 5, 8, 35, 36, 58).

44. The Working Group also received information that illustrates how digital tools – often created by civil society organizations – can be used not only to search for disappeared persons, but also – through interventions at early stages – to prevent arbitrary detentions from turning into enforced disappearances.[55] These tools offer free and secure options that help relatives of disappeared persons navigating the meanders of bureaucracy and quickly obtaining information that can prove vital, or managing their case file before domestic authorities.[56] Moreover, it has been suggested that existing applications used in the context of domestic violence,[57] could be adapted to prevent enforced disappearances or to facilitate search activities. The Working Group received information on how migrants fearing to be at immediate risk of being forcibly disappeared have used social media to share video footage of their location and live geo-coordinates and this has proved instrumental in establishing their fate and whereabouts and, on occasions, in collecting evidence of crimes perpetrated against them.

45. The Working Group acquired knowledge about studies aimed at exploring how the use of artificial intelligence and machine learning, through network smartphones data analysis, can contribute to establish the whereabouts of disappeared persons. These studies are at an embryonal stage and may prove crucial to reach the clarification of many cases, as shown also by successful experiences launched by civil society organizations which use artificial intelligence and digital advertising technologies to locate missing children.[58] These studies and experiences should be encouraged, including through funding and international cooperation. Nevertheless, the existence of significant socio-economic differences must be taken into consideration, with the aim to provide adequate support and ensure access to these new technologies to developing countries. In this context, States must cooperate and afford each other the greatest measure of mutual assistance in searching for, locating and releasing disappeared persons and, in the event of death, in exhuming and identifying them and returning their remains.[59]

IV. Use of new technologies to document cases of enforced disappearance and to hold perpetrators accountable

46. The use of technologies in the documentation of gross human rights violations and in the promotion of accountability, especially through open-source intelligence, has been the subject of growing attention[60] and of seminal reports published by other UN Special Procedures.[61] As mentioned, technologies can play a crucial role in obtaining data and information that allow to clarify the fate and whereabouts of the disappeared, but also to identify those responsible for the crimes concerned. However, findings acquired through such means must be secured in a way that stands up to scrutiny, including in the context of criminal proceedings, whereby the applicable standard of proof is "beyond reasonable doubt". Ascertaining the source of the evidence collected through technologies and excluding that it has been subjected to forgery or manipulation can be especially complex. Moreover, machine-learning deletion algorithms run by platforms such as Google or Facebook may quickly erase digital contents, thus leading to the loss of evidence that becomes virtually impossible to recover.

[55] E.g. the chatbot BUSQUEMOS, developed by the Mexican NGO Documenta, which facilitates the early search of disappeared persons who may be held in different detention facilities, ranging from prisons, police stations, army barracks or migration retention centres to institutions of mental health and hospitals. It offers free support, through interactions that last less than 5 minutes and that do not require users to disclose any sensitive data.

[56] E.g. the platform Nosomosexpedientes, developed by the Mexican NGO Centro de Derechos Humanos Miguel Augustín Pro Juárez, which supports families in their search efforts and in the management of their case files before domestic authorities.

[57] Reference was made to the platform Save You.

[58] See the platform launched in 2018 by the International Centre for Missing and Exploited Children.

[59] International Convention on the Protection of All Persons from Enforced Disappearance, art. 15.

[60] Among others, the symposium published in 2023 by Opinio Juris on fairness, equality, and diversity in open source investigations; the special issue published in 2021 by the Journal of International Criminal Justice on new technologies and the investigation of international crimes.

[61] A/HRC/29/37 and A/65/321.

47. This can be especially challenging in cases of enforced disappearance, a crime that, by nature, is shrouded in secrecy and characterised by concealment and "absence", rather than by the presence of manifest pieces of evidence. In this sense, while it may be relatively easier to document through new technologies two of constitutive elements of the crime (i.e. the deprivation of liberty of the victim and the affiliation of the perpetrators), the element of concealment of the fate or whereabouts of the disappeared poses more obstacles, as well as, where applicable (i.e. pursuant to the definition of enforced disappearance as a crime against humanity contained in the Rome Statute of the International Criminal Court),[62] that of the intention of removing the disappeared person from the protection of the law for a prolonged period of time.

48. As noted in one of the submissions received, the peculiarities of enforced disappearance call for an "aggregated" application of open-source intelligence, each of them targeting a specific element of the definition of the conduct. The "hidden" character of the crime, as well as the presence of a specific mental element in the definition of enforced disappearance as a crime against humanity contained in the Rome Statute of the International Criminal Court, makes it unlikely that open-source intelligence will provide single-handedly all the material qualifying a specific conduct as an enforced disappearance. Yet, it could offer useful indications on the identity of the victim, the act of depriving liberty, the location of the detention, the identity and the affiliation of the perpetrator. Open-source intelligence could even be used to document the contextual element of the crime in international criminal law – i.e., the presence of an attack directed against a civilian population, its widespread or systematic character, and the commission of the act as part of the attack.

49. Finding and piercing together corroborating information through technologies – and especially ICT – requires formidable efforts in terms of targeted investigation, verification and preservation, which should always be done in a systematic and professional manner, especially to ensure the chain of custody and, where necessary, admissibility in court at a later stage. Throughout the process, from the collection of evidence through technologies until its appearance in court, ethical and security implications must be adequately taken into account. In particular, risk-assessment should include consideration of privacy and data protection aspects, the obtaining – where feasible – of informed consent from relevant individuals and communities and Demographically Identifiable Data-based risks.

50. The first hours and days after the persons' deprivation of liberty are crucial to obtain data that could soon be erased or manipulated. The existence of publicly available satellite imagery, digital social networks and camera-enabled smartphones offers valuable data that can be accessed in a relatively easy and cheap way and provide evidence of the commission of crimes, including enforced disappearance. The Working Group learned with interest about applications and software programmes that capture and preserve evidentiary copies of online contents and audio-visual material, embedding them with the necessary meta-data to demonstrate authenticity in court, and facilitating contents annotation.[63]

51. The preservation of the chain of custody of evidence obtained with the use of new technologies is essential to ensure the authenticity of the material collected. The Berkeley Protocol enshrines the fundamental principles to be respected in this context and should be disseminated and implemented, along with other guidelines on the matter elaborated by civil society organizations.[64] Aspects that require special attention are related to the inherent fragile nature of technologies, the need to standardise the technical management of datasets archived and the validation of such data. The Working Group learned about programmes that, often using artificial intelligence, allow assessing the integrity of digital images and detecting falsified media. These technologies offer significant help in the collection of evidence admissible in court.

52. Video footings and images posted on social media or collected through body or dash-cams can contain evidence of the commission of gross human rights violations, including

[62] Art. 7, para. 2 (i), of the 1998 Rome Statute of the International Criminal Court and the domestic criminal legislations that reproduce the definition of the crime contained therein.

[63] See Annex I. The meta-data concerned include, as a minimum, a timestamp, location data and a unique alphanumeric code. They must then be stored in a secure manner, preferably after encryption.

[64] See, among others, the methodology for online open source investigation into incidents taking place in Ukraine since 24 February 2022 published by Bellingcat and Global Legal Action Network.

enforced disappearance, and they have been accepted as valid evidence in court, by international human rights bodies and inquiry commissions. For instance, the European Court of Human Rights considered a video posted on Youtube valid proof of the ill-treatment to which a disappeared person had been subjected to after having been deprived of his liberty.[65] The International Criminal Court issued an arrest warrant based primarily on evidence collected from social media posts;[66] the Independent International Fact-Finding Mission on Myanmar relied upon audio-visual data and written posts on social media as evidences to call for the investigation of international crimes;[67] and domestic courts admitted open source evidence in trials concerning international crimes.[68] The possibility to assess, verify and ultimately admit evidence collected through technologies depends on the capability of each court and the skills and knowledge of the personnel, which may vary significantly, especially at the domestic level. The Working Group considers that States must adopt all necessary measures in this regard, including by securing the necessary economic, technical and human resources and providing regular trainings to the authorities concerned.

53. The Working Group was informed that new technologies – including geo-location programmes, flight tracking, network analysis, 3D modelling, remote sensing, audio analysis, synchronisation, and photogrammetry – have already proved effective in reconstructing crime scenes and in tracking alleged perpetrators of crimes and human rights abuses. Their use should therefore be envisaged as part of a regular investigation protocol concerning enforced disappearance. A combination of techniques (e.g. satellite imagery, digital mapping, analysis of video footages and chrono-location) has also been successfully used to collect evidences of enforced disappearances of migrants and to establish their fate and whereabouts.[69]

54. The Working Group received information on a growing number of cases where, in the face of the indifference or inactivity of the authorities, relatives of disappeared persons or their representatives, or multiple civil society organizations through crowd-solving exercises, managed to collect, using technologies, information on the circumstances of the disappearance, and the identity or affiliation of the perpetrators. They used social media, the Internet, CCTV, call-logs, mobile data tracking and geo-localisation or satellite imagery. Whilst these experiences led to meaningful results, they also exposed the persons concerned to great risks, as illustrated in section II.

55. The Working Group notes that the burden to collect this kind of data through technologies cannot be left to the relatives of the disappeared and their representatives, while authorities do not seem to search for, verify, analyse and secure these evidences in a systematic manner, although they are under an obligation to do so. States need to intensify their efforts and take all necessary measures to strengthen the capacity of the competent authorities to use technologies in the investigation of enforced disappearance. States shall afford one another the greatest measure of mutual legal assistance in connection with criminal proceedings brought in respect of an enforced disappearance, including the gathering and supply of all evidence at their disposal that is necessary for the proceedings.[70]

V. Conclusions and recommendations

56. **As in many aspects relevant to new technologies, their relationship with human rights – in this case in the realm of enforced disappearance – is ambivalent. On the one hand, new technologies, and in particular ICT, are frequently used to facilitate or**

[65] ECtHR, Case S.T. and Y.B. v. Russia, judgment of 19 October 2021, paras. 10, 22, 48 and 80.

[66] See the arrest warrants issued respectively in 2017 and 2018 by the International Criminal Court in the case Prosecutor v. Al-Werfalli. In recent years, the Court's Investigative Division established a Scientific Advisory Board and a Technology Advisory Board.

[67] Irving E., The Role of Social Media is Significant: Facebook and the Fact-Finding Mission on Myanmar, in Opinio Juris, 2018.

[68] Among others, Report by the European Union's Eurojust Genocide Network, 2018, that illustrates examples from Germany, Finland and Sweden.

[69] Among others, www.borderviolence.eu/pushback-from-north-macedonia-visual-analysis/ and https://forensic-architecture.org/investigation/pushbacks-across-the-evros-meric-river-the-case-of-parvin.

[70] International Convention on the Protection of All Persons from Enforced Disappearance, art. 14.

conceal the commission of enforced disappearance, to hinder the work of human rights defenders and relatives of disappeared persons, and to intimidate or harass them. Technologies are developing at a rapid pace and they are often traded and used without the application of human rights due diligence by both States and corporations, in the absence of a sound regulatory framework that takes into account international human rights law, foresees independent oversight and promotes accountability and offers an effective remedy in case of violations.

57. **The Working Group is especially concerned at the use of Internet shutdowns and targeted connectivity disruptions; spyware programmes; targeted and mass surveillance, including gait and facial-recognition; cyberattacks and Government-sponsored troll factories; and the specious use of technology-related legislation to suppress dissent and target human rights defenders and relatives of disappeared persons.**

58. **With regard to the search for disappeared persons and the documentation of the crime and the promotion of accountability, new technologies can offer cost-effective solutions that have already proved useful and are likely to have further relevant consequences. The Working Group emphasizes that there should not be over-reliance upon new technologies in this realm and expectations must be realistic: albeit they are going to facilitate the processes concerned, they are not going to solve all the existing problems. Traditional approaches and techniques to documenting, monitoring and reporting should not be abandoned and cannot be entirely replaced by digital material and new technologies.**

59. **Complementarity between these strategies should be pursued and actively promoted and traditional human-centred processes must be fomented and strengthened accordingly. In parallel, access to new technologies shall be conceived in a way that does not reproduce or deepen existing digital divide and socio-economic differences and no developing country or relevant stakeholder can be left behind.**

60. **The fact that new technologies offer cost-effective solutions that could make significantly advance both the search for the disappeared and criminal investigations and that some of the relevant tools are easily accessible and can be used also by civil society organizations and associations of relatives of disappeared persons is a positive development that can prove instrumental in offering a better protection against enforced disappearance.**

61. **The Working Group encourages civil society organizations to explore these possibilities and to strengthen their capacities, but it reaffirms that the search for the disappeared and the corresponding criminal investigations are international obligations of States, that cannot leave the burden entirely on civil society and relatives of the disappeared and rely solely on their initiative. States should adopt measures to include new technologies in search activities and criminal investigations. States are also under an obligation to cooperate and afford one another the greatest measure of assistance in these domains.**

62. **The Working Group notes that cooperation among different stakeholders, including States, corporations, civil society organizations, National Human Rights Institutions, academic institutions and donors is indispensable and, as such, it should be promoted. The following recommendations reflect this understanding. In particular, the Working Group encourages strengthened coordination and cooperation among different stakeholders to forge alliances to detect risks concerning new technologies and enforced disappearance, devise mitigation strategies and effective measures to overcome the obstacles identified and to promote tools to support those directly affected, including human rights defenders and relatives of disappeared persons. There is a shared responsibility to ensure that new technologies are developed and used within a human rights framework, ethically and responsibly.**

63. **The Working Group commits to regularly monitor the issue of new technologies and enforced disappearance and to systematically include remarks and recommendations concerning this subject in its activities, including in communications, urgent appeals, allegations, referrals, prompt intervention letters, country visits and awareness-raising.**

The Working Group also offers assistance to States on the subject through cooperation and advisory services.

64. **The Working Group calls on all concerned stakeholders to regularly engage and cooperate with it and report on the negative impact of new technologies in the enjoyment of human rights, especially of human rights defenders and relatives of disappeared persons, as well as on progresses made with regard to the use of new technologies in the search for disappeared persons and in the investigation and promotion of accountability.**

65. **To the above ends, the Working Group recommends that States:**

(a) **Refrain from imposing Internet shutdowns, and restrictions to the access to communications or specific social media platforms;**

(b) **Maximize Internet access and remove the multiple obstacles standing in the way of communications;**

(c) **Adopt all necessary measures to ensure that human rights defenders, relatives of disappeared persons, journalists and social-media users can exercise without undue interference their right to hold opinions and freedom of expression online (e.g. through social media, blogs or similar accounts) without being criminalised for reporting or denouncing enforced disappearances; measures should also be taken to ensure that legislation on cybersecurity is not speciously applied to curb dissent;**

(d) **Ensure that the downloading and use of an application cannot be relied upon as sole or decisive evidence of a criminal offence;**

(e) **Ensure the training of law enforcement personnel, civil or military, and public officials on the fundamental guarantees to be ensured upon the arrest of any individual, in particular as to the norms applicable to confiscation, inspection or destruction of electronic devices; and holding accountable those who fail to respect such rules;**

(f) **Take all measures to prevent cyberattacks, smearing and disinformation campaigns against human rights defenders, including relatives of disappeared persons, conducted through phishing, malware, ransomware, espionage, tainted leaks, troll farms and doxxing, and investigate all relevant instances with a view at identifying, prosecuting and sanctioning those responsible and offering redress to victims;**

(g) **Impose an immediate moratorium on the export, sale, transfer, use or servicing of privately developed targeted and mass surveillance tools, including spyware, facial-recognition and similar programmes, until a human rights-compliant safeguards regime is in place;**

(h) **Develop and enforce without delay a legal framework by which the licensing of any technology, and especially targeted and mass surveillance technologies, would be conditional upon a national human rights review and corporations' compliance with the Guiding Principles on Business and Human Rights; the said framework must ensure that the transfer, sale and acquisition of targeted and mass surveillance technologies is subject to public consultation and oversight;**

(i) **Take all necessary measures to investigate, prosecute and hold accountable individuals, corporations and States responsible for human rights violations related to the sale, transfer and use of targeted and mass surveillance technologies;**

(j) **Ensure that individuals or civil society organizations targeted can exercise their right to an effective remedy and obtain reparation;**

(k) **Guarantee that collection, retention and use of biometric and genetic data is regulated in law and in practice, is narrow in scope, transparent, necessary and proportionate to meeting a legitimate security goal, and is not based on any distinction, exclusion, restriction or preference based on race, colour, descent or national or ethnic origin;**

(l) **Review, through a multi-disciplinary process, the adequacy of the applicable policies and legal frameworks, to devise strategies to prevent and address negative impact on human rights generated by the use of new technologies, including machine-learning and artificial intelligence;**

(m) **Ensure that mass and targeted surveillance technologies, as well as AI and machine-learning solutions, are not used at borders for the purposes of performing pushback operations that may lead, and in certain cases amount to, enforced disappearance. Data on migratory movements gathered through these technologies should be used for facilitating search and rescue operations and for humanitarian purposes;**

(n) **Ensure that technologies used for the search for the disappeared and the corresponding investigations incorporate the collection and analysis of details about the person concerned with a gendered lens, to encompass non-normative experiences and expressions;**

(o) **Proactively search for the disappeared person alive and adopt the measures and resources necessary to develop and apply technologies that focus on the early stages of an enforced disappearance;**

(p) **Adopt all the necessary measures to guarantee that the authorities in charge of the search for disappeared persons and the corresponding criminal investigations count on adequate financial, human and technical resources and, in particular, state-of-the-art technologies (including LiDAR, SONAR units, drones, satellite imagery, etc.) and are regularly and duly trained, including on the application of the Berkley Protocol;**

(q) **Cooperate with other States, affording one another the greatest measure of mutual assistance in the use of technologies to facilitate the search for disappeared persons and regarding legal assistance in connection with criminal proceedings brought in respect of an enforced disappearance, including the gathering and supply of all evidence at their disposal that is necessary for the proceedings;**

(r) **Ensure the inter-operability of genetic databases that can be instrumental in the search for disappeared persons, guaranteeing that data contained therein are stored in a secure manner and used for solely humanitarian purposes. In particular, initiatives directed at enhancing biometric and genetic inter-force identification and exchange, especially at borders, should be guided by the fact that alleged security considerations cannot prevail over the guarantee of fundamental human rights, including the right to know the truth in connection with possible enforced disappearances;**

(s) **Adopt all necessary measures, including through technologies, to preserve and facilitate access to archives that may contain relevant information on enforced disappearance;**

(t) **Provide adequate and regular training to domestic investigative and judicial authorities on the collection, storage, validation and assessment of evidence obtained through new technologies, securing the necessary resources and developing or strengthening the corresponding infrastructure.**

66. **The Working Group recommends that technology and software corporations:**

(a) **Conduct their activities, especially with regard to the development, sale, transfer and use of new technologies, abiding by the United Nations Guiding Principles on Business and Human Rights;**

(b) **Take all measures to prevent Internet disruptions and shutdowns that they have been requested by State to implement and undertake due diligence to assess and act upon the human rights risks, mitigate possible adverse effects and guarantee access to a remedy;**

(c) **Take all measures to prevent cyberattacks, smearing and disinformation campaigns against human rights defenders, including relatives of disappeared persons,**

conducted through phishing, malware, ransomware, espionage, tainted leaks, troll farms and doxxing;

(d) **Internet service providers, social media and related platforms should alert their users to Government hacking attempts and develop a guide for users of digital platforms, informing them on the risks of cyberattacks and theft and use of their data and metadata, sharing good practices to prevent such instances; they should also put in place robust guarantees to protect users' metadata from malicious exploitation;**

(e) **Surveillance corporations should take all necessary measures to abide by their international human rights obligations; in particular, they should exercise due diligence and carry out a thorough human rights impact assessment prior to any potential sale or transfer involving targeted and mass surveillance technologies, including facial-recognition, spyware and similar programmes; they should include contractual clauses that prohibit the use of surveillance technologies in violation of international human rights law and, upon detecting misuse, promptly report them to the relevant domestic, regional or international oversight bodies; and they should put in place remedial mechanisms that enable victims of abuses to submit complaints and seek redress;**

(f) **Contribute to the development of more secure means to collect, store and analyse data – especially sensitive information concerning disappeared persons and their relatives, ensuring its exclusively humanitarian use; and also develop open source and easily accessible tools to perform forensic analysis of potentially compromised electronic devices and digital spaces;**

(g) **Contribute to the development of technologies that allow to proactively search for disappeared persons alive and that focus on the early stages of an enforced disappearance;**

(h) **Consider investing in the development of technologies that, coupled with traditional human-centred approaches, are instrumental in the search for persons whose enforced disappearance commenced prior to the existence of smartphones and the corresponding criminal investigations;**

(i) **Promote the development of technologies, including forensic tools that allow to ensure validation, identification, analysis, interpretation, documentation and presentation of digital information derived from digital sources and to cross-check multiple archives.**

67. **The Working Group recommends that civil society organizations, national human rights institutions and academic institutions:**

(a) **Continue their efforts to document and advocate against instances of Internet shutdowns and targeted disruptions, as well as cyberattacks, smearing and disinformation campaigns against human rights defenders, including relatives of disappeared persons;**

(b) **Make every effort to increase awareness of existing risks related to the use of new technologies, and, in particular, data sensitivity and harm, with a view at building core competences on digital literacy and hygiene;**

(c) **Continue their efforts to develop digital tools that support relatives of disappeared persons in the management of case files, assist them in the search process and support the prevention of enforced disappearance;**

(d) **Continue their efforts to conduct open-source intelligence, applying the principles enshrined in the Berkeley Protocol;**

(e) **Conduct further research on issues relating to new technologies and enforced disappearances, especially with regard to existing good practices, thus contributing to improving their visibility and dissemination.**

68. **The Working Group recommends that development agencies and donors:**

(a) **Integrate human rights considerations into efforts to expand communications networks and close the global digital divide;**

(b) **Take all measures necessary to secure affordable Internet access for the greatest number of people to increase the use of Internet-based technologies as enablers and facilitators for the exercise of human rights, including with regard to the search for disappeared persons and the documentation of the corresponding crimes;**

(c) **Support projects aiming at documenting and advocating against the adverse effects on human rights of new technologies, in particular in cases concerning enforced disappearance;**

(d) **Support training programmes on digital literacy and hygiene, as well as on open-source intelligence, directed at civil society organizations and, in particular, at associations of relatives of disappeared persons, with a view at raising awareness on existing risks and ensuring that they build core capacities in these domains, including to diagnose, respond to and recover from adverse digital events;**

(e) **Support the development of technologies aimed at facilitating the search for disappeared persons and the corresponding investigations and guarantee access to such tools – as well as adequate training for the personnel – in least developed countries;**

(f) **Support projects to promote the use of technologies to ensure verification, analysis, interpretation and presentation of information contained in archives and digital sources;**

(g) **Support studies aimed at exploring how the use of artificial intelligence and machine-learning, through network smartphones data analysis, can contribute to establish the whereabouts of disappeared persons and the development of the corresponding technologies.**

69. **The Working Group recommends that other human rights mechanisms and international courts:**

(a) **Promote accountability for States, corporations or individuals responsible for the misuse of targeted or mass surveillance technologies, as well as in cyberattacks, and, in general, in the use of new technologies to facilitate or conceal the commission of enforced disappearance;**

(b) **Adapt the applicable evidentiary criteria so that evidence of enforced disappearance produced through open-source intelligence is duly considered in the relevant proceedings.**

70. **The Working Group recommends that the Office of the United Nations High Commissioner for Human Rights:**

(a) **Ensures that adequate means are provided to strengthen the protection of sensitive information concerning disappeared persons and their relatives by the Office of the High Commissioner, special procedures or other mechanisms, such as commissions of inquiry or fact-finding missions;**

(b) **Disseminates and promotes the application of the Berkeley Protocol.**

Annex I

Mapping of publicly available tools, contacts and free resources that may provide useful information on new/digital technologies and assist in, and facilitate, the search for disappeared persons and the corresponding criminal investigations [non-exhaustive]

Non-Profit Organisations, Collectives and Tech Companies

- Access now: dedicated to defending and extending the digital rights of people and communities at risks
- Bellingcat: independent collective for online investigations
- Border Forensics: agency using spatial and visual analysis to investigate practices of border violence
- Citizen Forensic Researchers: United Forces for Our Disappeared in Nuevo León (FUNDENL); United Forces for Our Disappeared in Coahuila (FUUNDEC); United Forces for our Disappeared in Mexico (FUUNDEM) – organizations that are part of victim-led movements with unique approaches to utilizing technology to search for their loved ones
- CyberPeace Institute: NGO that works, including by providing support to civil society organisations, to reduce the harms from cyber-attacks
- Digipower Academy: supports people and NGOs in learning about data and data flows
- Digital Preservation Coalition: organisation that supports delivering long-term access to digital content and services
- Electronic Frontier Foundation: NGO defending civil liberties in the digital space
- Equipo Argentino de Antropología Forense (EAAF): NGO since 1986 engaged in developing forensic anthropology techniques to help locate and identify victims of enforced disappearances
- Frontline Defenders: NGO that provides support to human rights defenders at risk, including due to the (ab)use of new technologies
- Human Rights Data Analysis Group: offering statistical analysis of data referring to gross human rights violations
- HURIDOCS: NGO that helps human rights groups gather, organise and use information
- ICT4peace: foundation promoting the use of ICT for peacebuilding
- Locate International: UK-registered charity that, in partnership with universities, law enforcement agencies, police and the families of missing persons, helps the latter in finding their loved ones
- Meedan: technology non-profit that builds software and initiatives to strengthen global journalism, digital literacy and accessibility of information
- MNEMONIC: company that help business and organisations manage security risks, protect their data and defend against cyber threats
- Mnemonic.org: NGO that supports human rights defenders effectively use digital documentation of human rights violations and international crimes
- Personaldata.io: NGO working on issues related to data protection
- R3D: Mexican NGO working on the promotion and protection of human rights in the digital sphere

- SITU: interdisciplinary applied-research division, investigating and addressing human rights issues through architectural lenses (including fact-finding and spatial analysis)

- Storyful: a news and intelligence agency

- Tactical Tech: NGO that engages with citizens and civil society organisations to explore and mitigate the impacts of technology on society

- The Whistle: academic start-up, based at the university of Cambridge, developing tools to connect witnesses of human rights abuses to local organisations through a secure platform

- TraceLabs: non-profit organisation whose mission is to accelerate the family reunification of missing persons

- Videre est credere: NGO working with local activists to train them and provide them with technology to capture visual evidence of human rights abuses

- WITNESS: non-profit organisation that helps people using video and technology to protect and defend human rights

Tools

- Adarga.ai: artificial intelligence platform that uses analytics technology processes to extract information at speed from unstructured data and present it in a comprehensible format

- ADS-B Exchange: source of flight data

- Archives.is: tool to take snapshots of webpages

- ARcGIS: geo-database (proprietary)

- AToM: open source application for standards-based archival description and access in a multilingual, multi-repository environment

- Blender: open source application for 3D modelling, best suited for digital spatial event reconstruction including geolocation, chrono-location, and forensic reconstruction

- BUSQUEMOS [in Spanish, relevant for Mexico]: chatbot developed by the Mexican NGO Documenta, used to ensure early detection of arbitrary detentions and prevention of enforced disappearances

- Compass in the sky: a tool to strengthen chrono-location skills

- Deepaware: tool to scan video and images and detect whether they have been manipulated

- Descartes Labs: platform that offers geo-processing tools

- DFace: application that detects and blurs faces in online imagery

- DevelopmentSeed Skynet: open source machine-learning on satellite imagery

- DigitalGlobe: (proprietary) tool to have access to satellite and aerial imagery

- Enigio Trace: (proprietary) tool to create and manage original online documents

- Exfitool: open source tool for reading, writing and editing meta-data

- Eyewitness to atrocities: mobile camera app that allows to record photos and videos that are embedded with the metadata needed to demonstrate their authenticity to a court

- Google Earth: tool that provides access to satellite imagery

- Hunch.ly: web capture tool designed for online investigations

- I-Familia: INTERPOL global database for identifying missing persons based on international DNA kinship matching

- Investigative dashboard: platform offering various tools to trace people, companies and assets across the globe

- InVid: platform offering various tools for verification

- KoboToolbox: survey tool for mobile phones that allows for taking testimonies, georeferencing information, and upload of information to secure servers
- Lookup-ID: tool to find Facebook IDs
- Maltego: Graphing tool for discovering and mapping relationships between entities of interest – people, online accounts and organizations
- Mapillary: app that allows to access street-level imagery and map data from all over the world
- MARTUS: free, open source, secure information collection and management tool
- MAXAR: tool that provides satellite imagery (proprietary)
- MediaConch: open source policy checker
- Mobile Justice: free app to record meetings and report abuses
- Mygeoposition.com: tool to find latitude and longitude
- Neo4J: a graph database management system, useful for discovering patterns and insights across complex datasets.
- Nosomosexpedientes.mx [in Spanish, for Mexico]: digital tool that supports families in their search efforts and in the management of their case files before domestic authorities
- Orbital Insights: a tool to use location data
- PeakVisor: 3D tool that allows to identify mountains and peaks, helpful in geo-location
- Planet: tool that provides access to satellite imagery
- PhotoDNA: technology developed to detect and remove images of child exploitation
- QGIS: open-source geo-spatial database
- SCION: clean-slate Internet architecture designed to provide route control, failure isolation, and explicit trust information for end-to-end communication
- Security in a Box: digital security tools and tactics
- Siegfried: signature-based file format identification tool
- Skynet: remote sensing platform (proprietary)
- SUNCALC: application that may allow to determine the date and time of the last appearance of a disappeared person by the position of the sun and the shadows of the day
- TC Slim app: application that allows users to study the widespread hidden data collection in mobile application
- TerraServer: tool that provides access to satellite imagery
- Timemap: open source software to visualise geospatial events in an interactive platform
- TinEye: reverse image search tool
- Toddington international: free open source investigation resources
- Truecaller: tool to trace phone numbers
- TweetBeaver: offers several tools, including to download and search within a user's timeline or to download a user's favorites, friends or followers list
- TwitterId: tool to find Twitter IDs
- Uwazi: content management system that allows a public or private website to be built to store data for different uses including criminal investigations, public advocacy, and generating statistical information for research
- vframe.io: tool that offers state-of-the-art computer vision technologies to human rights research and conflict zone monitoring
- Wayback machine: tool to capture, manage and search collections of digital contents

- Webstagram: tool to analyse and track Instagram accounts
- Wigle: tool for wireless network mapping
- Wikimapia: tool that consolidates multiple services of satellite imagery
- Wolfram Alpha: tool that allows access and comparison of information on the weather and others
- Yandex Panoramas: tool to access street-level imagery
- Youtube-dl: programme to download videos from YouTube and other video sites and platforms
- Freedomlab is a virtual gathering place for human rights defenders, containing a repository of training materials, tutorials and digital tools can be found at.
- A comprehensive list of tools for online investigation can be found in the Bellingcat's Online Investigation Toolkit.
- BBC Africa Eye / Forensics Dashboard also offers a comprehensive list of tools, datasets and other resources.
- There is a growing number of tools that allow to access satellite imagery and remote sensing, including Google Earth Pro (particularly useful the 'historical imagery' tool); Bird.i; Sentinel Hub Playground; QGIS; Digital Globe; Imagehunter.

Academic Institutions/Programmes

- Center for Human Rights Science, Carnegie Mellon University
- Forensic Architecture, research agency based at Goldsmiths, University of London
- Humanitarian Research Lab, Yale University
- Human Rights and Technology programme of the Human Rights Center of the University of Berkeley
- Human Rights, Big Data and Technology project of the University of Essex
- The Citizen Lab, interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto

Resources

- Amnesty International created the digital verification corps, i.e. a network of volunteers, trained to verify data and information retrieved through open source investigation and it published a Guide to conduct effective online inquiries (part I, II and III).
- Bellingcat elaborated several publicly available "Guides", including *First steps to getting started in open source research*; *A beginner's guide to Social Media verification*; *Unsure when a video or photo was taken? How to tell by measuring the length of shadows*; *Using the sun and the shadows for geolocation*; *Investigate TikTok like a pro!*; *Guide to using reverse image search for investigations*; *A beginner's guide to flight tracking*; *Using phone contact book apps for digital research*, etc.
- Berkeley Protocol on Digital Open Source Investigations, 2020: a practical guide on the effective use of digital open source information in investigating violations of international criminal, human rights and humanitarian law.
- How to interpret satellite image: five tips and strategies, by National Areonautics and Space Administration.
- Introductory Guide to Open Source Intelligence and Digital Verification by the University of Essex Human Rights Centre Clinic.

- OSR4Rights offers a guide for open source research for human rights and tutorials and technical tools (e.g. FaceSearch, Knowledge Hub Framework, Hate Speech Detection, and using natural language processing to identify the most relevant evidence).

- Reference Model for an Open Archival Information System contains recommended practices to provide long-term preservation of digital information

- Surveillance Self-Defence Guide by the Electronic Frontier Foundation.

- Verification Handbook: guide to verifying digital contents.

- Video as Evidence Field Guide by Witness to help users film videos to document human rights abuses and bring about justice.

- See also the non-exhaustive list of reports issued by UN Special Procedures relevant to new technologies.

Annex II

Glossary

Bot-net: network of private computers infected with malicious software and controlled as a group without the owners' knowledge, e.g. to send spam.

Cartographic regression: process of overlaying historic maps and aerial photographs on contemporary images to track changes in the territory

Chrono-location: act of determining or estimating a time or time frame of an event or situation that was captured by visual media.

Data-mining: the process of sorting through large data sets to identify patterns and relationships that can help solve problems or questions through data analysis and generate new information.

Doxxing: searching for and publishing private or identifying information about (a particular individual) on the internet, typically with malicious intent.

Facial recognition programme: technology based on artificial intelligence used for identification, verification, or categorization of biometric data.

Gait recognition programme: a programme based on a system that uses the shape of the human body and the way it moves in order to identify a person.

Ground-penetrating radar: a geophysical method that uses radar pulses to image the subsurface.

Malware: software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Photogrammetry: process by which several still photographs of an environment are combined to create, through triangulation, a 3D model.

Ransomware: a malicious software designed to block access to a computer system until a sum of money is paid.

Remote-sensing: scanning of the Earth by satellite or aircraft in order to obtain information about it.

Spyware: also referred to as “intrusion software”, is a malware that allows an operator to gain access to a targeted device and extract, modify or share its contents.

Troll-farm: organization employing people to make deliberately offensive, provocative or online posts, often containing false information in order to cause conflict or manipulate public opinion.