Conseil des droits de l'homme
Cinquante-quatrième session
11 septembre-6 octobre 2023
Point 3 de l'ordre du jour
Promotion et protection de tous les droits de l'homme, civils, politiques, économiques, sociaux et culturels, y compris le droit au développement

Nouvelles technologies et disparitions forcées

Rapport du Groupe de travail sur les disparitions forcées ou involontaires*

Résumé

Dans le présent rapport, le Groupe de travail sur les disparitions forcées ou involontaires examine comment les nouvelles technologies sont utilisées contre les proches des personnes disparues, leurs représentants et les défenseurs des droits de l'homme; comment elles peuvent être appliquées efficacement pour faciliter la recherche des personnes disparues; et comment elles peuvent être utilisées pour obtenir et sécuriser les preuves de la commission d'une disparition forcée.

Le Groupe de travail formule plusieurs recommandations à l'intention des États, des entreprises, des organisations de la société civile, des institutions nationales de défense des droits humains, des établissements universitaires, des donateurs, des tribunaux internationaux et autres mécanismes de défense des droits humains, ainsi que du Haut-Commissariat des Nations unies aux droits de l'homme.

TRADUCTION NON OFFICIELLE

* Ce document est une traduction non officielle de la version anglaise et n'a pas été édité officiellement

I. Introduction

1. Lors de sa 25e session, le Groupe de travail sur les disparitions forcées ou involontaires a annoncé son intention de mener une étude thématique sur les nouvelles technologies et les disparitions forcées.

2. Afin de recueillir des informations pertinentes, des réunions d'experts ont été organisées les 9 février et 11 mai 2022, lors des 26e et 27e sessions du Groupe de travail, respectivement. Le 17 octobre 2022, le Groupe de travail a diffusé un appel à contributions.[1] Au 2 août 2023, 29 communications écrites avaient été reçues par des États (5); d'institutions nationales des droits humains (1); d'organisations de la société civile, y compris d'associations de proches de personnes disparues (16); et d'experts ou d'universitaires (7).

3. Aux fins de l'étude, l'expression « nouvelles technologies » est utilisée au sens large, pour désigner les innovations technologiques survenues principalement au cours des 20 dernières années, y compris les technologies de l'information et de la communication matérielles et logicielles, qui englobent l'imagerie satellitaire, la science de l'information géographique et la télédétection, les réseaux sociaux numériques et les ensembles de données en ligne, l'utilisation de l'intelligence artificielle et le développement de l'apprentissage automatique, ainsi que les sciences médico-légaux numériques et les données biométriques.

4. Les nouvelles technologies qui sont aujourd'hui, pour la plupart, facilement accessibles au grand public et rentables, ont une relation ambivalente avec les questions liées aux droits humains. D'une part, les gouvernements répressifs, ainsi que d'autres acteurs tels que les réseaux criminels et les groupes armés, peuvent utiliser les nouvelles technologies contre, entre autres, les défenseurs des droits humains et les proches de personnes disparues pour restreindre leurs droits fondamentaux, notamment par la surveillance, le contrôle, l'intrusion, les campagnes de désinformation, le harcèlement en ligne et les cyber-attaques. D'autres acteurs, telles que les entreprises technologiques, peuvent également jouer un rôle crucial en développant du matériel et des logiciels utilisés pour entraver l'activité des défenseurs des droits humains et des proches des personnes disparues. D'autre part, les nouvelles technologies sont indispensables pour documenter et enquêter sur les violations des droits humains, obtenir et conserver des preuves et promouvoir l'obligation de rendre des comptes, y compris dans les cas de disparitions forcées.

5. Cette étude analyse comment les nouvelles technologies sont utilisées contre les proches des personnes disparues, leurs représentants, les défenseurs des droits humains et les organisations de la société civile et quelles stratégies de protection sont – ou peuvent être – mises en place; comment elles peuvent être appliquées efficacement pour faciliter la recherche des personnes disparues, en veillant à ce que leur sort et le lieu où elles se trouvent soient établis rapidement, de manière fiable et sûre; comment elles peuvent être utilisées pour obtenir des preuves de la commission de disparitions forcées, en gardant à l'esprit que ce crime international est par nature entouré de secret et, en tant que tel, pose de formidables obstacles en matière de preuves pour identifier et traduire en justice les auteurs de ces crimes.

6. L'étude est complétée par des annexes contenant un glossaire, une cartographie non exhaustive des outils, contacts et ressources accessibles au public qui peuvent aider à mettre en place des stratégies de protection contre les menaces en ligne, faciliter la recherche des personnes disparues et les enquêtes criminelles correspondantes. Le Groupe de travail vise également à développer dans un avenir proche la présentation d'une étude de cas hypothétique illustrant le processus étape par étape pour enquêter sur un cas de disparition forcée grâce à l'utilisation des nouvelles technologies, avec l'objectif de montrer les implications, à la fois en termes d'avantages et d'obstacles existants.

[1] L'appel à contributions et les contributions reçues (à l'exception de celles pour lesquelles la confidentialité a été demandée) sont disponibles à l'adresse suivante: www.ohchr.org/en/calls-for-input/2023/call-inputs-thematic-study-working-group-enforced-or-involuntary.

TRADUCTION NON OFFICIELLE

7. En particulier en ce qui concerne la recherche des personnes disparues, la documentation du crime et la promotion de la responsabilité, les nouvelles technologies offrent des solutions rentables qui sont susceptibles d'avoir un impact significatif. Cependant, seules, elles sont incapables de résoudre tous les problèmes existants. Par conséquent, les approches et les techniques traditionnelles de documentation, de suivi et de compte rendu ne doivent pas être abandonnées et ne peuvent pas être entièrement remplacées par le matériel numérique et les nouvelles technologies. Au contraire, la complémentarité entre les deux stratégies doit être recherchée et encouragée.

II. Utilisation des nouvelles technologies pour faciliter ou dissimuler la commission de disparitions forcées, ou comme moyen de représailles ou d'intimidation

8. L'expérience du Groupe de travail et les communications reçues montrent que les nouvelles technologies, et en particulier les TIC, sont fréquemment utilisées pour faciliter ou dissimuler la commission de disparitions forcées, pour entraver le travail des défenseurs des droits humains et des proches de personnes disparues, et pour les intimider ou les harceler. Parfois, la législation relative à la technologie (en particulier à l'utilisation des réseaux sociaux et à la cybercriminalité) est utilisée de manière spécieuse aux mêmes fins et pour poursuivre les défenseurs des droits humains et les proches des personnes disparues qui utilisent ces moyens pour dénoncer des disparitions forcées ou des abus.

9. Le Groupe de travail a reçu des informations sur des disparitions forcées perpétrées lorsque l'État avait perturbé l'accès à l'Internet et aux données mobiles, soit par des interventions générales, soit par des approches plus ciblées, notamment en restreignant la bande passante et en bloquant des plateformes médiatiques spécifiques.[2] Bien qu'il n'existe pas d'étude complète analysant la concomitance des fermetures ou des restrictions à l'Internet et des perturbations de l'accès aux données mobiles avec l'augmentation du nombre de disparitions forcées, les rapports reçus par le Groupe de travail semblent indiquer que la limitation de l'accès à Internet – ou sa fermeture complète – ont contribué à dissimuler des violations flagrantes des droits humains, y compris des disparitions forcées.

10. Les restrictions d'accès à l'Internet ont un impact sur l'exercice de divers droits humains et ne sont admissibles que dans des circonstances spécifiques et avec des garanties appropriées.[3] Souvent, après le rétablissement de la connexion à l'Internet, y compris l'utilisation des plateformes médiatiques, le Groupe de travail reçoit des rapports de disparition forcée ou de harcèlement contre les défenseurs des droits humains et les proches des personnes disparues perpétrés pendant la fermeture de l'accès à l'Internet. Dans ces cas, les fermetures ou les perturbations similaires empêchent concrètement le contrôle du respect des droits humains, ainsi que la documentation et le signalement rapide des crimes en question et entravent les enquêtes et les activités de recherche, ce qui compromet en fin de compte le droit de connaître la vérité et favorise l'impunité.

11. Le Groupe de travail a reçu un nombre croissant de communications faisant état de disparitions forcées qui auraient été perpétrées pour « réduire au silence » une personne active sur les médias sociaux, par exemple des personnes qui ont dénoncé des abus perpétrés par l'État, qui ont commémoré des événements, ou qui appartiennent à des minorités. Les personnes soumises à une disparition forcée dans ces circonstances sont notamment des défenseurs des droits humains, des journalistes, des blogueurs, des Youtubers, des activistes, des opposants politiques et des chefs religieux.[4]

[2] EGY 4/2011 ; IRN 37/2021 ; KAZ 1/2022.
[3] A/HRC/50/55. Voir également A/HRC/RES/44/20 ; A/HRC/RES/38/7 ; A/71/373 ; A/HRC/32/38 ; et A/HRC/47/24/Add.2.
[4] IRN 27/2012 ; ARE 1/2017 ; VNM 4/2020.

TRADUCTION NON OFFICIELLE

12. Une pratique détectée par le Groupe de travail et qui semble s'apparenter à un modus operandi commun aux forces de sécurité du monde entier consiste à confisquer tous les appareils électroniques des personnes soumises ultérieurement à une disparition forcée et, souvent, des proches ou de toute autre personne présente au moment de la privation de liberté. Les cas où les appareils électroniques de spectateurs ou de témoins potentiels d'une disparition forcée ont été détruits par les forces de sécurité, prétendument pour effacer toutes les preuves du crime, sont également récurrents.

13. En relation avec les circonstances décrites dans les paragraphes ci-dessus, le Groupe de travail a enregistré un nombre croissant de cas où des défenseurs des droits humains, y compris des proches de personnes disparues, ont été inculpés et poursuivis en vertu de la législation nationale sur la cybersécurité. Il s'agit notamment de cas où les personnes concernées ont publié des informations sur des disparitions forcées sur leurs comptes et dans les réseaux sociaux ou ont critiqué le gouvernement pour son implication présumée ou pour l'impunité dans les cas de disparitions forcées.[5] Dans d'autres cas, de faux comptes ont été utilisés pour accuser ensuite la personne concernée de diffuser des informations haineuses ou fausses, ou de compromettre la sécurité nationale.[6]

14. En outre, les mécanismes internationaux de défense des droits de l'homme ont été saisis de cas où l'utilisation – ou même le simple téléchargement – d'une application spécifique (comme, par exemple, l'application de messagerie ByLock) a été considérée par les autorités nationales comme la seule preuve décisive justifiant des arrestations massives de défenseurs des droits de l'homme et d'opposants politiques, conduisant dans certains cas à leur disparition forcée ou à leur mort en détention.[7] Ces affaires sont particulièrement préoccupantes, notamment en raison du manque de clarté des motifs juridiques invoqués. Un autre sujet de préoccupation concerne les technologies et les techniques utilisées par les autorités nationales pour accéder aux serveurs, obtenir les adresses IP et le contenu des échanges des utilisateurs, ce qui peut aller jusqu'au piratage, à l'infiltration et au vol de données sur les serveurs. Par exemple, dans le cas de ByLock, le serveur était situé dans un État différent de celui où les arrestations et les poursuites ont eu lieu.[8]

15. Selon les informations reçues par le Groupe de travail, les réseaux sociaux ont également été utilisés pour mener des campagnes de diffamation et menacer les défenseurs des droits humains, y compris les proches de personnes disparues. Les attaques signalées sur les médias sociaux contre des proches de personnes disparues ont souvent été caractérisées par des stéréotypes et une discrimination fondés sur le sexe[9] et des outils numériques (notamment des « fermes à trolls », des botnets et de faux comptes) ont été utilisés pour mener des campagnes ciblées de diffamation ou de désinformation, pour stigmatiser les personnes disparues ou leurs proches et pour permettre le harcèlement en ligne, y compris le harcèlement sexuel, et l'incitation à la haine.

16. Les cyberattaques menées contre les défenseurs des droits humains, y compris les proches de personnes disparues, comprennent le sabotage par *phishing*, *malwares* et les *ransomwares*, l'espionnage et la diffusion de désinformation, ainsi que les fuites d'information « contaminée » (*tainted leaks*) et le *doxxing*. Souvent, les personnes visées sont malicieusement dépeintes ou qualifiées d'espions, d'agents étrangers, de terroristes ou de contrebandiers, ce qui expose leurs comptes à une surveillance spéciale, à une suspension ou à des campagnes de haine, dans un scénario qui se caractérise par une sous-dénonciation des cas, des lacunes politiques et juridiques et des difficultés à juger les responsables, notamment en raison de l'implication de différentes juridictions.[10] Le Groupe de travail a pris connaissance avec inquiétude d'un cas où une défenseuse

[5] EGY 7/2018 ; NIC 3/2020 ; NIC 6/2022 ; ZMB 1/2021.
[6] BGD 1/2022.
[7] Cour européenne des droits de l'homme (CEDH), affaire Akgün c. Türkiye, arrêt du 20 juillet 2021 ; et Comité des droits de l'homme, affaire Açikkollu c. Türkiye, communication n° 3730/2020, avis du 25 octobre 2022.
[8] Groupe de travail sur la détention arbitraire, Avis n° 42/2018 du 21 août 2018, par. 33.
[9] A/HRC/50/25 et A/HRC/38/47.
[10] Le Conseil de l'Europe a tenté de surmonter certains des obstacles mentionnés en adoptant la Convention sur la cybercriminalité de 2001 et le deuxième protocole additionnel à la Convention sur la cybercriminalité relatif au renforcement de la coopération et à la divulgation des preuves électroniques (qui n'est pas encore entré en vigueur) de 2022.

TRADUCTION NON OFFICIELLE

des droits humains enquêtant sur une disparition forcée a été contactée par le biais de ses réseaux sociaux par une personne utilisant une fausse identité, qui a profité de ces échanges pour lui envoyer des liens vers des fichiers contenant un *malware*, compromettant ainsi la sécurité et la confidentialité de ses données.[11]

17. En outre, le Groupe de travail a été informé que des sites Web, créés par des proches de personnes disparues ou leurs associations, soit pour honorer et préserver la mémoire de leurs proches, soit sur la question des disparitions forcées en général, ont fait l'objet de cyberattaques, qui constituent des ingérences graves et injustifiées, une forme de revictimisation et des atteintes à la dignité et à la réputation des personnes disparues et de leurs proches. A la connaissance du Groupe de travail, ces attaques et entraves – qui peuvent être le fait d'acteurs privés engagés par l'État et d'acteurs non étatiques[12] – font rarement l'objet d'enquêtes approfondies et efficaces et restent impunies, ce qui favorise la répétition d'infractions similaires.

18. Le Groupe de travail a reçu des informations sur des cas tout aussi récurrents où des technologies, en particulier des TIC, ont été utilisées pour espionner des proches de personnes disparues, leurs représentants ou associations et des défenseurs des droits humains. L'utilisation nationale ou transnationale de logiciels espions, tels que Candiru, Pegasus ou Predator, pour surveiller malicieusement les activités des défenseurs des droits humains, des journalistes, des militants et des avocats, notamment en déterminant leur localisation, en accédant à leurs listes de contacts pour démasquer d'autres personnes, en déposant des preuves à charge et en faisant chanter les personnes concernées, constituent une évolution particulièrement inquiétante.[13] Les logiciels espions ont été utilisés pour surveiller des proches de personnes disparues, notamment l'épouse et la fiancée de Jamal Khashoggi,[14] la fille de M. Paul Rusesabagina,[15] des défenseurs des droits humains qui soutiennent les proches de personnes disparues,[16] ou les membres d'une commission indépendante chargée d'enquêter sur la disparition forcée de 43 étudiants à Ayotzinapa, Mexique.[17] L'omniprésence des logiciels espions à un effet dissuasif sur les organisations de la société civile et les défenseurs des droits humains, y compris les proches de personnes disparues.[18]

19. Les proches des personnes disparues vivent souvent dans la crainte de représailles, ce qui les empêche fréquemment de signaler les abus, y compris par le biais de la procédure humanitaire du Groupe de travail. Les logiciels espions amplifient le risque en permettant un accès illimité à leurs appareils et à leurs données. Les informations recueillies par les logiciels espions peuvent être utilisées pour commettre d'autres abus à l'encontre des proches des personnes disparues, les faire chanter pour qu'ils gardent le silence ou leur causer d'autres préjudices. Les données obtenues grâce aux logiciels espions peuvent également aider à localiser des personnes pour les faire disparaître de force.

20. Les logiciels espions peuvent être acquis par les gouvernements, le plus souvent dans un contexte qui, en général, manque de contrôle indépendant et de réglementation suffisante, notamment en ce qui concerne l'importation, l'exportation et l'utilisation d'une telle technologie. Le Groupe de travail a pris connaissance avec intérêt de la législation applicable dans certains

TRADUCTION NON OFFICIELLE

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

12 Sur l'implication potentielle de mercenaires (comprenant des entités commerciales, des groupes de menaces persistantes avancées, des cyber-milices, des individus et des cyber-criminels) dans des cyber-attaques, voir A/76/151.

13 Haut-Commissaire des Nations unies aux droits de l'homme, Déclaration sur l'utilisation de logiciels espions pour surveiller les journalistes et les défenseurs des droits de l'homme, 19 juillet 2021; et www.oas.org/en/iachr/jsForm/?File=/en/iachr/media_center/preleases/2022/022.asp. Sur la surveillance numérique des journalistes, voir A/HRC/50/29. Voir également A/HRC/52/39, §§ 44-50.

14 A/HRC/4/CRP.1, §§ 68-71.

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

16 Voir 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 et A/HRC/41/35.

États et des réglementations régionales et accords internationaux existants[19] qui visent à soumettre la vente et le transfert de technologies à un contrôle plus strict. Bien qu'il s'agisse de bonnes pratiques, le cadre juridique applicable reste faible et fragmenté et un examen approfondi et indépendant de l'impact de ces technologies sur les droits humains devrait devenir la règle avant leur vente, leur transfert et leur utilisation.[20]

21. Les cas où les personnes – qu'il s'agisse d'États, d'entreprises ou d'individus – responsables de l'utilisation abusive des technologies de surveillance ou d'abus dans leur vente et leur transfert ont été jugées et sanctionnes sont extrêmement rares.[21] Jusqu'à ce que les lacunes réglementaires soient comblées de manière exhaustive et que les entreprises respectent pleinement leurs obligations en vertu du droit international, telles qu'elles sont énoncées dans les Principes directeurs relatifs aux entreprises et aux droits de l'homme, un moratoire sur la vente, le transfert et l'utilisation de logiciels espions devrait être appliqué.[22]

22. Le Groupe de travail a également observé avec inquiétude la prolifération incontrôlée de la surveillance de masse, de la reconnaissance faciale et de programmes similaires.[23] Par leur nature même, ces systèmes soumettent un nombre important d'individus à une surveillance indiscriminée, interférant systématiquement avec leurs droits humains. Le traitement des données biométriques, des images et des informations recueillies par ces moyens par des caméras vidéo dans les espaces publics a été utilisé pour identifier certaines personnes, y compris dans le contexte de manifestations sociales,[24] qui ont ensuite été arrêtées et, dans certains cas, ont été soumis à disparition forcée. Des systèmes de données centralisés fonctionnant par le biais d'applications mobiles utilisées par des fonctionnaires gouvernementaux auraient été utilisés pour effectuer des opérations similaires de surveillance de masse, conduisant au ciblage de certaines personnes considérées comme « suspectes » (y compris des défenseurs des droits humains et des personnes appartenant à des minorités ethniques ou religieuses) et à leur disparition forcée par la suite.

23. Selon les informations reçues par le Groupe de travail, les technologies de surveillance susmentionnées, ainsi que les solutions d'intelligence artificielle, les drones, les capteurs thermiques, les lunettes de vision nocturne, les systèmes d'identification biométrique, les tours de surveillance aérienne et les capteurs spécialisés dans la détection des émissions de téléphones portables et des dispositifs de localisation, sont de plus en plus utilisés aux frontières par les États et les agences régionales pour automatiser les processus d'identification et de suivi des mouvements des migrants, des réfugiés et des demandeurs d'asile, y compris dans les opérations

[19] Voir l'Arrangement de Wassenaar de 1995 sur le contrôle des exportations d'armes conventionnelles et de biens et technologies à double usage, tel qu'amendé en 2013 ; et le Règlement (UE) n° 2021/821 du 20 mai 2021 instituant un régime de contrôle des exportations, du courtage, de l'assistance technique, du transit et du transfert de biens à double usage. Voir également la loi japonaise sur le change et le commerce extérieur n° 228 de 1949, telle qu'amendée en 2005; et le projet d'orientation du gouvernement américain pour l'exportation de technologies de surveillance, Bureau de la démocratie, des droits de l'homme et du travail, Département d'État des États-Unis, 4 septembre 2019. Pour un projet d'engagement des États sur le commerce international des logiciels espions, voir A/HRC/52/39, annexe.

[20] Une initiative dans ce sens, appelée « Export Controls and Human Rights Initiative » (Initiative pour le contrôle des exportations et les droits de l'homme), a été lancée le 10 Décembre 2021 par l'Australie, le Danemark, la Norvège et les États-Unis d'Amérique.

[21] Les exceptions notables sont les suivantes : la décision de la Cour d'appel de Paris qui, en novembre 2022, a confirmé la mise en examen d'une société de surveillance et de ses dirigeants, en raison, entre autres, de la disparition de dissidents consécutive à la vente de logiciels de surveillance à des régimes autoritaires ; la décision rendue le 9 janvier 2023 par la Cour Suprême des États-Unis qui a autorisé la poursuite de la procédure engagée contre le groupe NSO sur la base d'une action en justice intentée par WhatsApp. Voir https://www.fidh.org/en/impacts/Surveillance-torture-Libya-Paris-Court-Appeal-indictment-AMESYS; et https://dockets.justia.com/docket/california/candce/3:2019cv07123/350613.

[22] Scandale des logiciels espions : Les experts de l'ONU demandent un moratoire sur la vente de technologies de surveillance qui mettent la vie en danger, 2021.

[23] Sur les défis uniques concernant l'utilisation des données personnelles et non personnelles dans le contexte de l'intelligence artificielle, voir A/HRC/46/37; et sur l'analyse des big data et les techniques de calcul basées sur l'intelligence artificielle, voir A/73/438. Voir également A/HRC/37/62 sur la surveillance et le droit à la vie privée; A/HRC/41/43 sur l'impact disproportionné de l'intelligence artificielle et de l'automatisation sur les femmes ; A/HRC/41/35 sur les technologies de surveillance privée et les droits de l'homme; A/74/159 sur les enquêtes sur les technologies numériques utilisées pour la surveillance; et A/HRC/34/60 sur les activités de surveillance gouvernementales.

[24] A/HRC/44/24.

TRADUCTION NON OFFICIELLE

de refoulement, ce qui conduit – ou dans certains cas équivaut– à des disparitions forcées.[25] Le Groupe de travail a également appris que les données recueillies grâce à ces technologies n'étaient pas utilisées par les équipes de recherche et de sauvetage et les autorités, ce qui n'a pas permis d'éviter que des migrants en détresse ne disparaissent ou ne meurent. Le Groupe de travail exprime sa profonde inquiétude face à une utilisation aussi vicieuse des nouvelles technologies et note que le cadre juridique international applicable – en particulier en ce qui concerne l'utilisation de l'intelligence artificielle – présente des lacunes et devrait être renforcé de toute urgence.[26]

24. Des cyberattaques sur des bases de données contenant des informations sensibles sur les personnes disparues et leurs proches ont également eu lieu. Par exemple, le 18 janvier 2022, des données personnelles et d'autres informations confidentielles concernant plus de 515000 personnes dans le monde, stockées dans les systèmes de l'Agence centrale de recherches du Comité international de la Croix-Rouge, ont été l'objet d'accès non autorisés.[27] Entre autres, plusieurs plateformes contenant des données sur des personnes disparues, ainsi que sur leurs proches (notamment l'application et le site web « Family Links Answers » et la plateforme « Trace the Face ») ont été compromises. L'enquête sur cette attaque a montré qu'il s'agissait d'une attaque très sophistiquée, menée dans le but d'extraire des données.

25. Des cas comme celui décrit ici confirment le besoin urgent de développer des moyens plus sûrs qui peuvent garantir l'utilisation exclusivement humanitaire des données[28] et des canaux de communication sûrs pour les défenseurs des droits de l'homme, les organisations de la société civile, les acteurs humanitaires, les organismes de défense des droits de l'homme et les proches des personnes disparues.[29] Dans l'attente, l'utilisation d'applications gratuites disponibles qui permettent la collecte, le stockage et l'analyse sécurisés des données est une première mesure d'atténuation du risque à mettre en place.[30] Le développement d'outils libres et facilement accessibles permettant d'effectuer une analyse médico-légale fiable des dispositifs susceptibles d'avoir été compromis a également été mentionné comme une action pertinente pour atténuer certains des risques décrits dans cette section.[31] En outre, de nombreuses contributions reçues par le Groupe de travail soulignent l'importance de fournir une formation adéquate aux membres des organisations de la société civile et aux proches des personnes disparues afin de les sensibiliser aux risques liés aux nouvelles technologies et de les atténuer, notamment en diffusant des informations sur l'hygiène numérique, la sensibilité des données, les préjudices et la minimisation. Ces programmes devraient permettre les organisations de la société civile à intégrer des méthodes de sécurité dans leur travail et à acquérir une capacité interne à diagnostiquer les risques existants et à se remettre des menaces ou des attaques.

III. Utilisation des nouvelles technologies pour faciliter la recherche des personnes disparues

26. Les innovations technologiques se sont révélées cruciales pour documenter les violations flagrantes des droits humains et sensibiliser l'opinion publique à ce sujet. Les données recueillies dans le cadre de la recherche des personnes disparues peuvent également être essentielles dans le contexte des enquêtes criminelles, bien que cet aspect soit examiné plus en profondeur dans la section IV. Comme l'indique le principe 13 des Principes directeurs pour la recherche des

[25] A/HRC/36/39/Add.2 et A/HRC/47/30. Comité des disparitions forcées, projet d'observation générale sur les disparitions forcées dans le contexte des migrations, mars 2023, §§ 22, 33 et 44 et note de bas de page 21.

[26] Des efforts sont en cours au niveau de l'UE pour adopter une règlementation sur l'intelligence artificielle.

[27] Voir https://www.icrc.org/en/document/sophisticated-cyber-attack-targets-red-cross-red-crescent-data-500000 personnes.

[28] Par exemple, le protocole connu sous le nom de SCION développé à l'école polytechnique de Zurich.

[29] Pour relever certains de ces défis, le CICR ouvre une délégation pour le cyberespace. L'Agence centrale de recherches s'appuie également sur un programme de numérisation, dans le cadre duquel ont été lancés un programme d'appariement numérique des données relatives aux personnes disparues et un projet intégré de recherches en ligne et d'enquêtes préalables. Plus généralement, voir le numéro de la Revue du CICR (2021) sur les technologies numériques et la guerre.

[30] Pour certaines de ces applications, voir l'annexe I.

[31] Entre autres, Amnesty International, Forensic Methodology Report, How to Catch NSO Group's Pegasus, 2021.

TRADUCTION NON OFFICIELLE

personnes disparues de 2019, la recherche des personnes disparues et l'enquête criminelle sur les responsables du crime devraient être liées et se renforcer mutuellement.[32]

27. L'une des communications reçues par le Groupe de travail souligne qu'à l'heure actuelle, la plupart des technologies utilisées dans la recherche des personnes disparues et les enquêtes correspondantes reposent sur une compréhension et une classification binaire du genre qui ignorent les expériences et les expressions non normatives. Les données recueillies et traitées de manière non réfléchie, et sans une compréhension plus large des spectres sexe-genre, ignorent des systèmes sociaux et culturels cruciaux et entravent les activités de recherche et les enquêtes. Une approche intégrée du traitement de l'information devrait intégrer la recherche exhaustive de détails sur la personne (avant/pendant/après la disparition) dans une optique sexo-spécifique et l'utilisation de ces informations tout au long du processus. Le Groupe de travail estime que cet aspect sera pris en compte lors de la conception d'outils et de technologies de collecte de données pour la recherche de personnes disparues et les enquêtes.[33]

28. Il a été porté à l'attention du Groupe de travail que certaines des technologies mentionnées dans la section précédente – logiciels espions, programmes de surveillance et de reconnaissance faciale, et technologies actuellement utilisées aux frontières pour le contrôle des migrations – qui ont été utilisées contre des défenseurs des droits humains et des proches de personnes disparues, et qui ont notamment contribué à la perpétration de disparitions forcées, pourraient à l'inverse être appliquées pour faciliter la recherche des personnes disparues et l'identification des coupables. Le Groupe de travail observe qu'il pourrait en effet être utile d'explorer cet aspect de ces technologies, en gardant à l'esprit qu'elles doivent toujours être utilisées en garantissant le respect des droits humains fondamentaux et que, dans ce domaine, les critères et les exigences imposés aux entreprises pour accorder l'accès aux données – au personnel chargé de l'application de la loi et à des tiers – pourraient être réévalués.

29. Le recours au renseignement à code source ouvert, qui s'appuie sur la technologie pour recueillir et analyser des données accessibles au public (par exemple sur les médias sociaux, imagerie satellite ou les outils de cartographie), peut jouer un rôle crucial à la fois dans la recherche des personnes disparues et dans l'identification et l'obtention de preuves permettant d'identifier les auteurs du crime. Elle sera donc mentionnée à la fois dans cette section et dans la section suivante de l'étude. Pour une analyse plus exhaustive de tous les aspects pertinents, le Protocole de Berkeley de 2020 est considéré par le Groupe de travail comme une référence essentielle quant à l'utilisation des données numériques à code source ouvert dans les enquêtes (« le Protocole de Berkeley »), qui contient un guide pratique sur l'utilisation efficace des preuves disponibles à code source ouvert dans le cadre des enquêtes sur les violations du droit international pénal, des droits de l'homme et du droit humanitaire.[34] Le Groupe de travail considère que le Protocole de Berkeley devrait être pris en compte par tous les acteurs impliqués dans la recherche des personnes disparues et dans les enquêtes sur les disparitions forcées.

30. En ce qui concerne les technologies qui sont principalement utilisées pour rechercher les personnes disparues, le Groupe de travail note que nombre d'entre elles ont été conçues et essentiellement utilisées pour rechercher des dépouilles mortelles. Bien que le Groupe de travail reconnaisse l'importance de ces techniques et analyse dans les paragraphes suivants certaines réalisations remarquables à cet égard, il convient de rappeler que les recherches doivent être menées en présumant que la personne disparue est vivante.[35] Le Groupe de travail estime que davantage d'efforts et de ressources – techniques, financières et humaines – devraient être consacrés au développement de technologies axées sur les premiers stades d'une disparition forcée et sur la recherche proactive de la personne disparue vivante, y compris par le suivi précoce des traces numériques de la personne disparue. Compte tenu de cette clarification, la manière dont les

[32] A/HRC/45/13/Add.3, § 56.
[33] Cela s'applique à l'analyse sémantique et thématique du contenu des données, aux efforts de localisation à l'aide de drones, aux technologies de reconnaissance des formes, aux technologies de reconstruction faciale et aux processus de visualisation numérique.
[34] Voir www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.
[35] Voir le principe 1 des Principes directeurs concernent la recherche des personnes disparues de 2019.

TRADUCTION NON OFFICIELLE

nouvelles technologies –- et en particulier les technologies numériques –- peuvent contribuer à la découverte et à la gestion des charniers constitue un sujet pertinent pour la recherche des personnes disparues et a déjà fait l'objet d'une analyse approfondie.[36]

31. Une technologie déjà utilisée depuis quelques années est le *Light Detection and Ranging* (LiDAR), qui est une méthode de détection à distance utilisée pour examiner la surface de la Terre. Par le passé, dans le cadre des opérations de recherche de personnes disparues, cette technologie a surtout été utilisée pour cartographier et localiser des lieux d'inhumation et des charniers[37]. L'amélioration des capacités cartographiques de la technologie LiDAR la rend également adaptée aux opérations de recherche et de sauvetage, car elle peut aider à identifier une forme humaine sur un terrain donné et à déterminer le moyen le plus efficace d'atteindre la personne concernée. Les unités de relevé LiDAR sont montées sur des drones ou de petits avions et survolent les zones à cartographier.[38]

32. Lors de sa visite en Uruguay, le Groupe de travail a appris qu'il avait fallu des mois à l'institution chargée de la recherche des personnes disparues pour mettre la main sur un appareil LiDAR, finalement emprunté à l'Argentine. Une fois l'appareil obtenu, un certain nombre d'obstacles bureaucratiques ont été rencontrés avant qu'il ne puisse être utilisé. Il s'est avéré par la suite que des unités LiDAR existaient en Uruguay et auraient pu être mises à disposition par l'armée (qui les possède) à un stade beaucoup plus précoce, ce qui aurait pu faciliter les opérations de recherche et leur efficacité.[39] Cet exemple suggère que les institutions chargées de la recherche des personnes disparues dans n'importe quel pays devraient avoir cette technologie à leur disposition et que des règles adéquates devraient être mises en place pour éviter toute entrave injustifiée à son utilisation. Des considérations similaires s'appliquent à l'utilisation des scanners sonores, de navigation et de télémétrie (connus sous le nom de SONAR), des drones et des radars à pénétration de sol.

33. Outre les images aériennes, l'imagerie satellitaire avec une résolution spatiale significative est aujourd'hui accessible également en dehors du domaine des gouvernements et peut faciliter la recherche des personnes disparues. Par exemple, elles ont été utilisées pour documenter l'existence de lieux de détention officiels ou secrets, localiser des sites de torture[40] et identifier des charniers ou des lieux d'inhumation.[41] Le temps qui passe peut constituer un obstacle à l'utilisation de cette technologie dans la recherche des personnes disparues, mais l'utilisation d'outils de recherche d'images inversées, de photogrammétrie et de régression cartographique peut atténuer certaines de ces difficultés.

34. Le Groupe de travail a pris connaissance de l'utilisation de l'analyse géospatiale, combinée aux statistiques spatiales et à la détection à distance, pour identifier les zones potentielles de recherche de charniers en Basse-Californie, au Mexique.[42] Les chercheurs ont utilisé le

[36] A/75/384.

[37] Voir www.coloniadignidad.cl/actualidad/noticias/la-tecnologia-lidar-en-la-busqueda-de-personas-detenidas-desaparecidas-en-las-ultimas-dictaduras-de-argentina-y-chile/. Voir également Corcoran A., Mundorff A.Z., White D.A. et 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] Il est utilisé, par exemple, par Frontex lors de ses opérations, voir la présentation PowerPoint (europa.eu). Voir aussi également Capacités basées sur l'intelligence artificielle pour le corps européen de garde-frontières et de garde-côtes (europa.eu) plus généralement pour les capacités d'intelligence artificielle de Frontex.

[39] A/HRC/54/22/Add.1, § 21.

[40] Amnesty International, « Cameroon's Secret Torture Chambers, 2017 ; et Humanitarian Research Lab, Extrajudicial Detentions and Enforced Disappearances in Kherson Oblast », 2022.

[41] Voir www.icrc.org/en/document/joint-statement-tripartite-commission et https://www.icrc.org/en/document/gulf-war-9-human-remains-identified-and-returned-their-families-after-30-years

[42] La technique employée reposait sur la prise en compte de la répartition spatiale des tombes cachées, de la visibilité spatiale, de l'accessibilité de zones spécifiques, et de l'accumulation d'azote identifiée par images satellite. Pour une reconstitution complète, voir Amnesty International, « Finding clandestine graves: using geospatial analysis to search for missing persons in Baja California, Mexico - Citizen Evidence Lab » ; J. Silván-Cárdenas, A. Alegre-Mondragón, J. Ruiz-Reyes, « Geospatial Analysis of Clandestine Graves in Baja California : New Approaches for the Search of Missing Persons in Mexico », *in* R. Tapia-McClung, O. Sánchez-Siordia, K. González-Zuccolotto, H. Carlos- Martínez (eds), *Advances in Geospatial Data Science*, Springer, 2022, pp. 29-40.

TRADUCTION NON OFFICIELLE

regroupement spatial et l'espace clandestin et les ont intégrés dans un modèle spatial au sein d'une application Web, dans le but de réduire les zones où la probabilité de trouver des tombes clandestines est la plus élevée, sur la base des informations initiales de 52 sites funéraires localisés par le Procureur Général. Cela a conduit à une réduction substantielle (<10%) des zones de recherche, produisant un modèle permettant de confirmer que les zones de recherche se trouvaient à distance raisonnable de zones urbaines. Cette méthodologie a donné des résultats encourageants et mériterait d'être étudiée et analysée plus en détail.

35. Les technologies sont également cruciales en termes de sciences médico-légales et se sont avérées essentielles pour déterminer le sort des personnes disparues et le lieu où elles se trouvent, notamment grâce à l'utilisation de données biométriques et à la mise en place de bases de données génétiques.[43] L'interopérabilité de ces bases de données reste un défi, tant au sein des États (en particulier les États fédéraux) qu'au niveau international. Le Groupe de travail a appris l'existence de bases de données globales[44] destinées à aider l'établissement de la filiation par correspondance ADN de et estime que ces efforts devraient être poursuivis. Selon les informations reçues, la bio-informatique médico-légale joue un rôle de plus en plus important dans la vérification des analyses d'ADN, contribuant ainsi à la réalisation du droit à connaître la vérité.

36. La question de la sécurité de la collecte et de l'échange des données – essentielle pour faciliter la recherche des personnes disparues – s'avère particulièrement difficile dans les cas impliquant des migrants. D'une part, il existe une réticence généralisée à partager des données sur les personnes disparues, par crainte que, en l'absence d'une protection adéquate, les informations collectées ne soient utilisées contre les personnes concernées ou leurs familles. D'autre part, il peut exister plusieurs bases de données, souvent situées dans différents pays, qui contiennent des informations pertinentes, mais qui n'offrent pas d'interopérabilité, notamment parce qu'elles ne suivent pas de critères harmonisés en ce qui concerne les données collectées, ce qui finit par faire échouer les tentatives de recherche. Des problèmes similaires se posent lorsque des restes humains susceptibles d'appartenir à une personne disparue se trouvent dans un État, mais que les bases de données contenant les données génétiques nécessaires à une identification fiable sont dispersées dans d'autres États.

37. Dans ce domaine, des ressources techniques, financières et humaines supplémentaires sont nécessaires, entre autres, pour développer des technologies permettant de surmonter ces obstacles en toute sécurité.[45] Les initiatives visant à améliorer l'identification biométrique et génétique entre les différentes institutions, en particulier aux frontières, devraient être guidées par cet but, en gardant à l'esprit que les prétendues considérations de sécurité ne sauraient prévaloir sur la garantie des droits humains fondamentaux, y compris le droit de connaître la vérité en ce qui concerne d'éventuelles disparitions forcées.

38. Le Groupe de travail a reçu des informations sur des cas où, grâce aux images de cameras de sécurité en circuit fermé (CCTV) sur le lieu où la personne disparue aurait été emmenée, les proches ou leurs représentants ont retrouvé la plaque d'immatriculation du véhicule utilisé ainsi que son itinéraire postérieur à sa disparition. En croisant ces informations avec les journaux d'appels et les données du téléphone portable de la personne disparue, ils ont recueilli des indications pertinentes sur l'endroit où elle pourrait se trouver. Dans certains cas, des informations similaires ont été obtenues grâce au contenu généré par les utilisateurs (par exemple, des photos ou des vidéos téléchargées sur les médias sociaux). Ces démarches ont souvent été laissées à l'initiative des proches des personnes disparues, de leurs représentants ou d'autres membres de la société civile, les exposant fréquemment à des risques, alors que les autorités ne semblent pas avoir développé une pratique systématique.

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

[44] I-Familia, géré par INTERPOL.

[45] CICR, Core Dataset for the Search for Missing Migrants, 2021; F. Laczko, A. Singleton, J. Black (ed), *Fatal Journeys, Vol. 3: Improving Data on Missing Migrants*, Organisation internationale pour les migrations, 2017.

TRADUCTION NON OFFICIELLE

39. Les proches des personnes disparues utilisent fréquemment les réseaux sociaux ou les applications de messagerie pour rechercher activement leurs proches.[46] Bien que cela puisse faciliter l'établissement du sort des personnes disparues et du lieu où elles se trouvent, on peut se demander si ces données hautement sensibles sont stockées et protégées de manière adéquate et sûre, compte tenu des cas de cyberattaques, d'atteintes à la protection des données et de piratage informatique mentionnés ci-dessus. Il a été porté à l'attention de Groupe de travail que, même lorsqu'il existe des réglementations rigoureuses en matière de protection des données, celles-ci pourraient être modifiées pour inclure des clauses traitant spécifiquement de la question des disparitions forcées, par exemple en prévoyant des procédures de « *quick freeze* » permettant la conservation des données à la demande d'une personne qui se sent en danger.

40. Certaines technologies peuvent ne pas être applicables ou pertinentes dans les cas où la personne a disparu avant l'existence des smartphones ou de l'internet. La disparition forcée est un crime permanent et une violation continue de multiples droits humains[47] et la recherche est donc une obligation permanente.[48] Il est donc essentiel d'investir davantage dans le développement de technologies qui peuvent également contribuer à élucider des cas où la disparition a commencé plusieurs décennies auparavant. Les nouvelles technologies peuvent apporter des résultats significatifs à cet égard, mais les techniques traditionnelles centrées sur l'être humain doivent également être maintenues et utilisées au même temps que les premières.

41. La recherche efficace de personnes disparues nécessite souvent la consultation et le recoupement de multiples archives qui peuvent être composées de centaines de milliers de pages et de téraoctets de fichiers. Les technologies peuvent faciliter la tâche et accroître l'efficacité de la consultation des archives.[49] Le Groupe de travail a appris de l'existence d'un programme appelé Angelus,[50] développé au Mexique par des mathématiciens en collaboration avec la Commission nationale de recherche de personnes disparues et qui repose sur l'utilisation d'un réseau d'algorithmes, de l'intelligence artificielle et de l'apprentissage automatique. Ce programme représente une bonne pratique, car il permet de traiter et de croiser une énorme quantité de données et de détecter l'existence de modèles, de contextes et de connexions qui peuvent faciliter la recherche des personnes disparues.

42. L'exploration de données (*data mining*), réalisée manuellement ou par le biais de différentes technologies basées sur des algorithmes, présente un grand potentiel en ce qui concerne la collecte d'informations qui peuvent s'avérer d'une importance cruciale à la fois pour la recherche des personnes disparues et pour la promotion de la responsabilité. Les résultats remarquables obtenus en termes d'établissement du sort et du lieu où les personnes disparues se trouvent et d'identification des auteurs de crimes, grâce aux informations extraites de l'Archive Historique de la police nationale guatémaltèque, découvert en 2005, en sont un exemple.

43. Cet exemple est emblématique de la manière dont la technologie et l'application de techniques adéquates, y compris les méthodes statistiques, en termes d'échantillon aléatoire de documents en plusieurs étapes, de modèle de données et de cadre de codage, permettent de préserver, de numériser et d'inspecter une énorme quantité de données, dans l'impossibilité d'examiner systématiquement chaque document individuel.[51] L'accès informatique, la reconnaissance optique des caractères, la reconnaissance de l'écriture manuscrite, ainsi que la reconnaissance faciale et

[46] Par exemple, s'agissant de l'application Telegram, plus de 200 photos de personnes portées disparues en Ukraine - dont certaines sont victimes de disparition forcée - sont publiées quotidiennement. M. Neuville, *Les réseaux sociaux, principaux alliés dans la recherche des personnes disparues*, 2022. Dans d'autres contextes, TikTok est utilisé pour signaler des abus, y compris des disparitions forcées.

[47] Article 17 de la Déclaration sur la protection de toutes les personnes contre les disparitions forcées ; Observation générale sur la disparition forcée en tant que crime continu et article 8 de la Convention internationale pour la protection de toutes les personnes contre les disparitions forcées.

[48] Principe 7 des Principes directeurs de 2019 pour la recherche des personnes disparues.

[49] Sur la manière dont les technologies peuvent contribuer à faire progresser la justice transitionnelle (par le biais de la documentation, de la numérisation et de la mémorialisation), voir le numéro spécial de 2019 de l'*International Journal of Transitional Justice*.

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

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

TRADUCTION NON OFFICIELLE

vocale pour analyser le matériel audiovisuel,[52] sont des outils cruciaux dans ce domaine. En outre, cet exemple montre le rôle central joué par la coopération internationale, que ce soit dans le contexte des organisations de la société civile, du monde universitaire[53] ou au niveau intergouvernemental.[54] Des considérations similaires s'appliquent aux quantités massives de données téléchargées dans les réseaux sociaux, ou aux sous-produits documentaires des initiatives de recherche de la vérité, qui peuvent contenir des preuves de crimes internationaux, y compris de disparitions forcées, et nécessitent une conservation et un traitement à long terme adéquats et bien réglementés. Les outils médico-légaux, y compris la comparaison des bases de données créées par différents acteurs, sont essentiels pour assurer la validation, l'identification, l'analyse, l'interprétation, la documentation et la présentation des informations numériques provenant de sources et d'archives numériques.

44. Le Groupe de travail a également reçu des informations qui illustrent comment les outils numériques – souvent créés par des organisations de la société civile – peuvent être utilisés non seulement pour chercher les personnes disparues, mais aussi – grâce à des interventions à un stade précoce – pour empêcher que des détentions arbitraires se transforment en disparitions forcées.[55] Ces outils offrent des options gratuites et sûres qui aident les proches des personnes disparues à naviguer dans les méandres de la bureaucratie et à obtenir rapidement des informations qui peuvent s'avérer vitales, ou à gérer leur dossier auprès des autorités nationales[56] En outre, il a été suggéré que les applications existantes utilisées dans le contexte des violences domestiques,[57] pourraient être adaptées pour prévenir les disparitions forcées ou pour faciliter les activités de recherche. Le Groupe de travail a reçu des informations sur la manière dont des migrants, craignant de courir un risque immédiat de disparition forcée, ont utilisé les réseaux sociaux pour partager des séquences vidéo de leur emplacement et des coordonnées géographiques en direct, ce qui s'est avéré utile pour déterminer leur sort et le lieu où ils se trouvent et, parfois, pour recueillir des preuves de crimes perpétrés à leur encontre.

45. Le Groupe de travail a pris connaissance d'études visant à explorer comment l'utilisation de l'intelligence artificielle et de l'apprentissage automatique, par le biais de l'analyse des données du réseau des smartphones, peut contribuer à établir le lieu où se trouvent les personnes disparues. Ces études en sont à un stade embryonnaire et peuvent s'avérer cruciales pour parvenir à la clarification de nombreux cas, comme le montrent les expériences réussies lancées par des organisations de la société civile qui utilisent l'intelligence artificielle et les technologies de la publicité numérique pour localiser des enfants portés disparus.[58] Ces études et expériences devraient être encouragées, notamment par le biais du financement et de la coopération internationale. Néanmoins, l'existence de différences socio-économiques significatives doit être prise en considération, dans le but de fournir un soutien adéquat et d'assurer l'accès à ces nouvelles technologies aux pays en développement. Dans ce contexte, les États doivent coopérer et

TRADUCTION NON OFFICIELLE

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

[53] Le groupe d'analyse des données sur les droits humains a conçu la stratégie et mis en œuvre les techniques qui ont permis d'obtenir les résultats remarquables mentionnés. L'Université du Texas, dans le cadre d'un projet de collaboration, a ainsi publié et héberge l'Archive Historique de la police nationale guatémaltèque.

[54] Le projet *Condor Document Archives* du Marché commun du Sud (MERCOSUR) est un exemple notable de coopération interétatique visant à renforcer les capacités en matière médico-légal et de documentation. Les Nations unies ont soutenu plusieurs initiatives d'identification et de collecte de données dans le monde entier (A/HRC/36/50/Add.1, §§ 5, 8, 35, 36, 58).

[55] Par exemple, le *chatbot* « BUSQUEMOS », développé par l'ONG mexicaine *Documenta*, facilite la recherche rapide des personnes disparues qui peuvent être détenues dans différents centres de détention, allant des prisons, commissariats de police, casernes ou centres de rétention des migrants aux institutions de santé mentale et aux hôpitaux. Il offre une assistance gratuite, par le biais d'interactions qui durent moins de 5 minutes et qui n'obligent pas les utilisateurs à divulguer des données sensibles.

[56] Par exemple, la plateforme « Nosomosexpedientes », développée par l'ONG mexicaine Centro de Derechos Humanos Miguel Augustín Pro Juárez, qui soutient les familles dans leurs efforts de recherche et dans la gestion de leurs dossiers auprès les autorités nationales.

[57] Référence a été faite à la plateforme « Save You ».

[58] Voir la plateforme lancée en 2018 par le Centre international pour les enfants portés disparus et exploités.

s'accorder l'entraide la plus large possible pour rechercher, localiser et libérer les personnes disparues et, en cas de décès, pour les exhumer, les identifier et restituer leurs restes.[59]

III. Utilisation des nouvelles technologies pour documenter les cas de disparitions forcées et juger et sanctionner les auteurs de ces crimes

46. L'utilisation des technologies pour documenter les violations flagrantes des droits humains et promouvoir l'obligation de rendre des comptes, en particulier par le biais de renseignements provenant de sources ouvertes, a fait l'objet d'une attention croissante[60] et de rapports fondamentaux publiés par d'autres procédures spéciales des Nations unies.[61] Comme indiqué, les technologies peuvent jouer un rôle crucial dans l'obtention de données et d'informations permettant de clarifier le sort des personnes disparues et le lieu où se trouvent, mais aussi pour identifier les responsables des crimes concernés. Toutefois, les résultats obtenus par ces moyens doivent être garantis de manière à résister à un examen minutieux, y compris dans le cadre d'une procédure pénale, où la norme de preuve applicable est « l'intime conviction » (« au- delà de tout doute raisonnable » dans certains systèmes). Il peut être particulièrement complexe de déterminer la source des éléments de preuve recueillis grâce aux technologies et d'exclure qu'ils aient fait l'objet d'une falsification ou d'une manipulation. En outre, les algorithmes de suppression par apprentissage automatique (*machine-learning deletion algorithms*) mis en œuvre par des plateformes telles que Google ou Facebook peuvent rapidement effacer des contenus numériques, entraînant ainsi la perte de preuves qu'il devient pratiquement impossible de récupérer.

47. Cette utilisation peut s'avérer particulièrement difficile dans les cas de disparition forcée, un crime qui, par nature, est entouré de secret et caractérisé par la dissimulation et l' « absence », plutôt que par la présence d'éléments de preuve manifestes. En ce sens, s'il peut être relativement facile d'apporter la preuve, grâce aux nouvelles technologies, de deux des éléments matériels constitutifs du crime (à savoir la privation de liberté de la victime et l'affiliation des auteurs), l'élément de dissimulation du sort de la personne disparue ou du lieu où elle se trouve pose davantage de difficultés, de même que, le cas échéant (c'est-à-dire conformément à la définition de la disparition forcée en tant que crime contre l'humanité contenue dans le Statut de Rome de la Cour pénale internationale),[62] celui de l'intention de soustraire la personne disparue à la protection de la loi pendant une période prolongée.

48. Comme indiqué dans l'une des communications reçues, les particularités des disparitions forcées nécessitent une application « agrégée » des renseignements à code source ouvert, chacun d'entre eux ciblant un élément spécifique de la définition de l'acte. Le caractère secret » du crime, ainsi que la présence d'un élément mental spécifique dans la définition de la disparition forcée en tant que crime contre l'humanité figurant dans le Statut de Rome de la Cour pénale internationale, font qu'il est peu probable que les renseignements à code source ouvert fournissent à eux seuls tous les éléments permettant de qualifier un comportement spécifique de disparition forcée. Cependant, ils pourraient fournir des indications utiles sur l'identité de la victime, l'acte de privation de liberté, le lieu de détention, l'identité et l'affiliation de l'auteur de la disparition forcée. Les renseignements à code source ouvert pourraient même être utilisés pour documenter l'élément contextuel du crime en droit international pénal – c'est-à-dire la présence d'une attaque dirigée contre une population civile, son caractère généralisé ou systématique, et la commission de l'acte dans le cadre de l'attaque.

[59] Convention internationale pour la protection de toutes les personnes contre les disparitions forcées, art. 15.

[60] Entre autres, le symposium publié en 2023 par *Opinio Juris* sur l'équité, l'égalité et la diversité dans les enquêtes sur les sources ouvertes; le numéro spécial publié en 2021 par le *Journal of International Criminal Justice* sur les nouvelles technologies et les enquêtes sur les crimes internationaux.

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

[62] Art. 7, paragraphe 2 (i), du Statut de Rome de 1998 de la Cour pénale internationale et les législations pénales qui transposent la même définition du crime dans les ordres juridiques nationaux.

TRADUCTION NON OFFICIELLE

49. Trouver et rassembler des informations concluantes par le biais des technologies – et en particulier des technologies de l'information et de la communication – exige des efforts considérables en termes d'investigation, de vérification et de conservation ciblées, qui devraient toujours être effectuées de manière systématique et professionnelle, notamment pour garantir la chaîne de conservation et, le cas échéant, l'admissibilité devant les tribunaux à un stade ultérieur. Tout au long du processus, depuis la collecte des preuves par le biais des technologies jusqu'à leur comparution devant un tribunal, les implications éthiques et sécuritaires doivent être dûment prises en compte. En particulier, l'évaluation des risques doit tenir compte des aspects liés à la protection de la vie privée et des données, de l'obtention – si possible – du consentement éclairé des personnes et des communautés concernées et des risques liés aux données démographiques identifiables.

50. Les premières heures et les premiers jours suivant la privation de liberté des personnes sont cruciaux pour obtenir des données qui pourraient rapidement être effacées ou manipulées. L'existence d'images satellites accessibles au public, de réseaux sociaux numériques et de smartphones équipés d'appareils photo offrent des données précieuses auxquelles il est possible d'accéder de manière relativement facile et peu coûteuse et qui fournissent des preuves de la commission de crimes, y compris de disparitions forcées. Le Groupe de travail a pris connaissance avec intérêt d'applications et de logiciels qui capturent et conservent des copies probantes de contenus en ligne et de matériel audiovisuel, en les intégrant avec les métadonnées nécessaires pour en démontrer l'authenticité devant les tribunaux, et en facilitant l'annotation des contenus.[63]

51. La préservation de la chaîne de contrôle des preuves obtenues grâce aux nouvelles technologies est essentielle pour garantir l'authenticité du matériel recueilli. Le Protocole de Berkeley consacre les principes fondamentaux à respecter dans ce contexte et devrait être diffusé et mis en œuvre, de même que d'autres lignes directrices en la matière élaborées par des organisations de la société civile.[64] Les aspects qui requièrent une attention particulière sont liés à la fragilité inhérente aux technologies, à la nécessité de normaliser la gestion technique des ensembles de données archivées et à la validation de ces données. Le Groupe de travail a pris connaissance de programmes qui, utilisant souvent l'intelligence artificielle, permettent d'évaluer l'intégrité des images numériques et de détecter les supports falsifiés. Ces technologies offrent une aide significative dans la collecte de preuves admissibles devant les tribunaux.

52. Les séquences vidéo et les images publiées sur les réseaux sociaux ou recueillies par des caméras corporelles ou de surveillance peuvent contenir des preuves de la commission de violations flagrantes des droits de l'homme, y compris les disparitions forcées, et ont été acceptés comme preuves valables devant les tribunaux, par les organisations internationales de défense des droits humains et par les commissions d'enquête. Par exemple, la Cour européenne des droits de l'homme a considéré qu'une vidéo postée sur Youtube constituait une preuve valable des mauvais traitements subis par une personne disparue après avoir été privée de sa liberté.[65] La Cour pénale internationale a délivré un mandat d'arrêt fondé principalement sur des preuves recueillies à partir de messages sur les réseaux sociaux;[66] la Mission internationale indépendante d'établissement des faits pour le Myanmar s'est appuyée sur des données audiovisuelles et des messages écrits sur les réseaux sociaux comme preuves pour demander l'ouverture d'une enquête sur des crimes internationaux;[67] et des tribunaux nationaux ont admis des preuves de sources ouvertes dans des procès concernant des crimes internationaux.[68] La possibilité d'évaluer, de vérifier et, en fin de compte, d'admettre des éléments de preuve recueillis par le biais de technologies dépend de la

[63] Voir l'annexe I. Les métadonnées concernées comprennent au minimum un horodatage, des données de localisation et un code alphanumérique unique. Elles doivent ensuite être stockées de manière sécurisée, de préférence après cryptage.

[64] Voir, entre autres, la méthodologie d'enquête en ligne sur les incidents survenus en Ukraine depuis le 24 février 2022, publiée par Bellingcat et Global Legal Action Network.

[65] CourEDH, *S.T. et Y.B. c. Russie*, arrêt du 19 octobre 2021, §§ 10, 22, 48 et 80.

[66] Voir les mandats d'arrêt délivrés respectivement en 2017 et 2018 par la Cour pénale internationale dans l'affaire *Le Procureur c. Al-Werfalli*. Ces dernières années, la Division des enquêtes de la Cour a mis en place un Conseil consultatif scientifique et un Conseil consultatif en matière de technologie.

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

[68] Entre autres, voir le rapport du réseau Eurojust « Genocide Network » de l'Union européenne, 2018, qui mentionne les exemples de l'Allemagne, de la Finlande et de la Suède.

TRADUCTION NON OFFICIELLE

capacité de chaque tribunal et des compétences et connaissances du personnel, qui peuvent varier considérablement, en particulier au niveau national. Le Groupe de travail estime que les États doivent adopter toutes les mesures nécessaires à cet égard, notamment en garantissant les ressources économiques, techniques et humaines nécessaires et en offrant des formations régulières aux autorités concernées.

53. Le Groupe de travail a été informé que les nouvelles technologies – y compris les programmes de géolocalisation, le suivi des vols, l'analyse des réseaux, la modélisation en 3D, la télédétection, l'analyse audio, la synchronisation et la photogrammétrie – se sont déjà révélées efficaces pour reconstituer les scènes de crime et retrouver les auteurs présumés de crimes et de violations des droits de l'homme. Leur utilisation devrait donc être envisagée dans le cadre d'un protocole d'enquête régulier sur les disparitions forcées. Une combinaison de techniques (par exemple, l'imagerie satellite, la cartographie numérique, l'analyse de séquences vidéo et la chrono-localisation) a également été utilisée avec succès pour recueillir des preuves de disparitions forcées de migrants et pour établir leur sort et le lieu où ils se trouvent.[69]

54. Le Groupe de travail a reçu des informations sur un nombre croissant de cas où, face à l'indifférence ou à l'inaction des autorités, des proches de personnes disparues ou leurs représentants, ou de multiples organisations de la société civile, par le biais d'exercices de *crowd-solving*, ont réussi à recueillir, à l'aide de technologies, des informations sur les circonstances de la disparition et sur l'identité ou l'affiliation des auteurs de la disparition. Ils ont utilisé les réseaux sociaux, l'Internet, des caméras en circuit fermé (CCTV), les registres d'appels, le suivi des données mobiles et la géolocalisation ou l'imagerie satellite. Si ces expériences ont permis d'obtenir des résultats significatifs, elles ont également exposé les personnes concernées à des risques importants, comme l'illustre la section II.

55. Le Groupe de travail note que la charge de la collecte de ce type de données par le biais des technologies ne peut être laissée aux proches des disparus et à leurs représentants, alors que les autorités ne semblent pas rechercher, vérifier, analyser et sécuriser ces preuves de manière systématique, bien qu'elles soient dans l'obligation de le faire. Les États doivent intensifier leurs efforts et prendre toutes les mesures nécessaires pour renforcer la capacité des autorités compétentes à utiliser les technologies dans les enquêtes sur les disparitions forcées. Les États s'accordent mutuellement l'entraide judiciaire la plus large possible dans le cadre des procédures pénales engagées à la suite d'une disparition forcée, y compris le rassemblement et la communication de tous les éléments de preuve dont ils disposent et qui sont nécessaires aux fins la procédure.[70]

V. Conclusions et recommandations

56. Comme dans de nombreux aspects des nouvelles technologies, la relation de ces dernières avec les droits de l'homme – dans ce cas, dans le domaine des disparitions forcées – est ambivalente. D'une part, les nouvelles technologies, et notamment les technologies de l'information et de la communication, sont fréquemment utilisées pour faciliter ou dissimuler la commission de disparitions forcées, entraver le travail des défenseurs des droits de l'homme et des proches des personnes disparues, et les intimider ou les harceler. Les technologies se développent à un rythme rapide et sont souvent commercialisées et utilisées sans diligence raisonnable en matière de droits humains par les États et les entreprises, en l'absence d'un cadre réglementaire solide qui tienne compte du droit international des droits de l'homme, assure une surveillance indépendante et promeut la responsabilisation et la responsabilité et offre un recours efficace en cas de violations.

57. Le Groupe de travail est particulièrement préoccupé par le recours aux fermetures de l'accès à l'Internet et aux interruptions ciblées de la connectivité, aux programmes de

[69] Parmi d'autres, www.borderviolence.eu/pushback-from-north-macedonia-visual-analysis/ et https://forensic-architecture.org/investigation/pushbacks-across-the-evros-meric-river-the-case-of- parvin.

[70] Convention internationale pour la protection de toutes les personnes contre les disparitions forcées, art. 14.

TRADUCTION NON OFFICIELLE

logiciels espions, à la surveillance ciblée et de masse, y compris la reconnaissance de la démarche et du visage, aux cyberattaques et aux usines à trolls parrainées par les gouvernements, ainsi qu'à l'utilisation spécieuse de la législation liée à la technologie pour réprimer la dissidence et cibler les défenseurs des droits de l'homme et les proches des personnes disparues.

58. En ce qui concerne la recherche des personnes disparues, la documentation du crime et la promotion de la responsabilité, les nouvelles technologies peuvent offrir des solutions rentables qui se sont déjà avérées utiles et qui sont susceptibles d'avoir d'autres conséquences pertinentes. Le Groupe de travail souligne qu'il ne faut pas trop compter sur les nouvelles technologies dans ce domaine et que les attentes doivent être réalistes: même si elles vont faciliter les processus concernés, elles ne vont pas résoudre tous les problèmes existants. Les approches et les techniques traditionnelles de documentation, de suivi et d'établissement de rapports ne doivent pas être abandonnées et ne peuvent pas être entièrement remplacées par le matériel numérique et les nouvelles technologies.

59. La complémentarité entre ces stratégies doit être recherchée et activement promue, et les processus traditionnels centrés sur l'être humain doivent être encouragés et renforcés en conséquence. Parallèlement, l'accès aux nouvelles technologies doit être conçu de manière à ne pas reproduire ou aggraver la fracture numérique et les différences socio-économiques existantes et à ne laisser aucun pays en développement ou acteur concerné à la traîne.

60. Le fait que les nouvelles technologies offrent des solutions rentables qui pourraient faire progresser de manière significative la recherche des personnes disparues et les enquêtes criminelles et que certains des outils pertinents sont facilement accessibles et peuvent être utilisés également par les organisations de la société civile et les associations de familles de personnes disparues est une évolution positive qui peut s'avérer déterminante pour offrir une meilleure protection contre les disparitions forcées.

61. Le Groupe de travail encourage les organisations de la société civile à explorer ces possibilités et à renforcer leurs capacités, mais il réaffirme que la recherche des personnes disparues et les enquêtes pénales correspondantes sont des obligations internationales des États, qui ne peuvent pas en laisser l'entière responsabilité à la société civile et aux proches des personnes disparues et s'en remettre à leur seule initiative. Les États devraient adopter des mesures pour inclure les nouvelles technologies dans les activités de recherche et les enquêtes criminelles. Les États ont également l'obligation de coopérer et de se prêter mutuellement l'entraide la plus large possible dans ces domaines.

62. Le Groupe de travail note que la coopération entre les différents acteurs concernés, notamment les États, les entreprises, les organisations de la société civile, les institutions nationales des droits humains, les universités et les bailleurs de fonds, est indispensable et qu'elle doit donc être encouragée. Les recommandations suivantes reflètent ce point de vue. En particulier, le Groupe de travail encourage le renforcement de la coordination et de la coopération entre les différents acteurs concernés afin de forger des alliances pour détecter les risques liés aux nouvelles technologies et aux disparitions forcées, concevoir des stratégies d'atténuation et des mesures efficaces pour surmonter les obstacles identifiés et promouvoir des outils pour soutenir les personnes directement concernées, y compris les défenseurs des droits humains et les proches des personnes disparues. Il est de notre responsabilité commune de veiller à ce que les nouvelles technologies soient développées et utilisées dans le respect des droits humains, de manière éthique et responsable.

63. Le Groupe de travail s'engage à suivre régulièrement la question des nouvelles technologies et des disparitions forcées et à inclure systématiquement des remarques et des recommandations à ce sujet dans ses activités, y compris dans les communications, les appels urgents, les allégations, les renvois, les lettres d'intervention rapide, les visites de pays et les actions de sensibilisation. Le Groupe de travail offre également son assistance en la matière aux États par le biais de services de coopération.

TRADUCTION NON OFFICIELLE

64. Le Groupe de travail appelle tous les acteurs concernés à collaborer régulièrement avec lui et à faire rapport sur l'impact négatif des nouvelles technologies sur la jouissance des droits humains, en particulier pour les défenseurs des droits humains et les proches des personnes disparues, ainsi que sur les progrès réalisés en ce qui concerne l'utilisation des nouvelles technologies dans la recherche des personnes disparues et dans les enquêtes et la promotion de l'obligation de rendre des comptes.

65. À cette fin, le Groupe de travail recommande aux États de:

(a) S'abstenir d'imposer des fermetures d'accès à l'Internet et des restrictions d'accès aux communications ou à des plateformes de réaux sociaux spécifiques;

(b) Maximiser l'accès à l'Internet et supprimer les multiples obstacles qui entravent les communications;

(c) Adopter toutes les mesures nécessaires pour garantir que les défenseurs des droits humains, les proches des personnes disparues, les journalistes et les utilisateurs des réseaux sociaux puissent exercer sans ingérence indue leur droit à la liberté d'opinion et à la liberté d'expression en ligne (par exemple, par le biais des réseaux sociaux, des blogs ou de comptes similaires) sans être poursuivis pour avoir informé sur, ou dénoncé des, disparitions forcées; des mesures devraient également être prises pour garantir que la législation sur la cybersécurité n'est pas appliquée de manière spécieuse pour freiner la dissidence;

(d) Veiller à ce que le téléchargement et l'utilisation d'une application ne puissent servir de preuve unique ou décisive d'une infraction pénale;

(e) Assurer la formation du personnel chargé de l'application de la loi, civil ou militaire, et des fonctionnaires sur les garanties fondamentales à assurer lors de l'arrestation de tout individu, en particulier en ce qui concerne les normes applicables à la confiscation, à l'inspection ou à la destruction des dispositifs électroniques; et juger et sanctionner ceux qui ne respectent pas ces règles ;

(f) Prendre toutes les mesures nécessaires pour prévenir les cyberattaques, les campagnes de diffamation et de désinformation contre les défenseurs des droits humains, y compris les proches des personnes disparues, par le biais du *phishing*, des *malware*, de *ransomware*, de l'espionnage, des fuites d'informations faux (*tainted leaks*), des « fermes de trolls » et du *doxxing*, et enquêter sur tous les cas pertinents en vue d'identifier, de poursuivre et de sanctionner les responsables et d'offrir une réparation aux victimes;

(g) Imposer un moratoire immédiat sur l'exportation, la vente, le transfert, l'utilisation ou l'entretien des outils de surveillance ciblée et de masse développés par le secteur privé, y compris les logiciels espions, la reconnaissance faciale et des programmes similaires, jusqu'à ce qu'un régime de sauvegarde conforme aux droits humains soit en place;

(h) Élaborer et mettre en œuvre sans délai un cadre juridique dans lequel l'octroi de licences pour toute technologie, et en particulier pour les technologies de surveillance ciblée et de masse, serait subordonné à un examen national des droits humains et au respect par les entreprises des Principes Directeurs relatifs aux entreprises et aux droits de l'homme; ce cadre doit garantir que le transfert, la vente et l'acquisition de technologies de surveillance ciblée et de masse fassent l'objet d'une consultation et d'un contrôle publics;

(i) Prendre toutes les mesures nécessaires pour enquêter sur les individus, les entreprises et les États responsables de violations des droits humains liées à la vente, au transfert et à l'utilisation de technologies de surveillance ciblée et de masse, les poursuivre et les obliger à rendre des comptes;

(j) Veiller à ce que les personnes ou les organisations de la société civile visées puissent exercer leur droit à un recours effectif et obtenir réparation;

TRADUCTION NON OFFICIELLE

(k) Garantir que la collecte, la conservation et l'utilisation des données biométriques et génétiques soient réglementées par la loi et dans la pratique, qu'elles aient une portée limitée, qu'elles sont transparentes, nécessaires et proportionnées à la réalisation d'un objectif légitime de sécurité et qu'elles ne soient pas fondées sur une distinction, exclusion, restriction ou préférence fondée sur la race, la couleur, l'ascendance ou l'origine nationale ou ethnique;

(l) Examiner, dans le cadre d'un processus multidisciplinaire, l'adéquation des politiques et des cadres juridiques applicables, afin de concevoir des stratégies visant à prévenir et à traiter les incidences négatives sur les droits humains générées par l'utilisation des nouvelles technologies, y compris l'apprentissage automatique et l'intelligence artificielle;

(m) Veiller à ce que les technologies de surveillance de masse et ciblée, ainsi que les solutions d'intelligence artificiel et d'apprentissage automatique, ne soient pas utilisées aux frontières dans le but de mener des opérations de refoulement qui peuvent conduire, et dans certains cas équivaloir à, des disparitions forcées. Les données sur les mouvements migratoires recueillies grâce à ces technologies devraient être utilisées pour faciliter les opérations de recherche et de sauvetage et à des fins humanitaires;

(n) Veiller à ce que les technologies utilisées pour la recherche des personnes disparues et les enquêtes correspondantes intègrent la collection et l'analyse de détails sur la personne concernée dans une optique de genre, afin d'englober les expériences et les expressions non normatives;

(o) Rechercher de manière active la personne disparue vivante et adopter les mesures et les ressources nécessaires pour développer et appliquer des technologies qui se concentrent sur les premiers étapes d'une disparition forcée;

(p) Adopter toutes les mesures nécessaires pour garantir que les autorités chargées de la recherche des personnes disparues et des enquêtes criminelles correspondantes disposent de ressources financières, humaines et techniques adéquates et, en particulier, de technologies de pointe (y compris LiDAR, unités SONAR, drones, imagerie satellite, etc.) et soient régulièrement et dûment formées, y compris à l'application du Protocole de Berkeley;

(q) Coopérer avec les autres États, en s'accordant mutuellement l'entraide la plus large possible dans l'utilisation des technologies visant à faciliter la recherche des personnes disparues et en ce qui concerne l'assistance juridique dans le cadre des procédures pénales engagées à la suite d'une disparition forcée, y compris la collecte et la communication de tous les éléments de preuve dont ils disposent et qui sont nécessaires aux fins de la procédure;

(r) Assurer l'interopérabilité des bases de données génétiques qui peuvent contribuer à la recherche des personnes disparues, en garantissant que les données qu'elles contiennent soient stockées de manière sécurisée et utilisées à des fins exclusivement humanitaires. En particulier, les initiatives visant à améliorer l'identification et l'échange biométriques et génétiques entre les forces, notamment aux frontières, devraient être guidées par le fait que les prétendues considérations de sécurité ne peuvent prévaloir sur la garantie des droits humains fondamentaux, y compris le droit de connaître la vérité en ce qui concerne d'hypothétiques disparitions forcées;

(s) Adopter toutes les mesures nécessaires, y compris par le biais des technologies, pour préserver et faciliter l'accès aux archives susceptibles de contenir des informations pertinentes sur les disparitions forcées;

(t) Fournir une formation adéquate et régulière aux autorités d'enquête et judiciaires nationales sur la collecte, le stockage, la validation et l'évaluation des preuves obtenues grâce aux nouvelles technologies, en garantissant les ressources nécessaires et en développant ou en renforçant l'infrastructure correspondante.

66. Le Groupe de travail recommande aux entreprises de technologies et de logiciels:

TRADUCTION NON OFFICIELLE

(a) Mener leurs activités, notamment en ce qui concerne le développement, la vente, le transfert et l'utilisation de nouvelles technologies, en respectant les Principes Directeurs des Nations unies relatifs aux entreprises et aux droits de l'homme;

(b) Prendre toutes les mesures pour prévenir les perturbations et les fermetures de l'accès à l'Internet que l'État leur a demandé de mettre en œuvre et faire preuve de diligence raisonnable pour évaluer les risques pour les droits humains et agir en conséquence, atténuer les effets négatifs éventuels et garantir l'accès à un recours;

(c) Prendre toutes les mesures nécessaires pour prévenir les cyberattaques, les campagnes de diffamation et de désinformation contre les défenseurs des droits humains, y compris les proches des personnes disparues, par le biais du *phishing*, des *malware*, des *ransomwares*, de l'espionnage, des fuites d'informations faux (*tainted leaks*), des « fermes de trolls » et du *doxxing*;

(d) Les fournisseurs d'accès à l'Internet, les réseaux sociaux et les plateformes connexes devraient alerter leurs utilisateurs sur les tentatives de piratage du gouvernement et élaborer un guide à l'intention des utilisateurs des plateformes numériques, les informant des risques de cyberattaques et de vol et d'utilisation de leurs données et métadonnées, en partageant les bonnes pratiques pour prévenir de tels instances; ils devraient également mettre en place des garanties solides pour protéger les métadonnées des utilisateurs contre la mauvais exploitation;

(e) Les entreprises de surveillance devraient prendre toutes les mesures nécessaires pour respecter leurs obligations internationales en matière de droits humains; en particulier, elles devraient faire preuve de diligence et procéder à une évaluation approfondie de l'impact sur les droits humains avant toute vente ou transfert potentiel impliquant des technologies de surveillance ciblée et de masse, y compris la reconnaissance faciale, les logiciels espions et des programmes similaires; elles devraient inclure des clauses contractuelles interdisant l'utilisation de technologies de surveillance en violation du droit international des droits de l'homme et, en cas de détection d'une utilisation abusive, le signaler rapidement aux organes de contrôle nationaux, régionaux ou internationaux compétents; elles devraient également mettre en place des mécanismes de réparation permettant aux victimes d'abus de déposer plainte et de demander réparation;

(f) Contribuer au développement de moyens plus sûrs pour collecter, stocker et analyser les données – en particulier les informations sensibles concernant les personnes disparues et leurs proches, en veillant à ce qu'elles soient utilisées exclusivement à des fins humanitaires; développer des outils libres et facilement accessibles pour effectuer une analyse médico-légale des appareils électroniques et des espaces numériques potentiellement compromis;

(g) Contribuer au développement de technologies qui permettent de rechercher de manière active les personnes disparues vivantes et qui se concentrent sur les premiers stades d'une disparition forcée;

(h) Envisager d'investir dans le développement de technologies qui, associées à des approches **traditionnelles centrées sur l'être humain, permettent de rechercher les personnes dont la disparition forcée a commencé avant l'existence des smartphones et de mener les enquêtes pénales correspondantes;**

(i) Promouvoir le développement de technologies, y compris d'outils médico-légaux, qui permettent d'assurer la validation, l'identification, l'analyse, l'interprétation, la documentation et la présentation des informations provenant de sources numériques et de procéder à des recoupements entre plusieurs archives.

67. Le Groupe de travail recommande aux organisations de la société civile, aux institutions nationales de défense des droits humains et aux universités de:

(a) Poursuivre leurs efforts pour documenter et dénoncer des cas de fermeture de

TRADUCTION NON OFFICIELLE

l'accès à l'Internet et de perturbations ciblées, ainsi que les cyberattaques, les campagnes de diffamation et de désinformation à l'encontre des défenseurs des droits humains, y compris les proches des personnes disparues;

(b) Mettre tout en œuvre pour accroître la sensibilisation aux risques existants liés à l'utilisation des nouvelles technologies et, en particulier, à la sensibilité et à l'altération des données, en vue de renforcer les compétences de base en matière de culture et d'hygiène numériques;

(c) Poursuivre leurs efforts pour développer des outils numériques qui aident les proches des personnes disparues dans la gestion des dossiers, les assistent dans le processus de recherche et soutiennent la prévention des disparitions forcées;

(d) Poursuivre leurs efforts en matière de renseignement à code source ouvert, en appliquant les principes énoncés dans le Protocole de Berkeley;

(e) Mener des recherches supplémentaires sur les questions relatives aux nouvelles technologies et aux disparitions forcées, en particulier en ce qui concerne les bonnes pratiques existantes, contribuant ainsi à améliorer leur visibilité et leur diffusion.

68. Le Groupe de travail recommande aux agences de développement et aux bailleurs de fonds de:

(a) Intégrer les considérations relatives aux droits humains dans les efforts visant à étendre les réseaux de communication et à réduire la fracture numérique mondiale;

(b) Prendre toutes les mesures nécessaires pour garantir au plus grand nombre un accès abordable à l'Internet afin d'accroître l'utilisation des technologies fondées sur l'Internet pour faciliter l'exercice des droits humains, notamment en ce qui concerne la recherche des personnes disparues et l'établissement des preuves des crimes correspondants;

(c) Soutenir les projets visant à documenter et à dénoncer les effets négatifs des nouvelles technologies sur les droits humains, en particulier dans les cas de disparitions forcées;

(d) Soutenir les programmes de formation sur la culture et l'hygiène numériques, ainsi que sur les renseignements provenant de données à code source ouvert, destinés aux organisations de la société civile et, en particulier, aux associations de familles de personnes disparues, afin de les sensibiliser aux risques existants et de veiller à ce qu'elles renforcent leurs capacités de base dans ces domaines, notamment pour détecter les événements numériques indésirables, y répondre et restaurer la situation à son état antérieur;

(e) Soutenir le développement de technologies visant à faciliter la recherche des personnes disparues et les enquêtes correspondantes et garantir l'accès à ces outils – ainsi qu'une formation adéquate du personnel - dans les pays les moins développés;

(f) Soutenir des projets visant à promouvoir l'utilisation des technologies pour assurer la vérification, l'analyse, l'interprétation et la présentation des informations contenues dans les archives et les sources numériques;

(g) Soutenir les études visant à explorer comment l'utilisation de l'intelligence artificielle et de l'apprentissage automatique, par le biais de l'analyse des données des smartphones de réseau, peut contribuer à établir le lieu où se trouvent les personnes disparues et le développement des technologies correspondantes.

69. Le Groupe de travail recommande aux autres mécanismes de protection des droits humains et aux tribunaux internationaux:

(a) Promouvoir l'obligation de rendre des comptes pour les États, les entreprises ou les particuliers responsables de l'utilisation abusive des technologies de surveillance ciblée ou de masse, les cyberattaques et, en général, de l'utilisation des nouvelles technologies pour faciliter ou dissimuler la commission de disparitions forcées;

(b) Adapter les critères de preuve applicables afin que les preuves de disparition

TRADUCTION NON OFFICIELLE

forcée produites par des renseignements provenant de sources ouvertes soient dûment prises en compte dans les procédures concernées.

70. Le Groupe de travail recommande au Haut-Commissariat des Nations unies aux droits de l'homme:

(a) Veiller à ce que des moyens adéquats soient fournis pour renforcer la protection des informations sensibles concernant les personnes disparues et leurs proches par le Haut-Commissariat, les Procédures Spéciales ou d'autres mécanismes, tels que les commissions d'enquête ou les missions d'établissement des faits;

(b) Diffuser et promouvoir l'application du Protocole de Berkeley.

TRADUCTION NON OFFICIELLE

Annexe I

Cartographie des outils, contacts et ressources gratuites accessibles au public qui peuvent fournir des informations utiles sur les technologies nouvelles/numériques et aider et faciliter la recherche des personnes disparues et les enquêtes criminelles correspondantes [non exhaustive]

Organisations à but non lucratif, collectifs et entreprises technologiques

- Access now: dédiée à la défense et extension des droits numériques des personnes et des communautés à risque
- Bellingcat: collectif indépendant d'enquêtes en ligne
- Border Forensics: agence utilisant l'analyse spatiale et visuelle pour enquêter sur les pratiques de violence à la frontière
- Chercheurs citoyens médico-légaux: Forces unies pour nos disparus de Nuevo León (FUNDENL); Forces unies pour nos disparus de Coahuila (FUUNDEC); Forces unies pour nos disparus du Mexique (FUUNDEM) - organisations qui font partie de mouvements dirigés par des victimes et qui ont une approche unique à l'utilisation de la technologie pour la recherche de leurs proches disparus
- Institut CyberPeace: ONG qui œuvre, notamment en soutenant les organisations de la société civile, à la réduction des dommages causés par les cyber-attaques
- Digipower Academy: aide les personnes et les ONG à se familiariser avec les données et les flux de données
- Digital Preservation Coalition: organisation qui soutient la fourniture d'un accès à long terme aux contenus et services numériques
- Electronic Frontier Foundation: ONG défendant les libertés civiles dans l'espace numérique
- Equipo Argentino de Antropología Forense (EAAF): ONG engagée depuis 1986 dans le développement de techniques d'anthropologie médico-légale pour aider à localiser et à identifier les victimes de disparitions forcées
- Frontline Defenders: ONG qui soutient les défenseurs des droit humains en danger, notamment en raison de l'(ab)us des nouvelles technologies
- Human Rights Data Analysis Group: offrit une analyse statistique des données relatives aux violations flagrantes des droits humains
- HURIDOCS: ONG qui aide les groupes de défense des droits humains à recueillir, organiser et utiliser des informations
- ICT4peace: fondation promouvant l'utilisation des technologies de l'information et de la communication pour la construction de la paix
- Locate International: organisme caritatif enregistré au Royaume-Uni qui, en partenariat avec des universités, des organismes d'application de la loi, la police et les familles de personnes disparues, aide ces dernières à retrouver leurs proches
- Meedan: association technologique à but non lucratif qui développe des logiciels et des initiatives visant à renforcer le journalisme mondial, la culture numérique et l'accessibilité de l'information

TRADUCTION NON OFFICIELLE

- MNEMONIC: société qui aide les entreprises et les organisations à gérer les risques de sécurité, à protéger leurs données et à se défendre contre les cyber-menaces

- Mnemonic.or : ONG qui aide les défenseurs des droits humains à utiliser efficacement la documentation numérique sur les violations des droits humains et les crimes internationaux

- Personaldata.io: ONG travaillant sur des questions liées à la protection des données

- R3D: ONG mexicaine travaillant à la promotion et à la protection des droits humains dans la sphère numérique

- SITU: division interdisciplinaire de recherche appliquée, qui étudie et traite les questions relatives aux droits humains sous l'angle de l'architecture (y compris l'établissement des faits et l'analyse spatiale)

- Storyful: agence de presse et de renseignement

- Tactical Tech: ONG qui collabore avec les citoyens et les organisations de la société civile afin d'étudier et d'atténuer l'impact de la technologie sur la société

- The Whistle: start-up universitaire, basée à l'université de Cambridge, qui développe des outils permettant de mettre en relation des témoins de violations des droits humains avec des organisations locales par l'intermédiaire d'une plateforme sécurisée

- TraceLabs: organisation à but non lucratif dont la mission est d'accélérer la réunion familiale des personnes disparues

- Videre est credere: ONG travaillant avec des activistes locaux pour les former et leur fournir la technologie nécessaire à la capture de preuves visuelles des violations des droits humains

- WITNESS: organisation à but non lucratif qui aide les personnes à utiliser les vidéos et la technologie pour protéger et défendre les droits humains

Outils

- Adarga.ai: plateforme d'intelligence artificielle qui utilise des processus technologiques d'analyse pour extraire rapidement des informations à partir de données non structurées et les présenter dans un format compréhensible

- ADS-B Exchange: source de données de vols aériens

- Archives.is: outil permettant de prendre des instantanés de pages web

- ARcGIS: base de données géographiques (propriétaire)

- AToM: application à code source ouvert pour la description et l'accès aux archives fondées sur les standards de l'ICA dans un environnement multilingue et multiréférentiel

- Blender: application libre pour la modélisation 3D, la mieux adaptée à la reconstruction numérique d'événements spatiaux, y compris la géolocalisation, la chrono-localisation et la reconstruction médico-légale

- BUSQUEMOS [en espagnol, pertinent pour le Mexique]: *chatbot* développé par l'ONG mexicaine Documenta, utilisé pour assurer la détection précoce des détentions arbitraires et la prévention des disparitions forcées

- Compass in the sky: un outil pour renforcer les compétences en matière de chrono-localisation

- Deepaware: outil permettant d'analyser des vidéos et des images et de détecter si elles ont été manipulées

- Descartes Labs: plateforme proposant des outils de géo-traitement

- DFace: application qui détecte et estompe les visages dans les images en ligne

TRADUCTION NON OFFICIELLE

- DevelopmentSeed Skynet: projet à code source ouvert sur l'imagerie satellite
- DigitalGlobe: outil (propriétaire) permettant d'accéder à l'imagerie satellitaire et aérienne
- Enigio Trace: outil (propriétaire) pour créer et gérer des documents originaux en ligne
- Exfitool: outil à code source ouvert pour la lecture, l'écriture et l'édition de métadonnées
- Eyewitness to atrocities: application de caméra mobile permettant d'enregistrer des photos et des vidéos intégrant les métadonnées nécessaires pour prouver leur authenticité devant un tribunal
- Google Earth: outil permettant d'accéder à l'imagerie satellitaire
- Hunch.ly: outil de capture web conçu pour les enquêtes en ligne
- I-Familia: base de données mondiale d'INTERPOL permettant d'identifier des personnes disparues sur la base de la comparaison internationale de l'ADN et des liens de familles
- Investigative dashboard: plateforme offrant divers outils pour retrouver des personnes, des entreprises et des actifs dans le monde entier
- InVid: plateforme offrant divers outils de vérification
- KoboToolbox: outil d'enquête pour téléphones mobiles qui permet de recueillir des témoignages, de géo-localiser des informations et de télécharger des informations vers des serveurs sécurisés
- Lookup-ID: outil pour trouver les identifiants Facebook
- Maltego: outil graphique permettant de découvrir et de cartographier les relations entre les entités d'intérêt - personnes, comptes en ligne et organisations
- Mapillary: application permettant d'accéder à des images au niveau de la rue et à des données cartographiques du monde entier
- MARTUS: outil gratuit et sécurisé de collecte et de gestion de l'information, à code source ouvert
- MAXAR: outil d'imagerie satellitaire (propriétaire)
- MediaConch: vérificateur de mise en œuvre et des politiques concernant des fichiers audiovisuels à code source ouvert
- Justice mobile: une application gratuite pour enregistrer les réunions et signaler les abus
- Mygeoposition.com: outil pour trouver la latitude et la longitude d'une localisation
- Neo4J: un système de gestion de base de données graphique, utile pour découvrir des modèles et des idées dans des ensembles de données complexes
- Nosomosexpedientes.mx [en espagnol, pour le Mexique]: outil numérique qui soutient les familles dans leurs recherches et dans la gestion de leurs dossiers auprès des autorités nationales
- Orbital Insights: un outil pour utiliser les données de localisation
- PeakVisor: outil 3D permettant d'identifier les montagnes et les sommets, utile pour la géolocalisation
- Planet: outil permettant d'accéder à l'imagerie satellitaire
- PhotoDNA: technologie développée pour détecter et supprimer les images d'exploitation d'enfants
- QGIS: base de données géo-spatiales à code source ouvert
- SCION: architecture Internet moderne qui vise à offrir une disponibilité élevée et une livraison efficace de paquets point à point, même en présence d'opérateurs et d'appareils de réseau activement malveillants

TRADUCTION NON OFFICIELLE

- Security in a Box: outils et tactiques de sécurité numérique
- Siegfried: outil d'identification de format de fichier basé sur la signature
- Skynet: plateforme de détection à la distance (propriétaire)
- SUNCALC: application permettant de déterminer la date et l'heure de la dernière apparition d'une personne disparue en fonction de la position du soleil et des ombres de la journée
- TC Slim app: application qui permet aux utilisateurs d'étudier la collection généralisée de données cachées dans une application mobile
- TerraServer: outil permettant d'accéder à l'imagerie satellitaire
- Timemap: logiciel de source ouverte pour visualiser les événements géo-spatiaux dans une plateforme interactive
- TinEye: outil de recherche d'images inversées
- Toddington international: ressources d'investigation de source ouverte et gratuite
- Truecaller: outil de traçage des numéros de téléphone
- TweetBeaver: offre plusieurs outils, notamment pour télécharger et rechercher dans la chronologie d'un utilisateur ou pour télécharger les favoris d'un utilisateur, sa liste d'amis ou de *followers*
- TwitterId: outil permettant de trouver les identifiants Twitter
- Uwazi: système de gestion de contenu qui permet de créer un site web public ou privé pour stocker des données destinées à différents usages, notamment les enquêtes criminelles, la défense des intérêts publics et la production d'informations statistiques pour la recherche
- vframe.io: outil offrant des technologies de pointe en matière de vision par ordinateur pour la recherche sur les droits humains et la surveillance des zones de conflit
- Wayback machine: outil de capture, de gestion et de recherche de collections de contenus numériques
- Webstagram: outil d'analyse et de suivi des comptes Instagram
- Wigle: outil de cartographie des réseaux wifi
- Wikimapia: outil qui consolide de multiples services d'imagerie satellitaire
- Wolfram Alpha: outil qui permet d'accéder et de comparer des informations sur la météo et autres
- Yandex Panoramas: outil collaboratif permettant de se localiser dans des espaces peu référencés
- Youtube-dl: programme permettant de télécharger des vidéos de YouTube et d'autres sites et plateformes vidéo
- Freedomlab est un lieu de rencontre virtuel pour les défenseurs des droits humains, qui contient un répertoire de matériel de formation, de tutoriels et d'outils numériques
- Une liste complète d'outils d'investigation en ligne est disponible dans la boîte à outils d'investigation en ligne de Bellingcat
- BBC Africa Eye / Forensics Dashboard offre également une liste complète d'outils, d'ensembles de données et d'autres ressources
- Il existe un nombre croissant d'outils permettant d'accéder à l'imagerie satellitaire et à la télédétection, notamment Google Earth Pro (l'outil "imagerie historique" est particulièrement utile); Bird.i; Sentinel Hub Playground; QGIS; Digital Globe; Imagehunter.

TRADUCTION NON OFFICIELLE

Institutions/programmes universitaires

- Center for Human Rights Science, Université Carnegie Mellon
- Forensic Architecture, agence de recherche basée à Goldsmiths, University of London
- Humanitarian Research Lab, Université de Yale
- Human Rights and Technology programme of the Human Rights Centre de l'université de Berkeley
- Human Rights, Big Data and Technology project de l'Université d'Essex
- The Citizen Lab, laboratoire interdisciplinaire basé à la Munk School of Global Affairs and Public Policy, Université de Toronto

Ressources

- Amnesty International a créé un corps de vérification numérique, c'est-à-dire un réseau de bénévoles formés pour vérifier les données et les informations obtenues par le biais d'enquêtes en sources ouvertes, et a publié un guide pour mener des enquêtes en ligne efficaces (parties I, II et III).
- Bellingcat a élaboré plusieurs "guides" accessibles au public, notamment : "*First steps to get 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.
- Protocole de Berkeley sur les enquêtes sur les sources numériques à code source ouvert, 2020: un guide pratique sur l'utilisation efficace des informations numériques ouvertes dans les enquêtes sur les violations du droit international pénal, des droits de l'homme et du droit humanitaire.
- How to interpret satellite image: five tips and strategies, par National Areonautics and Space Administration.
- Introductory Guide to Open Source Intelligence and Digital Verification par University of Essex Human Rights Centre Clinic.
- OSR4Rights propose un guide de la recherche libre en matière de droits humains ainsi que des tutoriels et des outils techniques (par exemple FaceSearch, Knowledge Hub Framework, Hate Speech Detection, et l'utilisation du traitement du langage naturel pour identifier les preuves les plus pertinentes).
- Le modèle de référence pour un système d'information archivistique ouvert contient des pratiques recommandées pour assurer la préservation à long terme de l'information numérique.
- Surveillance Self-Defence Guide (Guide d'autodéfense en matière de surveillance) par l'Electronic Frontier Foundation.
- Verification Handbook: guide de vérification des contenus numériques.
- Video as Evidence Field Guide by Witness pour aider les utilisateurs à filmer des vidéos pour documenter les violations des droits humains et poursuivre la justice.
- Voir également la liste non exhaustive des rapports publiés par les procédures spéciales des Nations unies concernant les nouvelles technologies.

TRADUCTION NON OFFICIELLE

Annexe II

Glossaire

Bot-net: réseau d'ordinateurs privés infectés par des *malware* et contrôlés en groupe à l'insu de leurs propriétaires, par exemple pour envoyer des *spam*.

Chrono-localisation : action de déterminer ou d'estimer l'heure ou le cadre temporel d'un événement ou d'une situation qui a été capturé par des médias visuels.

Data mining: processus de tri de grands ensembles de données afin d'identifier des modèles et des relations qui peuvent aider à résoudre des problèmes ou des questions grâce à l'analyse de données et à générer de nouvelles informations.

Détection à distance: balayage de la Terre par satellite ou par avion afin d'obtenir des informations sur celle-ci.

Doxxing: recherche et publication d'informations privées ou d'identification sur (une personne en particulier) sur l'internet, généralement dans une intention malveillante.

Ferme à trolls: organisation employant des personnes pour rédiger des messages en ligne délibérément offensants, provocateurs ou contenant souvent de fausses informations afin de provoquer des conflits ou de manipuler l'opinion publique.

Malware: logiciel spécifiquement conçu pour perturber, endommager ou obtenir un accès non autorisé à un système informatique.

Photogrammétrie: processus par lequel plusieurs photographies d'un environnement sont combinées pour créer, par triangulation, un modèle 3D.

Programme de reconnaissance faciale: technologie basée sur l'intelligence artificielle utilisée pour l'identification, la vérification ou la catégorisation de données biométriques.

Programme de reconnaissance de la démarche: programme basé sur un système qui utilise la forme du corps humain et la façon dont il bouge pour identifier une personne.

Radar à pénétration de sol: méthode géophysique qui utilise des impulsions radar pour obtenir des images du sous-sol.

Ransomware: logiciel conçu pour bloquer l'accès à un système informatique jusqu'à ce qu'une somme d'argent soit versée.

Régression cartographique: processus consistant à superposer des cartes historiques et des photographies aériennes à des images contemporaines afin de suivre l'évolution du territoire.

Spyware (logiciels espions), également appelés « logiciels d'intrusion », sont des logiciels malveillants qui permettent à un opérateur d'accéder à un appareil ciblé et d'en extraire, d'en modifier ou d'en partager le contenu.

TRADUCTION NON OFFICIELLE