**Consejo de Derechos Humanos**
**Quincuagésimo cuarto período**
11 de septiembre-6 de octubre de 2023
Punto 3 del Orden del día
**Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo.**

# Nuevas tecnologías y desapariciones forzadas

## Informe del Grupo de Trabajo sobre Desapariciones Forzadas o Involuntarias*

*Resumen*

En el presente informe, el Grupo de Trabajo sobre Desapariciones Forzadas o Involuntarias examina cómo se están utilizando las nuevas tecnologías contra los familiaresde personas desaparecidas, sus representantes y las personas defensoras de los derechos humanos; cómo pueden aplicarse eficazmente para facilitar la búsqueda de personas desaparecidas; y cómo pueden utilizarse para obtener y asegurar pruebas de la comisión de desapariciones forzadas.

El Grupo de Trabajo hace varias recomendaciones a los Estados, las empresas, las organizaciones de la sociedad civil, las instituciones nacionales de derechos humanos, las instituciones académicas, los donantes, los tribunales internacionales y otros mecanismosde derechos humanos y a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.



* El presente documento es una traducción no oficial de la versión en inglés y se publica sin revisión editorial.

# I. Introducción

1. Durante su 125ª sesión, el Grupo de Trabajo sobre Desapariciones Forzadas o Involuntarias anunció su intención de realizar un estudio temático sobre nuevas tecnologías y desaparición forzada.

2. Para recopilar la información pertinente, se celebraron reuniones de expertos el 9 de febrero y el 11 de mayo de 2022, durante los períodos de sesiones 126º y 127º del Grupo de Trabajo, respectivamente. El 17 de octubre de 2022, el Grupo de Trabajo distribuyó llamado a contribuciones escritas.[1] Hasta el 2 de agosto de 2023, se habían recibido 29 comunicaciones escritas de Estados (5); instituciones nacionales de derechos humanos (1); organizaciones de la sociedad civil, incluidas asociaciones de familiares de personas desaparecidas (16); y expertos o académicos (7).

3. A efectos del estudio, la expresión "nuevas tecnologías" se utiliza en sentido amplio, para referirse a las innovaciones tecnológicas ocurridas sobre todo en los últimos 20 años, incluidas las tecnologías de la información y la comunicación (TIC) de *hardware* y *software*, que abarcan las imágenes por satélite, la ciencia de la información geográfica y la teledetección, las redes sociales digitales y los conjuntos de datos en línea, el uso de la inteligencia artificial y el desarrollo del aprendizaje automático, así como la informática forense y los biodatos.

4. Las nuevas tecnologías, que hoy en día son, en su mayoría, fácilmente accesibles al público en general y rentables, tienen una relación ambivalente con las cuestiones relacionadas con los derechos humanos. Por un lado, los Gobiernos represivos, así como otros actores como las organizaciones criminales y los grupos armados, pueden utilizar las nuevas tecnologías contra, entre otros, las personas defensoras los derechos humanos y los familiares de personas desaparecidas para limitar el goce de sus derechos fundamentales, entre otras cosas mediante la vigilancia, la supervisión, la intrusión, las campañas de desinformación, el acoso en línea y los ciberataques. Otros actores interesados, como las corporaciones tecnológicas, también pueden desempeñar un papel crucial a través del desarrollo de hardware y software utilizados para obstaculizar la actividad de las personas defensoras de derechos humanos y familiares de personas desaparecidas. Por otro lado, las nuevas tecnologías son indispensables para documentar e investigar violaciones de derechos humanos, obtener y conservar pruebas y promover la rendición de cuentas, incluso en casos de desaparición forzada.

5. Este estudio analiza cómo se están utilizando las nuevas tecnologías contra los familiares de las personas desaparecidas, sus representantes, las personas defensoras de los derechos humanos y las organizaciones de la sociedad civil, y qué estrategias de protección se han puesto - o pueden ponerse - en marcha; cómo pueden aplicarse eficazmente para facilitar la búsqueda de personas desaparecidas, garantizando que su suerte y paradero se establezcan con prontitud y de manera fiable y segura; y cómo pueden utilizarse para obtener pruebas de la comisión de desapariciones forzadas, teniendo en cuenta que este crimen internacional está, por su propia naturaleza, envuelto en el secreto y, como tal, plantea obstáculos probatorios extraordinarios para identificar y llevar ante la justicia a los autores.

6. El estudio se complementa con anexos, que contienen un glosario; un mapeo no exhaustivo de herramientas, contactos y recursos disponibles públicamente que pueden ayudar a poner en marcha estrategias de protección frente a amenazas online, facilitar la búsqueda de personas desaparecidas y las correspondientes investigaciones criminales. El Grupo de Trabajo también pretende desarrollar en un futuro próximo el estudio de casos hipotéticos que ilustren paso a paso el proceso para investigar una desaparición forzada mediante el uso de las nuevas tecnologías, con el objetivo de mostrar las implicaciones, tanto en términos de ventajas como de obstáculos existentes.

[1] El llamado a contribuciones y las contribuciones recibidas (excluidas aquéllas para las que se solicitó confidencialidad) están disponibles en https://www.ohchr.org/es/calls-for-input/2023/call-inputs-thematic-study-working-group-enforced-or-involuntary.

7. Especialmente en lo que concierne a la búsqueda de las personas desaparecidas y a la documentación del crimen y la promoción de la rendición de cuentas, las nuevas tecnologías ofrecen soluciones rentables que pueden tener un impacto significativo. Sin embargo, por sí solas son incapaces de resolver todos los problemas existentes y, por lo tanto, no deben abandonarse los enfoques y técnicas tradicionales de documentación, seguimiento e información, ni pueden sustituirse totalmente por material digital y nuevas tecnologías. Por el contrario, se debe buscar y fomentar la complementariedad entre ambas estrategias.

# II. Uso de las nuevas tecnologías para facilitar u ocultar la comisión de desapariciones forzadas o como medio de represalia o intimidación

8. La experiencia del Grupo de Trabajo y las contribuciones recibidas muestran que las nuevas tecnologías, y en particular las TIC se utilizan con frecuencia para facilitar u ocultar la comisión de desapariciones forzadas, para obstaculizar la labor de las personas defensoras de los derechos humanos y los familiares de personas desaparecidas, así como para intimidarlos u hostigarlos. En ocasiones, la legislación relacionada con la tecnología (especialmente con el uso de las redes sociales y el ciber-crimen) se utiliza como pretexto para los mismos fines y para perseguir a las personas defensoras de derechos humanos y familiares de personas desaparecidas que emplean estos medios para denunciar desapariciones forzadas o denunciar abusos.

9. El Grupo de Trabajo recibió información sobre desapariciones forzadas perpetradas en los casos en que el Estado había interrumpido el acceso a Internet y a los datos móviles, ya fuera mediante intervenciones generales o enfoques más acotados, como la limitación del ancho de banda y el bloqueo de determinadas plataformas de medios de comunicación.[2] A pesar de la falta de un estudio exhaustivo que analice la correlación entre los cierres o restricciones de Internet y las interrupciones del acceso a los datos móviles con el aumento del número de desapariciones forzadas, la información recibida por el Grupo de Trabajo parece indicar que la limitación del acceso a Internet - o su interrupción completa - han sido instrumental para ocultar graves violaciones de los derechos humanos, incluida la desaparición forzada.

10. Las restricciones al acceso a Internet repercuten en el goce de diversos derechos humanos y sólo se permitirán en circunstancias específicas y con las debidas garantías.[3] A menudo, una vez restablecida la conectividad a Internet, incluido el uso de plataformas de medios de comunicación, el Grupo de Trabajo recibe denuncias de desapariciones forzadas u hostigamiento contra personas defensoras de los derechos humanos y familiares de personas desaparecidas perpetrados durante el periodo de interrupción. En estos casos, los cortes o interrupciones similares impiden concretamente el monitoreo del respeto de los derechos humanos así como la documentación y denuncia rápida de los crímenes en cuestión y obstaculizan las investigaciones y las actividades de búsqueda, poniendo en peligro en última instancia el derecho a conocer la verdad y favoreciendo la impunidad.

11. El Grupo de Trabajo recibió un número cada vez mayor de comunicaciones en las que se hacía referencia a desapariciones forzadas presuntamente perpetradas para "silenciar" a alguien activo en las redes sociales, por ejemplo personas que habían denunciado abusos perpetrados por el Estado, conmemorado acontecimientos o personas que pertenecen a minorías. Entre las personas sometidas a desaparición forzada en estas circunstancias figuran personas defensoras de los derechos humanos, periodistas, blogueros, *youtubers*, activistas, opositores políticos y líderes religiosos.[4]

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

12. Una práctica detectada por el Grupo de Trabajo que parece constituir un modus operandi común a las fuerzas de seguridad de todo el mundo es la de confiscar todos los dispositivos electrónicos de las personas que posteriormente son sometidas a desaparición forzada y, con frecuencia, de los familiares o de cualquier otra persona presente en el momento de la privación de libertad. También son recurrentes los casos en los que las fuerzas de seguridad destruyen los dispositivos electrónicos de potenciales testigos presenciales de una desaparición forzada, supuestamente para borrar todas las pruebas del delito.

13. En relación con las circunstancias descritas en los párrafos anteriores, el Grupo de Trabajo registró un número creciente de casos en los que personas defensoras de los derechos humanos, incluidos familiares de personas desaparecidas, han sido acusados y procesados en virtud de la legislación nacional sobre ciberseguridad. Estos ejemplos incluyen casos en los que las personas afectadas habían publicado información sobre desapariciones forzadas en sus cuentas y redes sociales o criticado al Gobierno por su presunta implicación o por la impunidad en casos de desapariciones forzadas.[5] En otros casos, se utilizaron cuentas falsas para acusar posteriormente a la persona concernida de difundir odio o información falsa, o de poner en peligro la seguridad nacional.[6]

14. Además, los mecanismos internacionales de derechos humanos han tenido conocimiento de casos en los que el uso -o incluso la mera descarga- de una aplicación específica (como, por ejemplo, la aplicación de mensajería ByLock) fue considerada por las autoridades nacionales como la única prueba decisiva para justificar detenciones masivas de personas defensoras de los derechos humanos y opositores políticos, que en algunos casos condujeron a su posterior desaparición forzada o muerte bajo custodia.[7] Estos casos son especialmente problemáticos debido, entre otras cosas, a la falta de claridad sobre los fundamentos jurídicos invocados. Otro motivo de preocupación se refiere a las tecnologías y técnicas utilizadas por las autoridades nacionales para acceder a los servidores, obtener las direcciones IP y el contenido de los intercambios entre usuarios, lo que podría abarcar la piratería informática y la infiltración y robo de los datos de los servidores. Por ejemplo, en el caso de ByLock, el servidor estaba situado en un Estado distinto de aquel en el que se llevaron a cabo las detenciones y los juicios.[8]

15. Según la información recibida por el Grupo de Trabajo, las redes sociales también se han utilizado para llevar a cabo campañas de difamación y amenazar a personas defensoras de los derechos humanos, incluidos los familiares de personas desaparecidas. Los ataques denunciados en las redes sociales contra familiares de personas desaparecidas a menudo se han caracterizado por los estereotipos de género y la discriminación,[9] y se han utilizado herramientas digitales (como "granjas de trolls", botnets y cuentas falsas) para llevar a cabo campañas de difamación o desinformación, estigmatizar a las personas desaparecidas o asus familias y permitir el acoso en línea, incluido el acoso sexual, y la incitación al odio.

16. Los casos de ciberataques contra personas defensoras de los derechos humanos, incluidos familiares de personas desaparecidas, abarcan sabotaje mediante *phishing*, *malware* y *ransomware*, espionaje y suministro de desinformación, así como fugas de noticias 'contaminadas' llamadas *tainted leaks en inglés*) y el *doxxing*. A menudo, las personas contra las que se dirige el ataque son descritas o etiquetadas maliciosamente como espías, agentes extranjeros, terroristas o contrabandistas, lo que, a su vez, expone sus cuentas a una vigilancia especial, a la suspensión o a campañas de odio, en un escenario que se caracteriza por la falta de denuncias y por las lagunas políticas y jurídicas, así como por las dificultades para hacer rendir cuentas a los responsables, entre otras cosas debido a la competencia de diferentes jurisdicciones.[10] El Grupo de Trabajo tuvo

[5] EGY 7/2018; NIC 3/2020; NIC 6/2022; ZMB 1/2021.
[6] BGD 1/2022.
[7] Tribunal Europeo de Derechos Humanos (TEDH), Caso Akgün c. Türkiye, sentencia de 20 de julio de 2021; y Comité de Derechos Humanos, Caso Açikkollu c. Türkiye, Comunicación nº 3730/2020, dictamen de 25 de octubre de 2022.
[8] Grupo de Trabajo sobre la Detención Arbitraria, Opinión núm. 42/2018 de 21 de agosto de 2018, párr. 33.
[9] A/HRC/50/25 y A/HRC/38/47.
[10] Los intentos de superar algunos de los obstáculos mencionados, dentro del Consejo de Europa, son el Convenio sobre la Ciberdelincuencia de 2001 y el Segundo Protocolo Adicional al Convenio sobre la

conocimiento con preocupación de un caso en el que una defensora de los derechos humanos que investigaba una desaparición forzada fue contactada a través de sus redes sociales por alguien que utilizaba una identidad falsa, quien aprovechó estos intercambios para enviarle enlaces a archivos que contenían un malware, comprometiendo así la seguridad y perjudicando la privacidad de sus datos.[11]

17. Además, el Grupo de Trabajo ha sido informado de que los sitios web creados por familiares de personas desaparecidas o sus asociaciones, ya sea para honrar y preservar la memoria de sus seres queridos o sobre la cuestión de la desaparición forzada en general,han sido objeto de ataques cibernéticos, que equivalen a injerencias graves e injustificadas, una forma de revictimización y violaciones de la dignidad y la reputación de las personas desaparecidas y sus familiares. Según el conocimiento del Grupo de Trabajo, estos ataques e injerencias – que pueden ser llevados a cabo por actores privados contratados por el Estado y actores no estatales[12] – rara vez son objeto de investigaciones exhaustivas y eficaces y permanecen impunes, facilitando así la repetición de delitos similares.

18. El Grupo de Trabajo tuvo conocimiento de casos igualmente recurrentes en los que las tecnologías, especialmente las TIC, fueron utilizadas para espiar a familiares de personas desaparecidas, a sus representantes o asociaciones y a personas defensoras de derechos humanos. Un hecho especialmente preocupante es el del uso nacional o transnacional de programas espía, como Candiru, Pegasus o Predator, para vigilar maliciosamente las actividades de, entre otros, personas defensoras de los derechos humanos, periodistas, activistas y abogados, incluso determinando su ubicación, accediendo a listas de contactos para descubrir a otras personas, colocando pruebas incriminatorias y chantajeando a las personas afectadas con información personal.[13] Los programas espía se han utilizado para vigilar a familiares de personas desaparecidas, entre ellas, por ejemplo, la esposa y la prometida de Jamal Khashoggi,[14] o la hija del Sr. Paul Rusesabagina,[15] o personas defensoras de los derechos humanos implicadas en el apoyo a familiares de personas desaparecidas;[16] o los miembros de una comisión independiente encargada de investigar la desaparición forzada de 43 estudiantes en Ayotzinapa, México.[17] La omnipresencia de los programas espía tiene un efecto amedrentador sobre las organizaciones de la sociedad civil y las personas defensoras de los derechos humanos, incluidos los familiares de personas desaparecidas.[18]

19. Los familiares de personas desaparecidas suelen vivir con miedo a las represalias, loque a menudo les impide denunciar los abusos, incluso a través del procedimiento humanitario del Grupo de Trabajo. Los programas espía aumentan el riesgo al permitir el acceso sin restricciones a sus dispositivos y datos. La información obtenida a través de programas espía puede utilizarse para cometer nuevos abusos contra familiares de personas desaparecidas, chantajearlos para que guarden silencio o causarles más daño. Los datos obtenidos mediante programas espía también pueden ayudar a localizar a personas para posteriormente someterlas a desapariciones forzadas.

20. Los programas espía pueden ser adquiridos por los Gobiernos, sobre todo en un contextoque, en general, carece de supervisión independiente y de regulación suficiente, especialmente en lo

Ciberdelincuencia de 2022 relativo a la cooperación reforzada y la divulgación de pruebas electrónicas (aún no en vigor).

[11] Amnistía Internacional, Pakistán, los defensores de los derechos humanos son víctimas de una campaña de ciberataques y vigilancia, 15 de mayo de 2018.

[12] Sobre la posible implicación de mercenarios (que incluyen entidades empresariales, grupos de amenaza persistente avanzada, ciber-milicias, individuos y ciber-delincuentes) en ciberataques, véase A/76/151.

[13] Alto Comisionado de las Naciones Unidas para los Derechos Humanos, Declaración sobre el uso de programas espía para vigilar a periodistas y personas defensoras de los derechos humanos, 19 de julio de 2021; y www.oas.org/en/iachr/jsForm/?File=/en/iachr/mediacenter/preleases/2022/022.asp. Sobre la vigilancia digital de periodistas, véase A/HRC/50/29. También A/HRC/52/39, párrs. 44-50.

[14] A/HRC/4/CRP.1, párrs. 68-71.

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

[16] Véase 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 NSOSpyware, 2017.

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

que respecta a la importación, exportación y uso de este tipo de tecnología. El Grupo de Trabajo se enteró con interés de la legislación aplicable de algunos Estados y de los reglamentos regionales y acuerdos internacionales existentes[19] que tienen por objeto someter la venta y transferencia de tecnologías a un control más estricto. Aunque se trata de buenas prácticas, el marco jurídico aplicable sigue siendo débil y fragmentario, y un examen exhaustivo e independiente del impacto de estas tecnologías sobre los derechos humanos debería convertirse en la norma antes de su venta, transferencia y uso.[20]

21. Los casos en los que se ha enjuiciado y sancionado a los responsables -ya sean Estados, empresas o particulares- por el uso indebido de tecnologías de vigilancia o de abusos en su venta y transferencia son extremadamente escasos.[21] Hasta que se aborden las lagunas normativas de forma exhaustiva y las empresas cumplan plenamente las obligaciones que les impone el derecho internacional, tal y como se establece en los Principios Rectores sobre las Empresas y los Derechos Humanos, debería aplicarse una moratoria sobre la venta, transferencia y uso de programas espía.[22]

22. El Grupo de Trabajo también observó con preocupación la proliferación incontrolada de programas de vigilancia masiva, reconocimiento facial y otros similares.[23] Por naturaleza, estos sistemas someten a un número significativo de personas a una vigilancia indiscriminada, interfiriendo sistemáticamente en el goce de sus derechos humanos. El tratamiento de datos biométricos, imágenes e información recopilada a través de estos medios por videocámaras en espacios públicos se ha utilizado para señalar a determinadas personas, incluso en el contexto de protestas sociales,[24] que posteriormente han sido detenidas y, en algunos casos, sometidas a desaparición forzada. Los sistemas de datos centralizados operados a través de aplicaciones móvilesutilizadas por funcionarios gubernamentales se han utilizado presuntamente para llevar a cabo operaciones similares de vigilancia masiva, que han conducido a la selección de determinadas personas consideradas "sospechosas" (incluidas personas defensoras de los derechos humanos y personas pertenecientes a minorías étnicas o religiosas) y a su posterior desaparición forzada.

23. Según la información recibida por el Grupo de Trabajo, las tecnologías de vigilancia mencionadas, así como las soluciones de inteligencia artificial, los drones, los sensores de imágenes térmicas, las gafas de visión nocturna, los sistemas de identificación biométrica, las torres de vigilancia aérea y los sensores especializados para detectar emisiones de teléfonos móviles y dispositivos de rastreo, han sido utilizados cada vez más en las fronteras por los Estados y las agencias regionales para automatizar los procesos de identificación y seguimiento de los

[19] Véase el Arrangment de Wassenaar de 1995 sobre el control de las exportaciones de armas convencionales y de bienes y tecnologías de doble uso, modificado en 2013; y el Reglamento (UE) nº 2021/821, de 20 de mayo de 2021, por el que se establece un régimen de control de las exportaciones, el brokering, la asistencia técnica, el tránsito y la transferencia de productos de doble uso. Véase también Japan Foreign Exchange and Foreign Trade Act No. 228 of 1949, modificado en 2005; y Draft U.S. Government Guidance for the Export of Surveillance Technology, Bureau of Democracy, Human Rights, and Labor, U.S. Department of State, 4 de septiembre de 2019. Para un borrador sobre los compromisos de los Estados en materia de comercio internacional de programas espía, véase A/HRC/52/39, anexo.

[20] Una iniciativa en este sentido, denominada "Export Controls and Human Rights Initiative", se puso en marcha el 10 de diciembre de 2021 por Australia, Dinamarca, Noruega y los Estados Unidos de América.

[21] Excepciones notables son la de la Sala del Tribunal de Apelación de París que, en noviembre de 2022, confirmó la inculpación de una empresa de vigilancia y sus ejecutivos, debido a que la venta de software de vigilancia a regímenes autoritarios provocó, entre otras cosas, la desaparición de disidentes; así como la decisión emitida el 9 de enero de 2023 por el Tribunal Supremo de Estados Unidos que permitió que continuara el procedimiento contra el Grupo NSO basado en una demanda presentada por WhatsApp. Ver https://www.fidh.org/en/impacts/Surveillance-torture-Libya-Paris-Court-Appeal-indictment-AMESYS; y https://dockets.justia.com/docket/california/candce/3:2019cv07123/350613.

[22] Escándalo del software espía: Expertos de la ONU piden una moratoria en la venta de tecnología de vigilancia "potencialmente mortal", 2021.

[23] Sobre los desafíos únicos relativos al uso de datos personales y no personales en el contexto de la inteligencia artificial, véase A/HRC/46/37; y sobre el análisis de big data y las técnicas computacionales basadas en la inteligencia artificial, véase A/73/438. Véanse también A/HRC/37/62 sobre la vigilancia y el derecho a la intimidad; A/HRC/41/43 sobre el impacto desproporcionado de la inteligencia artificial y la automatización en las mujeres; A/HRC/41/35 sobre las tecnologías de vigilancia privada y los derechos humanos; A/74/159 sobre las investigaciones de las tecnologías digitales utilizadas para la vigilancia; y A/HRC/34/60 sobre las actividades gubernamentales de vigilancia.

[24] A/HRC/44/24.

movimientos de los migrantes, refugiados y solicitantes de asilo, incluso en operaciones de devolución, lo que conduce -o en algunos casos equivale- a desapariciones forzadas.[25] El Grupo de Trabajo también tuvo conocimiento de que no se utilizaron los datos recopilados mediante dichas tecnologías con los equipos de búsqueda y rescate y las autoridades, con lo que no se evitó que los migrantes en peligro desaparecieran omurieran. El Grupo de Trabajo expresa su profunda preocupación por este uso despiadado de las nuevas tecnologías y señala que el marco jurídico internacional aplicable, especialmente en lo que respecta al uso de la inteligencia artificial, es deficiente y debe reforzarse urgentemente.[26]

24. También se han producido ciberataques contra bases de datos que contieneninformación sensible sobre personas desaparecidas y sus familiares. Por ejemplo, el 18 de enero de 2022, se accedió a datos personales y otra información confidencial relativa a más de 515.000 personas de todo el mundo, almacenados en los sistemas de la Agencia Central de Búsqueda del Comité Internacional de la Cruz Roja.[27] Entre otras, se vieron comprometidas plataformas que contenían datos sobre personas desaparecidas, así como sobre sus familiares (entre ellas, la aplicación y el sitio web "Family Links Answers" y la plataforma "Trace the Face"). La investigación sobre el ataque demostró que se trataba de uno muy sofisticado, realizado con el objetivo de extraer datos.

25. Casos como el aquí descrito confirman la urgente necesidad de desarrollar medios más seguros que puedan garantizar el uso exclusivamente humanitario de los datos[28] y canales seguros de comunicación para las personas defensoras de los derechos humanos, las organizaciones de la sociedad civil, los actores humanitarios, los organismos de derechos humanos y los familiares de las personas desaparecidas.[29] Mientras tanto, el uso de aplicaciones gratuitas disponibles que permitan la recopilación, el almacenamiento y el análisis de datos de forma segura es una primera medida de mitigación que debe adoptarse.[30] El desarrollo de herramientas de código abierto y de fácil acceso para realizar análisis forenses fiables de dispositivos que puedan haber sido comprometidos también se ha mencionado como una acción relevante para mitigar algunos de los riesgos descritos en esta sección.[31] Además, muchas de las contribuciones recibidas por el Grupo de Trabajo hicieron hincapié en la importancia de proporcionar una formación adecuada a los miembros de las organizaciones de la sociedad civil y a los familiares de las personas desaparecidas para aumentar su concienciación sobre los riesgos relacionados con las nuevas tecnologías y mitigarlos,incluso mediante la difusión de información sobre higiene digital, sensibilidad de los datos, daños y minimización. Estos programas deberían permitir a las organizaciones de la sociedad civil integrar métodos de seguridad en su trabajo y adquirir capacidad interna para diagnosticar los riesgos existentes y recuperarse de amenazas o ataques.

# III. Uso de las nuevas tecnologías para facilitar la búsqueda de personas desaparecidas

26. Las innovaciones tecnológicas han demostrado ser cruciales para documentar y alertar sobre la perpetración de graves violaciones de los derechos humanos. Los datos recopilados con fines de

[25] A/HRC/36/39/Add.2 y A/HRC/47/30. Comité contra la Desaparición Forzada, proyecto de observación general sobre las desapariciones forzadas en el contexto de la migración, marzo de 2023, párr. 22, 33 y 44 y nota 21.

[26] Se están realizando esfuerzos a nivel de la UE para adoptar una Ley de Inteligencia Artificial.

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

[28] Por ejemplo, el protocolo conocido como SCION desarrollado en la Politécnica de Zúrich.

[29] Para hacer frente a algunos de estos retos, el CICR está abriendo una delegación para el ciberespacio. La Agencia Central de Búsquedas también cuenta con un programa de digitalización, en el marco del cual se han puesto en marcha un Programa de Comparación Digital de Personas Desaparecidas y un proyecto Integrado de Búsquedas en Línea y Precasos. Más en general, véase el número de la Revista del CICR (2021) sobre tecnologías digitales y guerra.

[30] Para conocer algunas de estas aplicaciones, véase el anexo I.

[31] Entre otros, Amnistía Internacional, Informe de metodología forense: Cómo atrapar al Pegaso del Grupo NSO, 2021.

búsqueda de los desaparecidos pueden ser esenciales también en el contexto de las investigaciones penales, aunque este aspecto se examina más a fondo en la sección IV. Como se establece en el Principio 13 de los Principios Rectores para la Búsqueda de Personas Desaparecidas de 2019, la búsqueda de la persona desaparecida y la investigación penal de los responsables del delito deben estar vinculadas y reforzarse mutuamente.[32]

27. Una de las comunicaciones recibidas por el Grupo de Trabajo subrayaba que, al día de hoy, la mayoría de las tecnologías utilizadas para la búsqueda de personas desaparecidas y las investigaciones correspondientes se basan en una comprensión y clasificación binarias del género que ignoran las experiencias y expresiones no normativas. Los datos recopilados y procesados de forma irreflexiva, y carentes de una comprensión más amplia de losespectros sexo-género, ignoran sistemas sociales y culturales cruciales y obstaculizan las actividades de búsqueda y las investigaciones. Un enfoque integrado del procesamiento de la información debería incorporar la búsqueda exhaustiva de detalles sobre la persona (pre/peri/post desaparición) con una lente de género y el uso de esta información a lo largo de todo el proceso. El Grupo de Trabajo considera que esto se tendrá en cuenta a la hora de diseñar herramientas y tecnologías de recopilación de datos para la búsqueda de personas desaparecidas y las investigaciones.[33]

28. Se ha puesto en consideración del Grupo de Trabajo que algunas de las tecnologías mencionadas en la sección anterior – *spyware* (programas espía) , programas de vigilancia y reconocimiento facial, y tecnologías actualmente empleadas en las fronteras para el control migratorio - que han sido utilizadas contra personas defensoras de derechos humanos y familiares de personas desaparecidas, siendo incluso instrumentales para la perpetración de desapariciones forzadas, podrían ser aplicadas a la inversa para facilitar la búsqueda de personas desaparecidas y la identificación de perpetradores. El Grupo de Trabajo observa que, en efecto, podría merecer la pena explorar este aspecto de dichas tecnologías, teniendo en cuenta que siempre deberán utilizarse garantizando el respeto de los derechos humanos fundamentales y que, en este ámbito, podrían reevaluarse los criterios y requisitos para que las empresas concedan acceso a los datos, tanto al personal encargado de hacer cumplir la ley como a terceros.

29. El uso de inteligencia de código abierto, que se basa en la tecnología para recopilar y analizar datos que están a disposición del público (por ejemplo, en las redes sociales, imágenes de satélite o herramientas cartográficas), puede desempeñar un papel crucial tanto en la búsqueda de personas desaparecidas como en la identificación y obtención de pruebas que permitan identificar a los autores del delito. Por lo tanto, se mencionará tanto en esta sección del estudio como en la siguiente. Para un análisis más exhaustivo de todos los aspectos pertinentes, una referencia esencial es el Protocolo de Berkeley de 2020 para investigaciones de código abierto de archivos digitales ("el Protocolo de Berkeley"), que contiene una guía práctica sobre el uso eficaz de la información digital de código abierto en la investigación de violaciones del derecho penal internacional, de los derechos humanos y del derecho humanitario.[34] El Grupo de Trabajo considera que el Protocolo de Berkeley debe ser tenido en cuenta por todas las partes implicadas en la búsqueda de personas desaparecidas y en la investigación de desapariciones forzadas.

30. En cuanto a las tecnologías más utilizadas para la búsqueda de personas desaparecidas, el Grupo de Trabajo observa que muchas de ellas han sido concebidas y se utilizan esencialmente para la búsqueda de restos mortales. Aunque el Grupo de Trabajo reconoce la importancia de estas técnicas, y en los párrafos siguientes analiza algunos logros notables al respecto, conviene recordar que la búsqueda debe realizarse bajo la presunción de que la persona desaparecida está viva.[35] El Grupo de Trabajo considera que deberían dedicarse más esfuerzos y recursos -técnicos, financieros y humanos- al desarrollo de tecnologías que se centran en las primeras etapas de la desaparición forzada y en la búsqueda proactiva de la persona desaparecida con vida, incluso

[32] A/HRC/45/13/Add.3, párr. 56.
[33] Esto se aplica al análisis de datos semánticos, temáticos y de contenido, a los esfuerzos de localización con el uso de drones, a las tecnologías de reconocimiento de patrones, a las tecnologías de reconstrucción facial forense y a los procesos de visualización digital.
[34] www.ohchr.org/sites/default/files/2022-04/OHCHR_BerkeleyProtocol.pdf.
[35] Véase el Principio 1 de los Principios Rectores para la Búsqueda de Personas Desaparecidas de 2019.

mediante el rastreo temprano de las huellas digitales de las personas desaparecidas. Teniendo en cuenta esta aclaración, un tema que ya se ha analizado a profundidad y que es relevante también para la búsqueda de personas desaparecidas es cómo las nuevas tecnologías – y en particular las tecnologías digitales – pueden contribuir al descubrimiento y la gestión de fosas comunes.[36]

31. Una tecnología que ya se utiliza desde hace algunos años es la conocida como Light Detection and Ranging (LiDAR), que es un método de detección a distancia utilizado para examinar la superficie de la Tierra. En el pasado, en las operaciones de búsqueda de personas desaparecidas, se ha utilizado sobre todo para realizar mapeos y localizar lugares de entierro y fosas comunes.[37] Los avances en las capacidades de mapeo del LiDAR hace que resulte útil también para las operaciones de búsqueda y rescate, ya que puede ayudar a identificar una forma humana en cualquier terreno y a detectar la forma más eficaz de llegar hasta la persona en cuestión. Las unidades LiDAR se colocan en drones o pequeños aviones y sobrevuelan las zonas que se van a mapear.[38]

32. Durante su visita a Uruguay, el Grupo de Trabajo tuvo conocimiento de que la institución encargada de la búsqueda de personas desaparecidas tardó meses en conseguir una unidad LiDAR, que finalmente pidió prestada a Argentina. Una vez obtenida, se encontraron una serie de obstáculos burocráticos antes de que pudiera ser utilizada. Más tarde se supo que en Uruguay existían unidades LiDAR y que el ejército (que es su propietario) podría haberlas puesto a disposición en una fase mucho más temprana, facilitando así las operaciones de búsqueda y su eficacia.[39] Este ejemplo sugiere que las instituciones encargadas de la búsqueda de personas desaparecidas en cualquier país deberían disponer de esta tecnología y que deberían existir normas adecuadas para evitar trabas indebidas a su uso. Consideraciones similares se aplican al uso de escáneres de sonido, navegación y alcance (conocidos como SONAR), drones y radares de penetración terrestre.

33. Además de las imágenes aéreas, las imágenes por satélite con una resolución espacial significativa son hoy accesibles también más allá de los Gobiernos y pueden facilitar la búsqueda de personas desaparecidas. Por ejemplo, se han utilizado para documentar el establecimiento de lugares de detención oficiales o secretos, localizar sitios de tortura[40] e identificar fosas comunes o lugares de enterramiento.[41] El paso del tiempo puede plantear obstáculos al uso de esta tecnología en la búsqueda de personas desaparecidas, pero el empleo de herramientas de búsqueda inversa de imágenes, fotogrametría y regresióncartográfica puede mitigar algunos de los retos existentes.

34. El Grupo de Trabajo tuvo conocimiento del uso del análisis geoespacial, en combinación con la estadística espacial y la detección a distancia para identificar posibles zonas de búsqueda de fosas comunes en Baja California, México.[42] Los investigadores utilizaron la agrupación espacial y el espacio clandestino y los integraron en un modelo espacial dentro de una aplicación web, con

[36] A/75/384.

[37] Véase www.coloniadignidad.cl/actualidad/noticias/la-tecnologia-lidar-en-la-busqueda-de-personas-detenidas-desaparecidas-en-las-últimas-dictaduras-de-argentina-y-chile/. Véase también Corcoran A., Mundorff A.Z., White D.A. y 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] Lo utiliza, por ejemplo, Frontex durante sus operaciones, véase la presentación en PowerPoint (europa.eu). Véase también capacidades basadas en la inteligencia artificial para la Guardia Europea de Fronteras y Costas (europa.eu) más en general para las capacidades de inteligencia artificial de Frontex.

[39] A/HRC/54/22/Add.1, párr. 21.

[40] Amnistía Internacional, Cameroon's Secret Torture Chambers, 2017; y Humanitarian Research Lab, Extrajudicial Detentions and Enforced Disappearances in Kherson Oblast, 2022.

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

[42] La técnica empleada se basó en la consideración de la distribución espacial de las fosas ocultas, la visibilidad espacial y la accesibilidad de zonas específicas, y la acumulación de nitrógeno identificada mediante imágenes de satélite. Para una reconstrucción completa, véase Finding clandestine graves: using geospatial analysis to search for missing persons in Baja California, Mexico - Citizen Evidence Lab - Amnesty International; y Silván-Cárdenas J., Alegre-Mondragón A., Ruiz-Reyes J., 'Geospatial Analysis of Clandestine Graves in Baja California: Nuevos enfoques para la búsqueda de personas desaparecidas en México', en Tapia- McClung R., Sánchez-Siordia O., González-Zuccolotto K., Carlos-Martínez H. (eds.), Advances in Geospatial Data Science, Springer, 2022, pp. 29-40.

el objetivo de filtrar la zonas con mayor probabilidad de encontrar más fosas clandestinas, basándose en la información original de 52 fosas localizadas por el Fiscal General. Esto condujo a una reducción sustancial (<10%) de las áreas de búsqueda, produciendo un modelo que garantiza que las áreas de búsqueda se encuentren a distancias prácticas de los asentamientos urbanos. Esta metodología arrojó resultados alentadores y merece la pena seguir estudiándola y analizándola.

35. Las tecnologías son cruciales también en lo que respecta a las ciencias forenses y han demostrado ser decisivas para determinar la suerte y el paradero de las personas desaparecidas, en particular mediante el uso de datos biométricos y la creación de bases de datos genéticos.[43] La interoperabilidad de dichas bases de datos sigue siendo un reto, tanto dentro de los Estados (especialmente los federales) como a escala internacional. El Grupode Trabajo tuvo conocimiento de la existencia de bases de datos globales[44] destinadas al cotejo de parentesco por ADN y considera que estos esfuerzos deben continuar. Según la información recibida, la bioinformática forense desempeña un papel cada vez más importante en la verificación de los análisis de ADN, contribuyendo así a la realización del derecho a conocer la verdad.

36. La cuestión de la seguridad en la recopilación y el intercambio de datos -fundamental para facilitar la búsqueda de personas desaparecidas- está resultando especialmente difícil en los casos relacionados con personas migrantes. Por un lado, existe una reticencia generalizada a compartir datos sobre las personas desaparecidas, por temor a que, en ausencia de una protección adecuada, la información recopilada pueda utilizarse contra las personas afectadas o sus familias. Por otro lado, puede haber varias bases de datos, a menudo ubicadas en distintos países, que contengan información relevante, pero que no ofrezcan interoperatividad, entre otros porque no siguen criterios armonizados en cuanto a los datos recogidos, lo que acaba frustrando los intentos de búsqueda. Problemas similares surgen cuando los restos mortales que pueden pertenecer a una persona desaparecida se encuentran en un Estado, pero las bases de datos que contienen los datos genéticos necesarios para realizar una identificación fiable están dispersas por distintos países.

37. En este ámbito, se necesitan recursos técnicos, financieros y humanos adicionales, con vistas, entre otras cosas, a desarrollar tecnologías que permitan superar estos obstáculos de forma segura.[45] Las iniciativas dirigidas a mejorar la identificación biométrica y genética entre fuerzas de seguridad, especialmente en las fronteras, deben guiarse por este espíritu, teniendo en cuenta que las supuestas consideraciones de seguridad no pueden prevalecer sobre la garantía de los derechos humanos fundamentales, incluido el derecho a conocer la verdaden relación con posibles desapariciones forzadas.

38. El Grupo de Trabajo recibió información sobre casos en los que, a través de grabaciones de los circuitos cerrados de televisión (CCTV) del lugar donde supuestamente se llevaron a la persona desaparecida, los familiares o sus representantes rastrearon la matrícula del vehículo utilizado y su itinerario posterior. Cruzando esta información con los registros de llamadas y los datos del móvil de la persona desaparecida, recopilaron indicios relevantes sobre el posible paradero de la persona. En algunos casos, se obtuvo información similar a través de contenidos generados por los usuarios (por ejemplo, fotos o vídeos subidos a las redes sociales). Estos pasos se han dejado a menudo a la iniciativa de los familiares de las personas desaparecidas, sus representantes u otros miembros de la sociedad civil, exponiéndolos con frecuencia a riesgos, mientras que las autoridades no parecen haber desarrollado una práctica sistemática.

39. Los familiares de personas desaparecidas utilizan con frecuencia las redes sociales o las aplicaciones de mensajería para buscar proactivamente a sus seres queridos.[46] Si bien esto puede

[43] Equipo Argentino de Antropología Forense, Guía forense para la investigación, recuperación de restos óseos humanos, 2020.

[44] I-Familia, gestionada por INTERPOL.

[45] CICR, Core Dataset for the Search for Missing Migrants, 2021; y Laczko F., Singleton A., Black J. (eds.), Fatal Journeys Vol. 3: Improving Data on Missing Migrants, Organización Internacional para las Migraciones, 2017

[46] Por ejemplo, en la aplicación Telegram se publican a diario más de 200 fotos de personas dadas por desaparecidas en Ucrania, algunas de ellas víctimas de desaparición forzada. Neuville M., Les réseaux sociaux, principaux alliés dans la recherche des personnes disparues, 2022. En otros contextos, TikTok se utiliza para denunciar abusos, incluida la desaparición forzada.

facilitar el establecimiento de la suerte y el paradero de las personas desaparecidas, existe una preocupación sobre el almacenamiento y protección adecuada y segura de estos datos altamente sensibles, , teniendo en cuenta también los casos de ciberataques, violaciones de datos y piratería informática mencionados anteriormente. Es así que se ha planteado al Grupo de Trabajo que, incluso cuando existen normas rigurosas de protección de datos, podrían modificarse para incluir cláusulas que traten específicamente la cuestión de la desaparición forzada, por ejemplo, previendo procedimientos de "congelación rápida" (*quick freeze*) que permiten la conservación de datos a petición de una persona que se sienta en peligro.

40. Algunas tecnologías pueden no ser aplicables o relevantes para los casos en los que la persona desapareció antes de que existieran los “teléfonos inteligentes” (*smartphone*) o Internet. La desaparición forzada es un delito permanente y una violación continuada de múltiples derechos humanos[47] y, por lo tanto, la búsqueda es una obligación continua.[48] Por ello, es esencial seguir invirtiendo en el desarrollo de tecnologías que puedan ser decisivas también para esclarecer casos en los que la desaparición comenzó hace décadas. Las nuevas tecnologías pueden aportar resultados significativos en este sentido, pero las técnicas tradicionales centradas en el ser humano también deben mantenerse y utilizarse junto conlas primeras.

41. La búsqueda eficaz de personas desaparecidas requiere a menudo consultar y cotejar múltiples archivos que pueden estar compuestos por cientos de miles de páginas y terabytes de documentos. Las tecnologías pueden facilitar la tarea y aumentar la eficacia de la consulta dearchivos.[49] El Grupo de Trabajo recibió información al respecto de la existencia de un programa llamado Angelus,[50] desarrollado en México por matemáticos en colaboración con la Comisión Nacional de Búsqueda de Personas Desaparecidas y que se basa en el uso de una red de algoritmos, inteligencia artificial y aprendizaje automático. Este programa representa una buena práctica, ya que permite procesar y cruzar una enorme cantidad de datos y detectar la existencia de patrones, contextos y conexiones que pueden facilitar la búsqueda de personas desaparecidas.

42. El *data mining*, realizado manualmente o a través de diferentes tecnologías basadas en algoritmos, tiene un gran potencial en lo que respecta a la recopilación de información que puede resultar de crucial importancia tanto para la búsqueda de personas desaparecidas como para la promoción de la rendición de cuentas. Un ejemplo son los notables resultados obtenidos tanto en términos de establecer la suerte y el paradero de las personas desaparecidas como de identificar a los perpetradores, a partir de la información recuperada del Archivo Histórico de la Policía Nacional de Guatemala, descubierto en 2005.

43. Este caso es emblemático de cómo la tecnología y la aplicación de técnicas adecuadas, incluidos los métodos estadísticos, en términos de cruce aleatorio de documentos en varias etapas, modelo de datos y marco de codificación, son fundamentales para conservar, digitalizar e inspeccionar una enorme cantidad de datos, ante la imposibilidad de examinar sistemáticamente cada documento individual.[51] El acceso informático, el reconocimientoóptico de caracteres, el reconocimiento de escritura a mano, así como el reconocimiento facial y de voz para analizar material audiovisual,[52] son herramientas cruciales en este ámbito. Además, el ejemplo muestra el papel fundamental que desempeña la cooperación internacional, ya sea en el contexto de las

[47] Artículo 17 de la Declaración sobre la Protección de Todas las Personas contra las Desapariciones Forzadas; Observación General sobre la Desaparición Forzada como Delito Continuado; y artículo 8 de la Convención Internacional sobre la Protección de Todas las Personas contra las Desapariciones Forzadas.

[48] Principio 7 de los Principios Rectores de la Búsqueda de Personas Desaparecidas de 2019.

[49] Sobre cómo las tecnologías pueden ser decisivas para hacer avanzar la justicia transicional (a través de la documentación, la digitalización y la memorialización), véase el número especial de 2019 de la Revista Internacional de Justicia Transicional.

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

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

[52] Donida Labati R. et al., Reconocimiento facial automático para la identificación forense de personas fallecidas en emergencias humanitarias, 2021.

organizaciones de la sociedad civil, el mundo académico[53] o a nivel intergubernamental.[54] Consideraciones similares se aplican también a las cantidades masivas de datos cargados en las redes sociales, o al subproducto documental de las iniciativas de búsqueda de la verdad, que pueden contener pruebas de crímenes internacionales, incluida la desaparición forzada, y que requieren una conservación y un procesamiento adecuados y debidamente regulados a largo plazo. Las herramientas forenses, incluida la comparación de bases de datos creadas por diferentes partes interesadas, son esenciales para garantizar la validación, identificación, análisis, interpretación, documentación y presentación de la información digital procedente de fuentes y archivos digitales.

44. El Grupo de Trabajo también recibió información que ilustra cómo las herramientas digitales -a menudo creadas por organizaciones de la sociedad civil- pueden utilizarse no sólo para buscar a personas desaparecidas, sino también -mediante intervenciones en las primeras etapas- para evitar que las detenciones arbitrarias se conviertan en desapariciones forzadas.[55] Estas herramientas ofrecen opciones gratuitas y seguras que ayudan a los familiares de las personas desaparecidas a navegar por los meandros de la burocracia y a obtener rápidamente información que puede resultar vital, o a gestionar el expediente de su caso ante las autoridades nacionales.[56] Además, se ha sugerido que las aplicaciones existentes utilizadas en el contexto de la violencia doméstica,[57] podrían adaptarse para prevenir las desapariciones forzadas o para facilitar las actividades de búsqueda. El Grupo de Trabajo recibió información sobre cómo los migrantes que temen estar en riesgo inmediato de ser desaparecidos forzadamente han utilizado las redes sociales para compartir imágenes de vídeo de su ubicación y coordenadas geográficas en vivo, lo que ha resultado fundamental para establecer su suerte y paradero y, en ocasiones, para reunir pruebas de los delitos perpetrados contra ellos.

45. El Grupo de Trabajo tuvo conocimiento de estudios dirigidos a explorar cómo el uso de la inteligencia artificial y del aprendizaje automático, a través del análisis de datos de redes de smartphones, puede contribuir a establecer el paradero de personas desaparecidas. Estos estudios se encuentran en una fase embrionaria y pueden resultar cruciales para llegar al esclarecimiento de muchos casos, como demuestran también experiencias exitosas puestas en marcha por organizaciones de la sociedad civil que utilizan tecnologías de inteligencia artificial y publicidad digital para localizar a niños desaparecidos.[58] Estos estudios y experiencias deben fomentarse, incluso mediante financiación y cooperación internacional. No obstante, debe tenerse en cuenta la existencia de importantes diferencias socioeconómicas, con el fin de proporcionar un apoyo adecuado y garantizar el acceso a estas nuevas tecnologías a los países en desarrollo. En este contexto, los Estados deben cooperar y prestarse todo el auxilio posible en la búsqueda, localización y liberación de las personas desaparecidas y, en caso de fallecimiento, en su exhumación e identificación y en la restitución de sus restos.[59]



[53] El Grupo de Análisis de Datos sobre Derechos Humanos diseñó la estrategia y aplicó las técnicas que permitieron los notables resultados mencionados. La Universidad de Texas, a través de un proyecto de colaboración, creó y alberga el archivo digital.

[54] Un ejemplo notable de cooperación interestatal destinada a crear capacidades forenses y de documentación es el proyecto Archivos Documentales Cóndor del Mercado Común del Sur (MERCOSUR). Las Naciones Unidas han apoyado varias iniciativas sobre identificación y recopilación de datos en todo el mundo (A/HRC/36/50/Add.1, párrs. 5, 8, 35, 36, 58).

[55] El chatbot BUSQUEMOS, desarrollado por la ONG mexicana Documenta, que facilita la búsqueda temprana de personas desaparecidas que puedan estar recluidas en diferentes centros de detención, desde prisiones, comisarías, cuarteles del ejército o centros de retención de migrantes hasta instituciones de salud mental y hospitales. Ofrece apoyo gratuito, a través de interacciones que duran menos de 5 minutos y que no requieren que los usuarios revelen ningún dato sensible.

[56] Por ejemplo, la plataforma Nosomosexpedientes, desarrollada por la ONG mexicana Centro de Derechos Humanos Miguel Agustín Pro Juárez, que apoya a las familias en sus esfuerzos de búsqueda y en la gestión de sus expedientes ante las autoridades nacionales.

[57] Se hizo referencia a la plataforma Salvarte.

[58] Véase la plataforma lanzada en 2018 por el Centro Internacional para Menores Desaparecidos y Explotados.

[59] Convención Internacional para la Protección de Todas las Personas contra las Desapariciones Forzadas, art. 15.

# III. Uso de nuevas tecnologías para documentar casos de desaparición forzada y enjuiciar y castigar a los perpetradores

46. El uso de las tecnologías en la documentación de violaciones graves de los derechos humanos y en la promoción de la rendición de cuentas, especialmente a través de la inteligencia de fuente abierta, ha sido objeto de una atención creciente[60] y de informes seminales publicados por otros Procedimientos Especiales de la ONU.[61] Como ya se ha mencionado, las tecnologías pueden desempeñar un papel crucial en la obtención de datos e información que permitan esclarecer la suerte y el paradero de las personas desaparecidas, pero también identificar a los responsables de los crímenes en cuestión. Sin embargo, los hallazgos adquiridos a través de estos medios deben garantizarse de manera que resistan el escrutinio, incluso en el contexto de los procedimientos penales, en los que el estándar de prueba aplicable es "más allá de toda duda razonable". Averiguar la fuente de las pruebas recogidas mediante tecnologías y descartar que hayan sido objeto de falsificación o manipulación puede resultar especialmente complejo. Además, los algoritmos de borrado mediante aprendizaje automático (*machine-learning deletion algorithms*) que aplican plataformas como Google o Facebook pueden borrar rápidamente los contenidos digitales, lo que conlleva la pérdida de pruebas que resultan prácticamente imposibles de recuperar.

47. Esto puede resultar especialmente difícil en los casos de desaparición forzada, un delito que, por su naturaleza, está envuelto en el secreto y se caracteriza por la ocultación y la "ausencia", más que por la presencia de pruebas manifiestas. En este sentido, si bien puede ser relativamente más fácil documentar a través de las nuevas tecnologías dos de loselementos constitutivos del delito (es decir, la privación de libertad de la víctima y la afiliación de los autores), el elemento de ocultación de la suerte o el paradero de las personas desaparecidas plantea más obstáculos, así como, en su caso (es decir, conforme a la definición de desaparición forzada como crimen de lesa humanidad contenida en el Estatuto de Roma de la Corte Penal Internacional),[62] el de la intención de sustraer a la persona desaparecida de la protección de la ley durante un período prolongado.

48. Como se señala en una de las contribuciones recibidas, las peculiaridades de la desaparición forzada exigen una aplicación "agregada" de herramientas de código abierto, cada una de ellas dirigida a un elemento específico de la definición de la conducta. El carácter "oculto" del crimen, así como la presencia de un elemento mental específico en la definición de desaparición forzada como crimen de lesa humanidad contenida en el Estatuto de Roma de la Corte Penal Internacional, hace improbable que el código abierto proporcione por sí solo todo el material que califique una conducta específica como desaparición forzada. Sin embargo, podría ofrecer indicaciones útiles sobre la identidad de la víctima, el acto de privación de libertad, el lugar de la detención así como la identidad y afiliación del autor. Asimismo, la inteligencia de código abierto podría utilizarse para documentar el elemento contextual del crimen en el derecho penal internacional, es decir, la presencia de un ataque dirigido contra una población civil, su carácter generalizadoo sistemático y la comisión del acto como parte del ataque.

49. Encontrar y reunir información corroborante a través de las tecnologías -y especialmente de TIC – requiere esfuerzos formidables en términos de investigación específica, verificación y preservación, que deben realizarse siempre de forma sistemática yprofesional, especialmente para garantizar la cadena de custodia y, en caso necesario, la admisibilidad en los tribunales en una fase posterior. A lo largo de todo el proceso, desde la recogida de pruebas por medio de tecnologías, hasta su comparecencia ante un tribunal, deben tenerse debidamente en cuenta las implicaciones éticas y de seguridad. En particular, la evaluación de riesgos debe incluir la consideración de los aspectos relacionados con la privacidad y la protección de datos, la obtención -cuando sea factible-

[60] Entre otros, el simposio publicado en 2023 por Opinio Juris sobre imparcialidad, igualdad y diversidad en las investigaciones de código abierto; el número especial publicado en 2021 por el Journal of International Criminal Justice sobre nuevas tecnologías e investigación de crímenes internacionales.

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

[62] Art. 7, párr. 2 (i), del Estatuto de Roma de la Corte Penal Internacional de 1998 y las legislaciones penales nacionales que reproducen la definición del delito contenida en el mismo.

del consentimiento informado de las personas y comunidades pertinentes y los riesgos basados en los datos de identificación demográfica.

50. Las primeras horas y días tras la privación de libertad de las personas son cruciales para obtener datos que pronto podrían ser borrados o manipulados. La existencia de imágenessatelitales de acceso público, redes sociales y smartphones con cámara ofrece datos valiosos a los que se puede acceder de forma relativamente fácil y barata y que proporcionan pruebas de la comisión de delitos, incluida la desaparición forzada. El Grupo de Trabajo recibió con interés información sobre aplicaciones y programas informáticos que capturan y conservan copias probatorias de contenidos en línea y material audiovisual, incorporándoles los metadatos necesarios para demostrar su autenticidad ante los tribunales y facilitando la anotación de datos.[63]

51. La preservación de la cadena de custodia de las pruebas obtenidas con el uso de las nuevas tecnologías es esencial para garantizar la autenticidad del material recogido. El Protocolo de Berkeley consagra los principios fundamentales que deben respetarse en este contexto y debe difundirse y aplicarse, junto con otras directrices sobre la materia elaboradas por organizaciones de la sociedad civil.[64] Los aspectos que requieren especial atención están relacionados con la fragilidad inherente a las tecnologías, la necesidad de normalizar la gestión técnica de los conjuntos de datos archivados y la validación de dichos datos. El Grupo de Trabajo recibió información sobre programas que, utilizando a menudo inteligencia artificial, permiten evaluar la integridad de las imágenes digitales y detectar soportes falsificados. Estas tecnologías ofrecen una ayuda significativa en la obtención de pruebas admisibles ante los tribunales.

52. Las grabaciones de vídeo e imágenes publicadas en las redes sociales o recogidas a través de cámaras corporales (*dash-cams)* pueden contener pruebas de la comisión de graves violaciones de los derechos humanos, entre ellas las desapariciones forzadas, y han sido aceptados como prueba válida ante tribunales, por organismos internacionales de derechos humanos y por comisiones de investigación. Por ejemplo, el Tribunal Europeo de Derechos Humanos consideró que un vídeo publicado en Youtube era una prueba válida de los malos tratos a los que había sido sometida una persona desaparecida tras haber sido privada de libertad.[65] La Corte Penal Internacional dictó una orden de detención basada principalmente en pruebas recogidas de publicaciones en las redes sociales;[66] la Misión Internacional Independiente de Investigación sobre Myanmar se basó en datos audiovisuales y publicaciones escritas en las redes sociales como pruebas para solicitar la investigación de crímenes internacionales;[67] y los tribunales nacionales admitieron pruebas de código abierto en juicios relativos a crímenes internacionales.[68] La posibilidad de evaluar, verificar y, en última instancia, admitir pruebas recogidas a través de las tecnologías depende de la capacidad de cada tribunal y de las habilidades y conocimientos del personal, que pueden variar significativamente, especialmente a nivel nacional. El Grupo de Trabajo considera que los Estados deben adoptar todas las medidas necesarias a este respecto, incluso asegurando los recursos financieros, técnicos y humanos necesarios y proporcionando formación periódica a las autoridades competentes.

53. Se informó al Grupo de Trabajo de que las nuevas tecnologías -incluidos los programas de geolocalización, el seguimiento de vuelos, el análisis de redes, el modelado en 3D, la teledetección o detección remota, el análisis de audio, la sincronización y la fotogrametría- ya han demostrado

[63] Véase el anexo I. Los metadatos en cuestión incluyen, como mínimo, una marca de tiempo, datos de localización y un código alfanumérico único. A continuación, deben almacenarse de forma segura, preferiblemente tras su encriptación.

[64] Véase, entre otros, la metodología para la investigación de fuentes abiertas en línea sobre los incidentes que están teniendo lugar en Ucrania desde el 24 de febrero de 2022, publicada por Bellingcat y Global Legal Action Network.

[65] TEDH, asunto S.T. e Y.B. contra Rusia, sentencia de 19 de octubre de 2021, párr. 10, 22, 48 y 80.

[66] Véanse las órdenes de detención emitidas respectivamente en 2017 y 2018 por la Corte Penal Internacional en el caso Fiscal contra Al-Werfalli. En los últimos años, la División de Investigación de la Corte estableció una Junta de Asesoramiento Científico y una Junta de Asesoramiento Tecnológico.

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

[68] Entre otros, Informe de la Red Eurojust contra el Genocidio de la Unión Europea, 2018, que ilustra ejemplos de Alemania, Finlandia y Suecia.

su eficacia en la reconstrucción de escenas del crimen y en el seguimiento de presuntos autores de delitos y violaciones de los derechos humanos. Por lo tanto, su uso debería contemplarse como parte de un protocolo de investigación regular relativo a las desapariciones forzadas. También se ha utilizado con éxito una combinación de técnicas (por ejemplo, imágenes por satélite, cartografía digital, análisis de secuencias de vídeo y crono-localización) para recopilar pruebas de desapariciones forzadas de migrantes y determinar su suerte y paradero.[69]

54. El Grupo de Trabajo recibió información sobre un número creciente de casos en losque, ante la indiferencia o inactividad de las autoridades, familiares de personas desaparecidas o sus representantes, o múltiples organizaciones de la sociedad civil a través de ejercicios de *crowd-solving*, consiguieron recopilar, utilizando diferentes tecnologías, información sobre las circunstancias de la desaparición, así como la identidad o la afiliación de los perpetradores. Utilizaron las redes sociales, Internet, CCTV, los registros de llamadas, el rastreo de datos móviles y la geolocalización o las imágenes por satélite. Aunque estas experiencias dieron resultados significativos, también expusieron a las personas afectadas a grandes riesgos, como se ilustra en la sección II.

55. El Grupo de Trabajo señala que la carga de recopilar este tipo de datos a través de las tecnologías no puede dejarse en manos de los familiares de las personas desaparecidas y sus representantes, mientras que las autoridades no parecen buscar, verificar, analizar y asegurar estas pruebas de manera sistemática, aunque tienen la obligación de hacerlo la obligación de hacerlo. Los Estados deben intensificar sus esfuerzos y tomar todas las medidas necesarias para reforzar la capacidad de las autoridades competentes para utilizar las tecnologías en la investigación de las desapariciones forzadas. Los Estados se deben prestar mutuamente todo el auxilio judicial posible en lo que respecta a cualquier procedimiento penal relativo a una desaparición forzada, inclusive el suministro de todas las pruebas necesarias para el proceso que obren en su poder.[70]

# V. Conclusiones y recomendaciones

**56. Como en muchos aspectos relacionados con las nuevas tecnologías, su relación con los derechos humanos -en este caso en el ámbito de las desapariciones forzadas- es ambivalente. Por un** lado**, las nuevas tecnologías, y en particular TIC se utilizan con frecuencia para facilitar u ocultar la comisión de desapariciones forzadas, obstaculizar la labor de los defensores de los derechos humanos y los familiares de las personas desaparecidas, e intimidarlos o acosarlos. Las tecnologías se desarrollan a un ritmo vertiginoso y a menudo se comercializan y utilizan sin que tanto los Estados como las empresas apliquen la diligencia debida en materia de derechos humanos, en ausencia de un marco normativo sólido que tenga en cuenta el derecho internacional de los derechos humanos, prevea una supervisión independiente y promueva la rendición de cuentas y ofrezca un recurso efectivo en caso de violaciones.**

**57. El Grupo de Trabajo está especialmente preocupado por el uso de apagones de Internet e interrupciones selectivas de la conectividad; programas espía; vigilancia selectiva y masiva, incluido el reconocimiento facial y de la forma de andar; ciberataques y fábricas de trolls patrocinadas por los Gobiernos; y el uso engañoso de legislación relacionada con la tecnología para reprimir la disidencia y atacar a personas defensoras de los derechos humanos y familiares de personas desaparecidas.**

**58. En lo que concierne a la búsqueda de personas desaparecidas, a la documentación del delito y a la promoción de la rendición de cuentas, las nuevas tecnologías pueden ofrecer soluciones rentables que ya han demostrado su utilidad y que probablemente tendrán nuevas consecuencias relevantes. El Grupo de Trabajo subraya que no se debe confiar**

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

[70] Convención Internacional para la protección de todas las personas contra las desapariciones forzadas, art. 14.

**excesivamente en las nuevas tecnologías en este ámbito y que las expectativas deben ser realistas: aunque van a facilitar los procesos en cuestión, no van a solucionar todos los problemas existentes. No deben abandonarse los enfoques y técnicas tradicionales de documentación, seguimiento y elaboración de informes, y no pueden sustituirse totalmente por material digital y nuevas tecnologías.**

**59. La complementariedad entre estas estrategias debe perseguirse y promoverse activamente, y los procesos tradicionales centrados en el ser humano deben fomentarse y reforzarse en consecuencia. Paralelamente, el acceso a las nuevas tecnologías deberá concebirse de forma que no reproduzca ni profundice la brecha digital y las diferencias socioeconómicas existentes, y que ningún país en desarrollo ni parte interesada relevante pueda quedar excluido.**

**60. El hecho de que las nuevas tecnologías ofrezcan soluciones rentables que podrían avanzar significativamente tanto la búsqueda de las personas desaparecidas como las investigaciones penales, y que algunas de las herramientas pertinentes sean fácilmente accesibles y puedan ser utilizadas también por organizaciones de la sociedad civil y asociaciones de familiares de personas desaparecidas, es un avance positivo que puede resultar decisivo para ofrecer una mejor protección contra las desapariciones forzadas.**

61. **El Grupo de Trabajo anima a las organizaciones de la sociedad civil a explorar estas posibilidades y a reforzar sus capacidades, pero reafirma que la búsqueda de las personas desaparecidas y las correspondientes investigaciones penales son obligaciones internacionales de los Estados, que no pueden dejarse enteramente en manos dela sociedad civil y de los familiares de las personas desaparecidas, ni depender únicamente de su iniciativa. Los Estados deben adoptar medidas para incluir las nuevas tecnologías en las actividades de búsqueda y en las investigaciones penales. Los Estados también tienen la obligación de cooperar y prestarse mutuamente el mayor auxilio posible en estos ámbitos.**

62. **El Grupo de Trabajo señala que la cooperación entre las diferentes partes interesadas, incluidos los Estados, las empresas, las organizaciones de la sociedad civil,las Instituciones Nacionales de Derechos Humanos, las instituciones académicas y los donantes es indispensable y, como tal, debe promoverse. Las siguientesrecomendaciones reflejan este entendimiento. En particular, el Grupo de Trabajo alienta a fortalecer la coordinación y la cooperación entre las diferentes partes interesadas a fin de forjar alianzas para detectar los riesgos relacionados con las nuevas tecnologías y la desaparición forzada, diseñar estrategias de mitigación y medidas eficaces para superar los obstáculos identificados y promover herramientas para apoyar a las personas directamente afectadas, incluidas las personas defensoras de los derechos humanos y los familiares de las personas desaparecidas. Existe una responsabilidad compartida para garantizar que las nuevas tecnologías se desarrollen y utilicen dentro de un marco de derechos humanos, de forma ética y responsable.**

**63. El Grupo de Trabajo se compromete a hacer un seguimiento periódico de la cuestión de las nuevas tecnologías y las desapariciones forzadas y a incluir sistemáticamente observaciones y recomendaciones sobre este tema en sus actividades, incluidas las comunicaciones, los llamamientos urgentes, las denuncias, las cartas de intervención inmediata, las visitas a países y las actividades de sensibilización. El Grupo de Trabajo también ofrece asistencia en la materia a los Estados mediante servicios de cooperación y asesoramiento.**

**64. El Grupo de Trabajo hace un llamamiento a todas las partes interesadas para que se comprometan y cooperen regularmente con él e informen sobre el impacto negativo de las nuevas tecnologías en el disfrute de los derechos humanos,especialmente de las personas defensoras de los derechos humanos y los familiares de las personas desaparecidas, así como sobre los progresos realizados en relación con el uso de las nuevas tecnologías en la búsqueda de personas desaparecidas y en la investigación y promoción de la rendición de cuentas.**

**65. Para ello, el Grupo de Trabajo recomienda a los Estados:**

**(a) Abstenerse de imponer apagones de Internet y restricciones al acceso a las comunicaciones o a determinadas plataformas de medios sociales;**

**(b) Maximizar el acceso a Internet y eliminar los múltiples obstáculos que se interponen en las comunicaciones;**

**(c) Adoptar todas las medidas necesarias para garantizar que las personas defensoras de los derechos humanos, los familiares de personas desaparecidas, los y las periodistas y los usuarios de redes sociales puedan ejercer sin injerencias indebidas su derecho a mantener opiniones y la libertad de expresión en línea (por ejemplo, através de redes sociales, blogs o cuentas similares) sin ser criminalizados por informar o denunciar desapariciones forzadas; también deben tomarse medidas para garantizar que la legislación sobre ciberseguridad no se aplique erróneamente para frenar la disidencia;**

**(d) Garantizar que la descarga y el uso de una aplicación no puedan invocarse como prueba única o decisiva de un delito;**

**(e) Garantizar la formación del personal de las fuerzas y cuerpos de seguridad, civiles o militares, y de los funcionarios públicos sobre las garantías fundamentales que deben asegurarse en el momento de la detención de cualquier persona, en particular en lo que respecta a las normas aplicables a la confiscación, inspección o destrucción de dispositivos electrónicos; y establecer la responsabilidad de quienes no respeten dichas normas;**

**(f) Tomar todas las medidas necesarias para impedir ciberataques, campañas de difamación y desinformación contra personas defensoras de los derechos humanos, incluidos familiares de personas desaparecidas, mediante phishing, malware, ransomware, espionaje, filtración de información contaminada (tainted leaks), "granjas de trolls" y doxxing, e investigar todos los casos pertinentes con vistas a identificar, enjuiciar y sancionar a los responsables y ofrecer reparación a las víctimas;**

**(g) Imponer una moratoria inmediata sobre la exportación, venta, transferencia, uso o servicio de herramientas de vigilancia selectiva y masiva desarrolladas por el sector privado, incluidos programas espía, de reconocimiento facial y similares, hasta que se establezca un régimen de salvaguardias que respete los derechos humanos;**

**(h) Desarrollar y aplicar sin demora un marco jurídico por el que la concesión de licencias de cualquier tecnología, y especialmente de las tecnologías de vigilancia selectiva y masiva, esté condicionada a una revisión nacional de los derechos humanos y al cumplimiento por parte de las empresas de los Principios Rectores sobre las Empresas y los Derechos Humanos; dicho marco debe garantizar que la transferencia, venta y adquisición de tecnologías de vigilancia selectiva y masiva esté sujeta a consulta y supervisión públicas;**

**(i) Adoptar todas las medidas necesarias para investigar, enjuiciar y exigir responsabilidades a las personas, empresas y Estados responsables de violaciones de derechos humanos relacionadas con la venta, transferencia y uso de tecnologías de vigilancia selectiva y masiva;**

**(j) Garantizar que las personas u organizaciones de la sociedad civil afectadas puedan ejercer su derecho a un recurso efectivo y obtener reparación;**

**(k) Garantizar que la recopilación conservación y utilización de datos biométricos y genéticos esté regulada en la ley y en la práctica, tenga un alcance limitado, sea transparente, necesaria y proporcionada para cumplir un objetivo legítimo de seguridad, y no se base en ninguna distinción, exclusión, restricción o preferencia por motivos de raza, color, ascendencia u origen nacional o étnico;**

**(l) Revisar, mediante un proceso multidisciplinar, la adecuación de las políticas y los marcos jurídicos aplicables, con el fin de diseñar estrategias paraprevenir y abordar el impacto negativo sobre los derechos humanos generado por el uso de las nuevas tecnologías, incluido el aprendizaje automático y la inteligencia artificial;**

**(m) Garantizar que las tecnologías de vigilancia masiva y selectiva, así como las soluciones de inteligencia artificial y aprendizaje automático no se utilicen en las fronteras para llevar a cabo operaciones de expulsión que puedan conducir, y en algunos casos equivaler, a desapariciones forzadas. Los datos sobre los movimientos migratorios recopilados a través de estas tecnologías deben utilizarse para facilitar las operaciones de búsqueda y rescate y con fines humanitarios;**

**(n) Garantizar que las tecnologías utilizadas para la búsqueda de las personas desaparecidas y las investigaciones correspondientes incorporen la recopilación y el análisis de detalles sobre la persona afectada desde una perspectiva de género, para abarcar las experiencias y expresiones no normativas;**

**(o) Buscar de forma proactiva a la persona desaparecida con vida y adoptar las medidas y recursos necesarios para desarrollar y aplicar tecnologías que se centren en las primeras etapas de una desaparición forzada;**

**(p) Adoptar todas las medidas necesarias para garantizar que las autoridades encargadas de la búsqueda de personas desaparecidas y de las investigaciones penales correspondientes cuenten con los recursos financieros, humanos y técnicos adecuados y, en particular, con las tecnologías más avanzadas (incluidos LiDAR, unidades SONAR, drones, imágenes por satélite, etc.) y reciban formación regular y adecuada, incluso sobre la aplicación del Protocolo de Berkeley;**

**(q) Cooperar con otros Estados, prestándose mutuamente todo el auxilioposible en el uso de tecnologías que faciliten la búsqueda de personas desaparecidas y en lo relativo a la asistencia jurídica en relación con los procedimientos penales incoados por una desaparición forzada, incluida la obtención y el suministro de todas las pruebas de que dispongan y que sean necesarias para los procesos;**

**(r) Asegurar la interoperabilidad de las bases de datos genéticos que pueden ser instrumentales en la búsqueda de personas desaparecidas, garantizando que los datos contenidos en ellas se almacenan de forma segura y se utilicen con fines exclusivamente humanitarios. En particular, las iniciativas dirigidas a mejorar la identificación y el intercambio biométrico y genético entre fuerzas de seguridad, especialmente en las fronteras, deben guiarse por el hecho de que las supuestas consideraciones de seguridad no pueden prevalecer sobre la garantía de los derechos humanos fundamentales, incluido el derecho a conocer la verdad en relación con posibles desapariciones forzadas;**

**(s) Adoptar todas las medidas necesarias, incluso mediante tecnologías, para preservar y facilitar el acceso a los archivos que puedan contener información relevante sobre desapariciones forzadas;**

**(t) Proporcionar formación adecuada y regular a las autoridades judiciales y de investigación nacionales sobre la recopilación, almacenamiento, validación y evaluación de las pruebas obtenidas a través de las nuevas tecnologías, asegurando los recursos necesarios y desarrollando o reforzando la infraestructura correspondiente.**

**66. El Grupo de Trabajo recomienda a las empresas de tecnología y software:**

**(a) Llevar a cabo sus actividades, especialmente en lo que respecta al desarrollo, venta, transferencia y uso de nuevas tecnologías, respetando los Principios Rectores sobre las Empresas y los Derechos Humanos de las Naciones Unidas;**

**(b) Adoptar todas las medidas para evitar los apagones y la restricción de acceso a Internet que les haya solicitado el Estado y actuar con la diligencia debida para evaluar los riesgos para los derechos humanos y operar en consecuencia, mitigar los posibles efectos adversos y garantizar el acceso a una reparación;**

**(c) Adoptar todas las medidas necesarias para impedir los ciberataques y las campañas de difamación y desinformación contra las personas defensoras de los derechos**

**humanos, incluidos los familiares de personas desaparecidas a través de phishing, malware, ransomware, espionaje, filtraciones de informaciones contaminadas (tainted leaks), "granjas de trolls" y doxxing;**

**(d) Los proveedores de servicios de Internet, las redes sociales y las plataformas relacionadas deben alertar a sus usuarios de los intentos de pirateo del Gobierno y elaborar una guía para los usuarios de plataformas digitales,en la que se les informe de los riesgos de ciberataques y de robo y uso de sus datos y metadatos, compartiendo buenas prácticas para prevenir estos casos; también deben establecer garantías sólidas para proteger los metadatos de los usuarios de la explotación malévola;**

**(e) Las empresas de vigilancia deben tomar todas las medidas necesarias para cumplir sus obligaciones internacionales en materia de derechos humanos; en particular, deben actuar con la diligencia debida y realizar una evaluación exhaustiva del impacto sobre los derechos humanos antes de cualquier posible venta o transferencia que implique tecnologías de vigilancia selectiva y masiva, incluidos programas de reconocimiento facial, programas espía y similares; deben incluir cláusulas contractuales que prohíban el uso de tecnologías de vigilancia que infrinjan el derecho internacional de los derechos humanos y, en caso de detectar un uso indebido, informar sin demora a los organismos de supervisión nacionales, regionales o internacionales pertinentes; y deben poner en marcha mecanismos de reparación que permitan a las víctimas de abusos presentar denuncias y obtener reparación;**

**(f) Contribuir al desarrollo de medios más seguros para recopilar, almacenar y analizar datos -especialmente información sensible relativa a personas desaparecidas y sus familiares-, garantizando su uso exclusivamente humanitario; y también desarrollar herramientas de código abierto y fácil acceso para realizar análisis forenses de dispositivos electrónicos y espacios digitales potencialmente comprometidos;**

**(g) Contribuir al desarrollo de tecnologías que permitan buscar proactivamente con vida a las personas desaparecidas y que se centren en las primeras etapas de una desaparición forzada;**

**(h) Considerar la posibilidad de invertir en el desarrollo de tecnologías que, unidas a los enfoques tradicionales centrados en el ser humano, sean decisivas para la búsqueda de personas cuya desaparición forzada comenzó antes de la existencia de lossmartphones y las correspondientes investigaciones penales;**

**(i) Promover el desarrollo de tecnologías, incluidas herramientas forensesque permitan garantizar la validación, identificación, análisis, interpretación, documentación y presentación de la información digital derivada de fuentes digitales y cotejar múltiples archivos.**

**67. El Grupo de Trabajo recomienda que las organizaciones de la sociedad civil, las instituciones nacionales de derechos humanos y las instituciones académicas:**

**(a) Continuar sus esfuerzos para documentar y denunciar los casos de apagones de Internet y restricciones selectivas, así como los ciberataques y las campañas de difamación y desinformación contra las personas defensoras de los derechos humanos, incluidos los familiares de personas desaparecidas;**

**(b) Hacer todo lo posible para aumentar la concienciación sobre los riesgos existentes relacionados con el uso de las nuevas tecnologías y, en particular, la sensibilidad y el daño de los datos, con vistas a crear competencias básicas sobre alfabetización e higiene digitales;**

**(c) Continuar sus esfuerzos para desarrollar herramientas digitales que apoyen a los familiares de las personas desaparecidas en la gestión de los expedientes de los casos, les ayuden en el proceso de búsqueda y apoyen la prevención de las desapariciones forzadas;**

**(d) Continuar sus esfuerzos para llevar a cabo inteligencia de código abierto,**

**aplicando los principios consagrados en el Protocolo de Berkeley;**

**(e) Seguir investigando sobre cuestiones relacionadas con las nuevas tecnologías y las desapariciones forzadas, especialmente en lo que respecta a las buenas prácticas existentes, contribuyendo así a mejorar su visibilidad y difusión.**

**68. El Grupo de Trabajo recomienda que las agencias de desarrollo y a los donantes:**

**(a) Integrar las** consideraciones **de derechos humanos en los esfuerzos por ampliar las redes de comunicaciones y cerrar la brecha digital mundial;**

**(b) Adoptar todas las medidas necesarias para garantizar un acceso asequible a Internet al mayor número de personas, a fin de incrementar el uso de las tecnologíasbasadas en Internet como facilitadoras y potenciadoras del ejercicio de los derechos humanos, también en lo que respecta a la búsqueda de personas desaparecidas y la documentación de los crímenes correspondientes;**

**(c) Apoyar proyectos destinados a documentar los efectos adversos de las nuevas tecnologías sobre los derechos humanos, en particular en casos relacionados con desapariciones forzadas;**

**(d) Apoyar programas de formación sobre alfabetización e higiene digitales, así como sobre inteligencia de código abiertos, dirigidos a organizaciones de la sociedad civil y, en particular, a asociaciones de familiares de personas desaparecidas, con vistas a alertar sobre los riesgos existentes y garantizar que desarrollencapacidades básicas en estos ámbitos, incluso para diagnosticar, responder y recuperarse de eventos digitales adversos;**

**(e) Apoyar el desarrollo de tecnologías destinadas a facilitar la búsqueda de personas desaparecidas y las investigaciones correspondientes y garantizar el acceso a dichas herramientas -así como la formación adecuada del personal- en los países menos desarrollados;**

**(f) Apoyar proyectos para fomentar el uso de tecnologías que garanticen la verificación, el análisis, la interpretación y la presentación de la información contenida en archivos y fuentes digitales;**

**(g) Apoyar los estudios destinados a explorar cómo el uso de la inteligencia artificial y el aprendizaje automático, mediante el análisis de datos de la red de los smartphones, puede contribuir a establecer el paradero de las personas desaparecidas y el desarrollo de las tecnologías correspondientes.**

**69. El Grupo de Trabajo recomienda que otros mecanismos de derechos humanos y tribunales internacionales:**

**(a) Promover la rendición de cuentas de los Estados, empresas o particulares responsables del uso indebido de tecnologías de vigilancia selectiva o masiva, así como de ciberataques y, en general, del uso de nuevas tecnologías para facilitar u ocultarla comisión de desapariciones forzadas;**

**(b) Adaptar los criterios probatorios aplicables para que las pruebas de desapariciones forzadas obtenidas a través de inteligencia de código abierto sean debidamente consideradas en los procesos pertinentes.**

**70. El Grupo de Trabajo recomienda que la Oficina del Alto Comisionado de lasNaciones Unidas para los Derechos Humanos:**

**(a) Garantice que se proporcionan los medios adecuados para reforzar la protección de la información sensible relativa a las personas desaparecidas y sus familiares por parte de la Oficina del Alto Comisionado, los Procedimientos Especiales u otros mecanismos, como comisiones de investigación o misiones de investigación;**

**(b) Difunda y promueva la aplicación del Protocolo de Berkeley.**

# Anexo I

## Mapeo de herramientas, contactos y recursos gratuitos a disposición del público que pueden proporcionar información útil sobre las tecnologías nuevas/digitales y ayudar y facilitar la búsqueda de personas desaparecidas y las correspondientes investigaciones penales [lista no exhaustiva]

### Organizaciones sin ánimo de lucro, colectivos y empresas tecnológicas

- Access now: dedicada a defender y ampliar los derechos digitales de las personas y comunidades en situación de riesgo (disponible en inglés)
- Bellingcat: colectivo independiente para investigaciones en línea
- Border Forensics: agencia que utiliza el análisis espacial y visual para investigar las prácticas de violencia en las fronteras (disponible en inglés y francés)
- CyberPeace Institute: ONG que trabaja, incluso prestando apoyo a organizaciones de la sociedad civil, para reducir los daños de los ciberataques (disponible en inglés y francés)
- Digipower Academy: ayuda a personas y ONGs a aprender sobre datos y flujos de datos (disponible en inglés y francés)
- Digital Preservation Coalition: organización que apoya el acceso a largo plazo a contenidos y servicios digitales (disponible en inglés)
- Electronic Frontier Foundation: ONG que defiende las libertades civiles en el espacio digital (disponible en inglés)
- Equipo Argentino de Antropología Forense (EAAF): ONG dedicada desde 1986 al desarrollo de técnicas de antropología forense para ayudar a localizar e identificar a víctimas de desapariciones forzadas
- Frontline Defenders: ONG que presta apoyo a personas defensoras de los derechos humanos en situación de riesgo, incluso debido al (ab)uso de las nuevas tecnologías
- Human Rights Data Analysis Group: ofrece análisis estadísticos de datos referentes a violaciones graves de los derechos humanos (disponible en inglés)
- HURIDOCS: ONG que ayuda a los grupos de defensa de los derechos humanos a recopilar, organizar y utilizar la información (disponible en inglés)
- ICT4peace: fundación que promueve el uso de las tecnologías de la información y la comunicación para la consolidación de la paz (disponible en inglés)
- Investigadores Forenses Ciudadanos: Fuerzas Unidas por Nuestros Desaparecidos en Nuevo León (FUNDENL); Fuerzas Unidas por Nuestros Desaparecidos en Coahuila (FUUNDEC); Fuerzas Unidas por Nuestros Desaparecidos en México (FUUNDEM) -organizaciones que forman parte de movimientos liderados por víctimas con enfoques únicos para utilizar la tecnología en la búsqueda de sus seres queridos desaparecidos
- Locate International: organización benéfica registrada en el Reino Unido que, en colaboración con universidades, fuerzas de seguridad, policía y familias de personas desaparecidas, ayuda a estas últimas a encontrar a sus seres queridos (disponible en inglés)
- Meedan: organización tecnológica sin ánimo de lucro que crea programas informáticos e iniciativas para reforzar el periodismo mundial, la alfabetización digital y la accesibilidad de la

información (disponible en inglés)

- Mnemonic.org: ONG que apoya a las personas defensoras de los derechos humanos en el uso eficaz de la documentación digital de las violaciones de los derechos humanos y los crímenes internacionales (disponible en inglés)

- Personaldata.io: ONG que trabaja en temas relacionados con la protección de datos (disponible en francés)

- R3D: ONG mexicana que trabaja en la promoción y protección de los derechos humanos en el ámbito digital

- SITU: división interdisciplinar de investigación aplicada, que investiga y aborda cuestiones de derechos humanos desde el punto de vista de la arquitectura (incluida la investigación y el análisis espacial) (disponible en inglés)

- Storyful: una agencia de noticias e inteligencia (disponible en inglés)

- Tactical Tech: ONG que trabaja con ciudadanos y organizaciones de la sociedad civil para explorar y mitigar el impacto de la tecnología en la sociedad (disponible en inglés)

- The Whistle: start-up académica, con sede en la universidad de Cambridge, que desarrolla herramientas para poner en contacto a testigos de violaciones de derechos humanos con organizaciones locales a través de una plataforma segura (disponible en inglés)

- TraceLabs: organización sin ánimo de lucro cuya misión es acelerar la reunificación familiar de personas desaparecidas (disponible en inglés)

- Videre est credere: ONG que trabaja con activistas locales para formarles y proporcionarles tecnología que les permita capturar pruebas visuales de las violaciones de los derechos humanos (disponible en inglés)

- WITNESS: organización sin ánimo de lucro que ayuda a las personas que utilizan vídeos y la tecnología para proteger y defender los derechos humanos

## Herramientas

- Adarga.ai: plataforma de inteligencia artificial que utiliza procesos de tecnología analítica para extraer información a gran velocidad de datos no estructurados y presentarla en un formato comprensible (disponible en inglés)

- ADS-B Exchange: fuente de datos de vuelo (disponible en inglés)

- Archives.is: herramienta para tomar instantáneas de páginas web (disponible en inglés)

- ARcGIS: base de datos geográficos (patentada)

- AToM: aplicación de código abierto para la descripción y el acceso a archivos basados en estándares en un entorno multilingüe y multi-repositorio.

- Blender: aplicación de código abierto para modelaje 3D, la más adecuada para la reconstrucción digital de eventos espaciales, incluidas la geolocalización, la crono-localización y la reconstrucción forense (disponible en inglés)

- BUSQUEMOS [relevante para México]: chatbot desarrollado por la ONG mexicana Documenta, utilizado para garantizar la detección temprana de detenciones arbitrarias y la prevención de desapariciones forzadas

- Compass in the sky: una herramienta para reforzar las capacidades de crono-localización (disponible en inglés)

- Deepaware: herramienta para escanear vídeos e imágenes y detectar si han sido manipulados (disponible en inglés)

- Descartes Labs: plataforma que ofrece herramientas de geo-procesamiento (disponible en inglés)

- DFace: aplicación que detecta y difumina rostros en imágenes en línea (disponible en inglés)

- DevelopmentSeed Skynet: aprendizaje automático de código abierto sobre imágenes de satélite (disponible en inglés)

- DigitalGlobe: herramienta (de propiedad) para acceder a imágenes satelitales y aéreas (disponible en inglés)

- Enigio Trace: herramienta (de propiedad) para crear y gestionar documentos originales en línea (disponible en inglés)

- Exfitool: herramienta de código abierto para leer, escribir y editar metadatos (disponible en inglés)

- Eyewitness to atrocities: aplicación de cámara móvil que permite grabar fotos y vídeos a los que se incorporan los metadatos necesarios para demostrar su autenticidad ante un tribunal

- Google Earth: herramienta que permite acceder a imágenes por satélite

- Hunch.ly: herramienta de captura web diseñada para investigaciones en línea (disponible en inglés)

- I-Familia: base de datos mundial de INTERPOL para la identificación de personas desaparecidas basada en cotejos internacionales de ADN de parentesco

- Investigative dashboard: plataforma que ofrece diversas herramientas paralocalizar personas, empresas y activos en todo el mundo

- InVid: plataforma que ofrece diversas herramientas de verificación (disponible en inglés)

- KoboToolbox: herramienta de encuestas para teléfonos móviles que permite tomartestimonios, georreferenciar la información y cargarla en servidores seguros (disponible en inglés)

- Lookup-ID: herramienta para encontrar identificadores de Facebook (disponible en inglés)

- Maltego: herramienta gráfica para descubrir y trazar relaciones entre entidades de interés: personas, cuentas en línea y organizaciones (disponible en inglés)

- Mapillary: aplicación que permite acceder a imágenes a pie de calle y datos cartográficos de todo el mundo (disponible en inglés)

- MARTUS: herramienta de recopilación y gestión de información segura, gratuita y de código abierto

- MAXAR: herramienta que proporciona imágenes por satélite (patentada) (disponible en inglés)

- MediaConch: comprobador de políticas de código abierto (disponible en inglés)

- Mobile justice: aplicación gratuita para grabar reuniones y denunciar abusos (disponible en inglés)

- Mygeoposition.com: herramienta para encontrar la latitud y la longitud (disponible en inglés)

- Neo4J: sistema de gestión de bases de datos gráficos, útil para descubrir patrones y perspectivas en conjuntos de datos complejos (disponible en inglés y francés)

- Nosomosexpedientes.mx [para México]: herramienta digital que apoya a lasfamilias en sus esfuerzos de búsqueda y en la gestión de sus expedientes ante las autoridades nacionales

- Orbital Insights: una herramienta para utilizar los datos de localización (disponible en inglés y japonés)

- PeakVisor: herramienta 3D que permite identificar montañas y picos, útil en geolocalización

- Planet: herramienta que permite acceder a imágenes por satélite (disponible en inglés)

- PhotoDNA: tecnología desarrollada para detectar y eliminar imágenes de explotación infantil (disponible en español dependiendo de la localización)

- QGIS: base de datos geoespacial de código abierto

- SCION: diseñada para proporcionar control de rutas, aislamiento de fallas e información de confianza explícita para la comunicación de extremo a extremo (disponible en inglés)

- Security in a Box: herramientas y tácticas de seguridad digital

- Siegfried: herramienta de identificación de formatos de archivo basada en firmas (disponible en inglés)

- Skynet: plataforma de detección a la distancia (patentada) (disponible en inglés y portugués)

- SUNCALC: aplicación que puede permitir determinar la fecha y hora de la última aparición de una persona desaparecida por la posición del sol y las sombras del día (disponible en inglés)

- TC Slim app: aplicación que permite a los usuarios estudiar la recogida generalizada de datos ocultos en la aplicación móvil (disponible en inglés)

- TerraServer: herramienta de acceso a imágenes de satélite (disponible en inglés)

- Timemap: software de código abierto para visualizar acontecimientos geoespaciales en una plataforma interactiva (disponible en inglés)

- TinEye: herramienta de búsqueda inversa de imágenes (disponible en inglés)

- Toddington international: recursos de investigación gratuitos y de código abierto (disponible en inglés)

- Truecaller: herramienta para rastrear números de teléfono

- TweetBeaver: ofrece varias herramientas, entre ellas descargar y buscar dentro deltimeline de un usuario o descargar la lista de favoritos, amigos o seguidores de un usuario (disponible en inglés)

- TwitterId: herramienta para encontrar IDs de Twitter (disponible en inglés)

- Uwazi: sistema de gestión de contenidos que permite crear un sitio web público o privado para almacenar datos destinados a distintos usos, como la investigación criminal, la defensa de los intereses de los ciudadanos y la generación de información estadística para la investigación (disponible en inglés)

- vframe.io: herramienta que ofrece tecnologías punteras de visión por ordenador para el monitoreo de derechos humanos y de las áreas de conflicto (disponible en inglés)

- Webstagram: herramienta de análisis y seguimiento de cuentas de Instagram (disponible en inglés)

- Wigle: herramienta de cartografía de redes inalámbricas (disponible en inglés)

- Wikimapia: herramienta que consolida múltiples servicios de imágenes por satélite

- Wolfram Alpha: herramienta que permite acceder y comparar información sobre el tiempo y otras (disponible en inglés)

- Yandex Panoramas: herramienta para acceder a imágenes a pie de calle (disponible en inglés)

- Youtube-dl: programa para descargar vídeos de YouTube y otros sitios y plataformas devídeo (disponible en inglés)

- Freedomlab es un lugar de encuentro virtual para las personas defensoras de los derechos humanos, que contiene un repositorio de materiales de formación, tutoriales y herramientas digitales (disponible en inglés, ruso y ucraniano)

- Puede encontrar una lista completa de herramientas para la investigación en línea en el

Bellingcat's Online Investigation Toolkit

- BBC Africa Eye / Forensics Dashboard también ofrece una lista completa de herramientas, conjuntos de datos y otros recursos (disponible en inglés)

- Cada vez hay más herramientas que permiten acceder a imágenes de satélite y detección a distancia, como Google Earth Pro (especialmente útil la herramienta de "imágenes históricas"); Bird.i (disponible en inglés); Sentinel Hub Playground; QGIS; Digital Globe; Imagehunter.

## Instituciones académicas/Programas

- Center for Human Rights Science, Universidad Carnegie Mellon (disponible en inglés)

- Forensic Architecture, agencia de investigación con sede en Goldsmiths, Universidad de Londres (disponible en inglés)

- Humanitarian Research Lab, Universidad de Yale (disponible en inglés)

- Human Rights and Technology programme del Centro de Derechos Humanos de la Universidad de Berkeley (disponible en inglés)

- Human Rights, Big Data and Technology Project de la Universidad de Essex (disponible en inglés)

- The Citizen Lab, laboratorio interdisciplinar con sede en la Munk School of Global Affairs and Public Policy de la Universidad de Toronto (disponible en inglés)

## Recursos

- Amnistía Internacional creó el digital verification corps, es decir, una red de voluntarios formados para verificar datos e información obtenidos a través de investigaciones de código abierto, y publicó una Guía para realizar investigaciones eficaces en línea (partes I, II y III). (disponible en inglés)

- Bellingcat elaboró varias "Guías" de acceso público, entre las que se incluyen *First steps to getting started in open source research*; *A beginner's guide to Social Media verification*; *Unsure when a video or photo was taken? How to tell by measuring the length of shadows*; *Using the sun and the shadows for geolocation*; *Investigate TikTok like a pro!*; *Guide to using reverse image search for investigations*; *A beginner's guide to flight tracking*; *Using phone contact book apps for digital research*, etc.

- Protocolo de Berkeley sobre investigaciones de código abierto digitales, 2020: guía práctica sobre el uso eficaz de la información de fuentes abiertas digitales en la investigación de violaciones del derecho penal internacional, de los derechos humanos y delderecho humanitario.

- How to interpret satellite image: five tips and strategies, por National Areonautics and Space Administration (disponible en inglés)

- Introductory Guide to Open Source Intelligence and Digital Verification por laClínica del Centro de Derechos Humanos de la Universidad de Essex.

- OSR4Rights ofrece una guía de investigación de código abierto para los derechos humanos y tutoriales y herramientas técnicas (por ejemplo, FaceSearch, Knowledge Hub Framework, Hate Speech Detection y el uso del procesamiento del lenguaje natural para identificar las pruebas más relevantes) (disponible en inglés)

- Reference Model for an Open Archival Information System contiene prácticas recomendadas para garantizar la conservación a largo plazo de la información digital. (disponible en inglés)

- Guía de Autodefensa de la Vigilancia de la Electronic Frontier Foundation.

- Manual de verificación: guía para verificar contenidos digitales (disponible en inglés)

- Video as Evidence Field Guide de Witness para ayudar a los usuarios a filmar vídeos para documentar violaciones de los derechos humanos y promover la justicia.

- Véase también la lista no exhaustiva de informes publicados por los Procedimientos Especiales de la ONU relacionados con las nuevas tecnologías.

# Anexo II

## Glosario

**Bot-net**: red de ordenadores privados infectados con malware y controlados en grupo sin el conocimiento de sus propietarios, por ejemplo, para enviar spam.

**Crono-localización**: acto de determinar o estimar un tiempo o marco temporal de un acontecimiento o situación captado por medios visuales.

**Data mining:** proceso de clasificación de grandes conjuntos de datos para identificar patrones y relaciones que puedan ayudar a resolver problemas o preguntas mediante el análisis de datos y generar nueva información.

**Detección a la distancia**: exploración de la Tierra por satélite o avión para obtener información sobre ella.

**Doxxing**: búsqueda y publicación de información privada o identificativa sobre (un individuo concreto) en Internet, normalmente con malas intenciones.

**Fotogrametría**: proceso por el que se combinan varias fotografías fijas de un entorno para crear, mediante triangulación, un modelo 3D.

**Granja de trolls**: organización que emplea a personas para que publiquen deliberadamente mensajes ofensivos, provocadores o contenido en línea, a menudo con información falsa, con el fin de provocar conflictos o manipular a la opinión pública.

**Programa de reconocimiento facial:** tecnología basada en inteligencia artificial utilizada para la identificación, verificación o categorización de datos biométricos.

**Programa de reconocimiento de la marcha:** programa basado en un sistema que utiliza laforma del cuerpo humano y su manera de moverse para identificar a una persona.

**Radar de penetración en el suelo**: método geofísico que utiliza impulsos de radar para obtener imágenes del subsuelo.

**Ransomware**: software malicioso diseñado para bloquear el acceso a un sistema informático hasta que se pague una suma de dinero.

**Regresión cartográfica:** proceso de superposición de mapas históricos y fotografías aéreassobre imágenes contemporáneas para rastrear los cambios en el territorio.

**Spyware**: también denominado "software de intrusión", es un programa malicioso que permite a un operador acceder a un dispositivo objetivo y extraer, modificar o compartir su contenido.