Protocolo de Berkeley

sobre las Investigaciones en Fuentes Abiertas Digitales

Guía práctica sobre la utilización eficaz de información en fuentes abiertas digitales en la investigación de violaciones del derecho penal internacional, el derecho internacional de los derechos humanos y el derecho internacional humanitario

HUMAN RIGHTS CENTER
UC Berkeley School of Law

NACIONES UNIDAS
DERECHOS HUMANOS
OFICINA DEL ALTO COMISIONADO

Protocolo de Berkeley

sobre las Investigaciones en Fuentes Abiertas Digitales

Guía práctica sobre la utilización eficaz de información en fuentes abiertas digitales en la investigación de violaciones del derecho penal internacional, el derecho internacional de los derechos humanos y el derecho internacional humanitario

HUMAN RIGHTS CENTER
UC Berkeley School of Law

NACIONES UNIDAS
DERECHOS HUMANOS
OFICINA DEL ALTO COMISIONADO

Nueva York y Ginebra, 2023

HR/PUB/20/2
ISBN: 978-92-1-154246-2
eISBN: 978-92-1-005345-7
Núm. de venta: S.20.XIV.4

Esta obra es una publicación conjunta de las Naciones Unidas, en nombre de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), y del Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley.

Imagen de portada: imagen *deepfake* de satélite creada por Ahmed Elgamal con la plataforma de inteligencia artificial Playform.

El Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley, agradece la financiación de los siguientes donantes: Sigrid Rausing Trust; Oak Foundation; distintos donantes de la Universidad de California, Berkeley; Open Society Foundations; y Rockefeller Foundation Bellagio Center.

Índice

Prólogo

Desde principios de la década de 1990, las herramientas digitales e Internet, al igual que anteriormente la cámara fotográfica y el teléfono, han revolucionado la forma en que se obtiene, recoge y difunde información sobre violaciones a derechos humanos y otras infracciones graves del derecho internacional, incluyendo crímenes internacionales.

Hoy en día, las personas investigadoras pueden obtener datos sobre posibles violaciones de derechos humanos y otras infracciones graves del derecho internacional, incluidos los crímenes internacionales, de una gran cantidad de imágenes de satélite, videos y fotografías al alcance del público, así como también material subido a Internet desde teléfonos inteligentes y mensajes publicados en plataformas de redes sociales. Esto ha permitido que personas que investigan puedan eludir a los Gobiernos y a otros gestores tradicionales de la información, para acceder a datos esenciales, incluso en tiempo real, que de otro modo no saldrían a la luz.

Sin embargo, la utilización de fuentes abiertas digitales apenas se ha sistematizado, ya que las organizaciones de derechos humanos, los organismos intergubernamentales, mecanismos de investigación y tribunales han tenido que vencer obstáculos para incorporar nuevos métodos digitales de determinación de los hechos y análisis en sus prácticas cotidianas. Uno de los mayores retos que enfrentan es el de encontrar y verificar el material pertinente dentro de un volumen cada vez mayor de información en línea, especialmente fotografías y videos tomados con dispositivos móviles, mismos que pueden estar comprometidos o atribuirse de manera errónea.

Mientras tanto, la aparición de tribunales penales y mecanismos de investigación internacionales, así como de dependencias nacionales dedicadas a investigar los crímenes de guerra, ha aumentado la necesidad de contar con normas comunes sobre la obtención, la preservación y el análisis de la información de fuentes abiertas para poder ser presentada este como medio de prueba en juicios penales. Para que la información de fuentes abiertas sea admisible como medio de prueba en los tribunales, las partes (acusación y defensa) deben demostrar su autenticidad y certificar la cadena de custodia. El manejo y tratamiento adecuados de este material aumentarán en gran medida la probabilidad de que pueda ser utilizado por la acusación y la defensa. Sin embargo, si los métodos de recolección y preservación utilizados no son óptimos, la información no podrá considerarse fiable para establecer los hechos de un caso. Tanto tribunales como los mecanismos de investigación podrán trabajar mejor si disponen de criterios claros para valorar la información de fuentes abiertas, sea como prueba de vinculación o como prueba del delito. El hecho de contar con normas metodológicas comunes sobre la autenticación y la verificación, beneficia también a las misiones de investigación de derechos humanos, que utilizan cada vez más material de fuentes abiertas digitales. Las comisiones de investigación, los componentes de derechos humanos de las operaciones de mantenimiento de la paz, las oficinas sobre el terreno de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) y otros mecanismos de las Naciones Unidas encargados de vigilar e investigar violaciones de derechos humanos, se verán reforzados si cuentan con principios y enfoques metodológicos sólidos para confirmar la validez y el peso de sus conclusiones.

Con el objetivo de atender a esta necesidad, nuestras instituciones —el Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley, y el ACNUDH— han colaborado en la preparación de este *Protocolo de Berkeley sobre las Investigaciones en Fuentes Abiertas Digitales: guía práctica sobre la utilización eficaz de información en fuentes abiertas digitales en la investigación de violaciones del derecho penal internacional, el derecho internacional de los derechos humanos y el derecho internacional humanitario*. El camino que condujo a esta publicación comenzó en el campus de Berkeley en 2009, cuando el Centro de Derechos Humanos reunió a eminencias del derecho, la tecnología y el periodismo, así como activistas, en busca de posibles estrategias que permitieran utilizar las tecnologías y metodologías digitales para sacar a la luz y documentar las violaciones de derechos humanos. Desde entonces, el Centro de Derechos Humanos ha organizado una serie de talleres interdisciplinarios, en colaboración con una serie de especialistas de los ámbitos técnico, jurídico y metodológico del ACNUDH y de otras instituciones, con el fin de intercambiar ideas, crear nuevas herramientas e identificar y definir criterios, normas y métodos para encontrar, evaluar, verificar y preservar información digital de fuentes abiertas que permita documentar las violaciones de derechos humanos y enjuiciar a los autores. Este proceso llegó en un momento oportuno para el ACNUDH, que quería elaborar orientaciones y herramientas para

ayudar y asesorar a las comisiones de investigación y misiones de determinación de los hechos de las Naciones Unidas y al personal del ACNUDH con respecto a su creciente utilización de información de fuentes abiertas en su labor de determinación de los hechos e investigación.

Contribuyeron a este Protocolo de Berkeley personas de diversos ámbitos profesionales, tradiciones jurídicas y culturales, géneros y nacionalidades, se realizaron más de 150 consultas con especialistas y se recibieron aportes de actores clave, entre ellos investigadores e investigadoras de derechos humanos de las Naciones Unidas. El Protocolo se inspira también en la experiencia de los grupos de trabajo especializados de la Sección de Metodología, Educación y Capacitación del ACNUDH y de la Fiscalía de la Corte Penal Internacional. De acuerdo con las normas internacionales sobre la creación de una nueva metodología, el ACNUDH y el Centro de Derechos Humanos llevaron a cabo un riguroso proceso de examen, revisión y validación del Protocolo de Berkeley.

Sobre la base de esta colaboración, el Protocolo de Berkeley incluye normas internacionales para realizar investigaciones en línea de presuntas violaciones del derecho internacional de los derechos humanos, el derecho internacional humanitario y el derecho penal internacional. También proporciona orientación sobre posibles metodologías y procedimientos para recoger, analizar y preservar la información digital de manera profesional, legal y ética. Por último, el Protocolo de Berkeley presenta una serie de medidas que las personas que investigan en línea pueden adoptar para proteger su seguridad digital, física y psicosocial y la de otras personas —como las que son testigos o víctimas y las que informan primero sobre los hechos (por ejemplo, miembros de la ciudadanía, activistas y periodistas)— que se arriesgan para documentar las violaciones de derechos humanos y las infracciones graves del derecho internacional.

El Protocolo de Berkeley sigue los pasos de dos protocolos anteriores de las Naciones Unidas: el Protocolo de Minnesota sobre la Investigación de Muertes Potencialmente Ilícitas (1991, actualizado en 2016) y el *Manual para la investigación y documentación eficaces de la tortura y otros tratos o penas crueles, inhumanos o degradantes* (Protocolo de Estambul) (1999, actualizado en 2004). El Protocolo de Minnesota, elaborado por juristas y forenses que habían participado en la búsqueda de personas desaparecidas en la década de 1980, establece normas y procedimientos internacionales para realizar investigaciones médico-legales de las muertes sospechosas o descubiertas después de mucho tiempo, método utilizado para evaluar la credibilidad de dichas investigaciones. Del mismo modo, el Protocolo de Estambul ayuda al personal médico y jurídico a reconocer y documentar las secuelas físicas y psicosociales de la tortura, de modo que la documentación pueda servir como prueba válida en los tribunales o en otros contextos, incluidas las investigaciones de derechos humanos y la labor de vigilancia en la materia. El punto de partida de los tres protocolos es el convencimiento de que la ciencia, la tecnología y el derecho pueden —y deben— trabajar juntos, al servicio de los derechos humanos. Al igual que los protocolos anteriores, el Protocolo de Berkeley se publicará en las lenguas oficiales de las Naciones Unidas para facilitar su uso y su utilidad en todo el mundo.

Confiamos en que, en un mundo cada vez más digitalizado, el Protocolo de Berkeley ayudará a las personas que investigan en línea —juristas, defensores y defensoras de los derechos humanos, periodistas u otras personas— a elaborar y aplicar procedimientos eficaces para documentar y verificar las violaciones del derecho internacional de los derechos humanos, el derecho internacional humanitario y el derecho penal internacional, aprovechando al máximo la información digital de fuentes abiertas, para que las personas responsables de dichas violaciones puedan ser enjuiciadas de manera justa.

Eric Stover
Director Docente del Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Michelle Bachelet
Alta Comisionada de las Naciones Unidas para los Derechos Humanos

Resumen

Las investigaciones en fuentes abiertas son investigaciones que utilizan, total o parcialmente, información al alcance del público para indagar en línea, de manera formal y sistemática, sobre presuntas infracciones. Hoy en día se pueden encontrar en Internet grandes cantidades de información al alcance del público. Este nuevo panorama digital, en constante y rápida evolución, ha dado lugar a nuevos tipos de información y fuentes que pueden ayudar a investigar presuntas violaciones de derechos humanos y graves crímenes internacionales. La posibilidad de realizar ese tipo de investigaciones es especialmente valiosa para el personal investigador que no puede acceder rápidamente al lugar de los hechos, lo que suele ocurrir en el caso de las investigaciones internacionales.

La información de fuentes abiertas puede proporcionar indicios, corroborar datos de inteligencia y servir de prueba directa en los tribunales de justicia. Sin embargo, para que pueda utilizarse en los procesos de investigación formales, incluidas las investigaciones judiciales, las misiones de determinación de los hechos y las comisiones de investigación, el personal investigador debe emplear métodos coherentes que refuercen la exactitud de sus conclusiones y permitan a los tribunales y a sus pares evaluar la calidad del propio proceso de investigación. El Protocolo de Berkeley sobre las Investigaciones en Fuentes Abiertas Digitales se elaboró con el objetivo de proporcionar una serie de normas y orientaciones internacionales a las personas que investigan en los ámbitos de la justicia penal internacional y de los derechos humanos. Esas personas proceden de diversas instituciones, como medios de comunicación, grupos de la sociedad civil y organizaciones no gubernamentales, organizaciones internacionales, tribunales y organismos de investigación nacionales e internacionales. El establecimiento de una serie de normas coherentes y mensurables para contribuir a este ámbito multidisciplinar es una forma de profesionalizar la práctica de las investigaciones en fuentes abiertas.

Si bien es cierto que las directrices y la capacitación sobre la utilización de determinadas herramientas y programas computacionales son esenciales para mejorar la calidad de las investigaciones en fuentes abiertas digitales, el Protocolo de Berkeley no se centra en tecnologías, plataformas, programas computacionales o herramientas concretas, sino en una serie de principios subyacentes y metodologías que puedan aplicarse de forma constante, aunque la propia tecnología evolucione. En esos principios se sustentan las normas legales y éticas mínimas para realizar investigaciones eficaces en fuentes abiertas. Las personas investigadoras podrán seguir las orientaciones del Protocolo de Berkeley para asegurar la calidad de su trabajo al tiempo que minimizan los riesgos físicos, psicosociales y digitales para si mismas y para otras personas.

El Protocolo de Berkeley está concebido como una herramienta pedagógica y una guía de referencia para las personas que realizan investigaciones en fuentes abiertas. Después de un primer capítulo introductorio, los tres siguientes están dedicados a las cuestiones generales de los principios, las consideraciones legales y la seguridad. Los capítulos restantes se centran en el proceso de investigación propiamente dicho. Esa última sección del Protocolo de Berkeley comienza con un capítulo sobre la preparación y la planificación estratégica, seguido de uno dedicado a las distintas etapas de investigación necesarias, a saber, las indagaciones en línea, la evaluación preliminar, la recogida, la preservación, la verificación y el análisis investigativo. Concluye con un capítulo sobre la metodología y los principios para presentar los resultados de una investigación con fuentes abiertas.

Contribuciones y colaboraciones

Comité Coordinador del Protocolo de Berkeley

Lindsay Freeman, Investigadora Jurídica Sénior del Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Alexa Koenig, Directora Ejecutiva del Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Eric Stover, Director Docente del Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Comité de Redacción del Protocolo de Berkeley

Sareta Ashraph, Consultora Jurídica Sénior; Abogada del bufete Garden Court Chambers; antigua Analista Superior del Equipo de Investigaciones de las Naciones Unidas para Promover la Rendición de Cuentas por los Crímenes del Estado Islámico en el Iraq y el Levante/Dáesh

Alix Dunn, Directora Ejecutiva de The Engine Room

Richard Goldstone, previo Magistrado del Tribunal Constitucional de Sudáfrica; antiguo Jefe de la Fiscalía del Tribunal Internacional para la ex-Yugoslavia y del Tribunal Penal Internacional para Rwanda

Brenda J. Hollis, Fiscal Internacional de las Salas Especiales de los Tribunales de Camboya; previa Jefa de la Fiscalía del Tribunal Especial Residual para Sierra Leona

Tanya Karanasios, Directora de Programas de WITNESS

Enrique Piracés, Director del Programa de Medios de Comunicación y Derechos Humanos del Centro para la Ciencia de los Derechos Humanos de la Universidad Carnegie Mellon

Beth Van Schaack, Profesora Invitada de Derechos Humanos de la Facultad de Derecho de la Universidad Stanford; antigua Adjunta del Embajador en Misión Especial para los Crímenes de Guerra de la Oficina de Justicia Penal Global del Departamento de Estado de los Estados Unidos

Michel de Smedt, Director de la División de Investigaciones de la Fiscalía de la Corte Penal Internacional

Alan Tieger, Fiscal Superior de la Fiscalía Especializada de Kosovo; antiguo Fiscal Auxiliar Principal del Tribunal Internacional para la ex-Yugoslavia

Christian Wenaweser, Representante Permanente de Liechtenstein ante las Naciones Unidas; antiguo Presidente de la Asamblea de los Estados Partes del Estatuto de Roma de la Corte Penal Internacional

Alex Whiting, Jefe de Investigaciones de la Fiscalía Especializada de Kosovo; Profesor de Práctica de la Facultad de Derecho de la Universidad de Harvard; antiguo Coordinador de Acusación y Coordinador de Investigaciones de la Fiscalía de la Corte Penal Internacional

Susan Wolfinbarger, Oficial de Relaciones Exteriores y Jefa del Equipo de Análisis del Departamento de Estado de los Estados Unidos; antigua Directora Superior del Proyecto de Tecnologías Geoespaciales de la Asociación Estadounidense para el Progreso de la Ciencia

Comité Asesor del Protocolo de Berkeley

Federica D'Alessandra, Directora Ejecutiva del Programa sobre la Paz y la Seguridad Internacionales de la Universidad de Oxford; editora del *Handbook on Civil Society Documentation of Serious Human Rights Violations: Principles & Best Practices*, publicado por el Public International Law and Policy Group

Stuart Casey-Maslen, Profesor *Honoris Causa* de la Facultad de Derecho de la Universidad de Pretoria; coautor del Protocolo de Minnesota sobre la Investigación de Muertes Potencialmente Ilícitas (2016)

Alison Cole, Asesora Especialista en Derechos Humanos del Departamento de Asuntos Internos de Nueva Zelandia

Francoise Hampson, Profesora Emérita de la Facultad de Derecho de la Universidad de Essex; miembro de la Comisión de Investigación sobre Burundi

Christof Heyns, Profesor de Derecho de los Derechos Humanos de la Universidad de Pretoria; miembro del Comité de Derechos Humanos; antiguo Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias; coordinador del Protocolo de Minnesota sobre la Investigación de Muertes Potencialmente Ilícitas (2016)

Vincent Iacopino, Asesor Médico Superior de Physicians for Human Rights; coautor principal del *Manual para la investigación y documentación eficaces de la tortura y otros tratos o penas crueles, inhumanos o degradantes* (Protocolo de Estambul)

Kelly Matheson, Abogada Superior y Directora de Programas de WITNESS; autora de *Video as Evidence Field Guide*

Hanny Megally, Miembro de la Comisión Internacional Independiente de Investigación sobre la República Árabe Siria; Investigador Asociado Superior del Centro sobre la Cooperación Internacional de la Universidad de Nueva York (NYU)

Juan Méndez, Profesor Visitante de Derecho de los Derechos Humanos del Washington College of Law; antiguo Relator Especial sobre la tortura y otros tratos o penas crueles, inhumanos o degradantes; coordinador del protocolo universal para las entrevistas de investigación y las garantías procesales

Aryeh Neier, Presidente Emérito de Open Society Foundations

Navi Pillay, Presidenta de la Comisión Internacional contra la Pena de Muerte; antigua Alta Comisionada de las Naciones Unidas para los Derechos Humanos; antigua Magistrada de la Corte Penal Internacional; antigua Presidenta del Tribunal Penal Internacional para Rwanda

Paulo Sérgio Pinheiro, Presidente de la Comisión Internacional Independiente de Investigación sobre la República Árabe Siria; antiguo Relator Especial sobre la situación de los derechos humanos en Burundi; antiguo Relator Especial sobre la situación de los derechos humanos en Myanmar

Thomas Probert, Profesor Extraordinario del Centro de Derechos Humanos de la Universidad de Pretoria; Investigador Asociado del Centro de Gobernanza y Derechos Humanos de la Universidad de Cambridge; coautor del Protocolo de Minnesota sobre la Investigación de Muertes Potencialmente Ilícitas (2016)

Stephen Rapp, Miembro Distinguido del Centro Simon-Skjodt para la Prevención del Genocidio del Museo Conmemorativo del Holocausto de los Estados Unidos; antiguo Embajador en Misión Especial para los Crímenes de Guerra de la Oficina de Justicia Penal Global del Departamento de Estado de los Estados Unidos; antiguo Fiscal del Tribunal Especial para Sierra Leona

Cristina Ribeiro, Coordinadora de Investigaciones de la Fiscalía de la Corte Penal Internacional

Patricia Sellers, Asesora Especial sobre Género de la Fiscalía de la Corte Penal Internacional; Investigadora Visitante del Kellogg College de la Universidad de Oxford; antigua Asesora Jurídica y Fiscal del Tribunal Internacional para la ex-Yugoslavia y del Tribunal Penal Internacional para Rwanda

Participantes en los talleres

"Taller sobre la nueva ciencia forense: la investigación de delitos graves sobre la base de información de fuentes abiertas" (Bellagio, Italia, 2017)

Hadi Al Khatib, Syrian Archive

Stuart Casey-Maslen, Universidad de Pretoria

Yvan Cuypers, Corte Penal Internacional

Scott Edwards, Amnistía Internacional

Lindsay Freeman, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Alexa Koenig, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Steve Kostas, Open Society Justice Initiative

Andrea Lampros, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Kelly Matheson, WITNESS

Félim McMahon, Corte Penal Internacional

Julian Nicholls, Corte Penal Internacional

Thomas Probert, Universidad de Cambridge

Cristina Ribeiro, Corte Penal Internacional

Gavin Sheridan, Vizlegal

Eric Stover, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Alan Tieger, Tribunal Internacional para la ex-Yugoslavia

Mark Watson, Commission for International Justice and Accountability

Guy Willoughby, Association for the Study of War Crimes

"Taller sobre la construcción de un marco ético para las investigaciones en fuentes abiertas" (Universidad de Essex (Reino Unido), 2019)

Fred Abrahams, Human Rights Watch

Leenah Bassouni, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Federica D'Alessandra, Universidad de Oxford

Sam Dubberley, Amnistía Internacional

Jennifer Easterday, JustPeace Labs

Scott Edwards, Amnistía Internacional

Lindsay Freeman, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Geoff Gilbert, Universidad de Essex

Christopher "Kip" Hale, Commission for International Justice and Accountability

Evanna Hu, Omelas

Gabriela Ivens, Investigadora de Mozilla y WITNESS

Alexa Koenig, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Matt Mahmoudi, Universidad de Cambridge

Lorna McGregor, Universidad de Essex

Daragh Murray, Universidad de Essex

Vivian Ng, Universidad de Essex

Enrique Piracés, Centro para la Ciencia de los Derechos Humanos de la Universidad Carnegie Mellon

Zara Rahman, The Engine Room

Sasha Robehmed, The Engine Room

Ilia Siatitsa, Privacy International

Representante del ACNUDH, de la Sección de Metodología, Educación y Capacitación

"Mesa redonda sobre las cuestiones jurídicas derivadas de las investigaciones en fuentes abiertas" (La Haya, 2019)

David Akerson, Equipo de Investigaciones de las Naciones Unidas para Promover la Rendición de Cuentas por los Crímenes del Estado Islámico en el Iraq y el Levante/Dáesh

Sareta Ashraph, Garden Court Chambers

Danya Chaikel, Fiscalía Especializada de Kosovo

Alan Clark, Corte Penal Internacional

Federica D'Alessandra, Universidad de Oxford

Nico Dekens, Bellingcat

Chris Engels, Commission for International Justice and Accountability

Lindsay Freeman, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Emma Irving, Universidad de Leiden

Michelle Jarvis, Mecanismo Internacional, Imparcial e Independiente para Ayudar en la Investigación y el Enjuiciamiento de los Responsables de los Delitos de Derecho Internacional Más Graves Cometidos en la República Árabe Siria desde Marzo de 2011

Edward Jeremy, Corte Penal Internacional

Ashley Jordana, Global Rights Compliance

Sang-Min Kim, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Alexa Koenig, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Nicholas Koumjian, Mecanismo Independiente de Investigación para Myanmar

Bastiaan Van Der Laaken, Mecanismo Internacional, Imparcial e Independiente para Ayudar en la Investigación y el Enjuiciamiento de los Responsables de los Delitos de Derecho Internacional Más Graves Cometidos en la República Árabe Siria desde Marzo de 2011

Dearbhla Minogue, Global Legal Action Network

Nick Ortiz, Universidad de Leiden

Matevz Pezdirc, Red sobre el Genocidio de la Agencia de la Unión Europea para la Cooperación Judicial Penal

Sanja Popovic, Fiscalía Especializada de Kosovo

Steven Powles, Doughty Street Chambers; Comité de Crímenes de Guerra de la International Bar Association

Stephen Rapp, Centro Simon-Skjodt para la Prevención del Genocidio del Museo Conmemorativo del Holocausto de los Estados Unidos

Cristina Ribeiro, Corte Penal Internacional

Mark Robson, Commission for International Justice and Accountability

Brad Samuels, SITU Research

Dalila Seoane, Civitas Maxima

Carsten Stahn, Universidad de Leiden

Melinda Taylor, Corte Penal Internacional

Alan Tieger, Fiscalía Especializada de Kosovo

Raquel Vázquez Llorente, eyeWitness to Atrocities

Especialistas adicionales

Elise Baker, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Sean Brooks, Centro de Ciberseguridad Duradera de la Universidad de California, Berkeley

Stephanie Croft, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Sam Dubberley, Amnistía Internacional

Thomas Ewing, The Center for Advanced Defense Studies

Christopher "Kip" Hale, Commission for International Justice and Accountability

Gabriela Ivens, Human Rights Watch

Felim McMahon, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Daragh Murray, Universidad de Essex

Yvonne Ng, WITNESS

Zara Rahman, The Engine Room

Mark Robson, Commission for International Justice and Accountability

Justin Seitz, Hunchly

Andrea Trewinnard, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley

Steve Trush, Centro de Ciberseguridad Duradera de la Universidad de California, Berkeley

Raquel Vázquez Llorente, eyeWitness to Atrocities

Reconocimiento especial

Los autores desean agradecer de manera especial a los miembros del Grupo de Trabajo de Investigaciones en Línea de la Fiscalía de la Corte Penal Internacional.

Asimismo, reconocen al gran número de colegas del ACNUDH cuya labor ha permitido hacer realidad esta publicación conjunta*.

* De acuerdo con la política del ACNUDH, las contribuciones a sus publicaciones no se atribuyen personalmente a ningún miembro de su personal.

Siglas y acrónimos

ACNUDH	Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos
CICR	Comité Internacional de la Cruz Roja
HTML	Lenguaje de Marcación de Hipertexto
IP	Protocolo Internet
ONG	organización no gubernamental
PDF	formato de documento portátil
PSI	proveedor de servicios de Internet
TIC	tecnología(s) de la información y las comunicaciones
URI	identificador uniforme de recursos
URL	localizador uniforme de recursos
VPN	red privada virtual

1

INTRODUCCIÓN

RESUMEN DEL CAPÍTULO

- Objetivo
- Público
- Definiciones

1. El Protocolo de Berkeley sobre las Investigaciones Digitales en Fuentes Abiertas describe las normas profesionales que deben seguirse en las tareas de identificación, recolección, preservación, análisis y presentación de información de fuentes abiertas digitales y al utilizar esa información en las investigaciones penales y de derechos humanos internacionales. La información de fuentes abiertas es la información que cualquier particular puede observar, adquirir o solicitar, sin necesidad de tener una categoría jurídica especial y sin acceder ilegalmente a ella. La información digital de fuentes abiertas es la información al alcance del público en formato digital, a la que generalmente se accede en Internet. La información de fuentes abiertas digitales comprende tanto los datos generados por los usuarios como los generados por máquinas, y puede incluir, por ejemplo: contenidos publicados en las redes sociales; documentos, imágenes, videos y grabaciones sonoras disponibles en sitios web y en plataformas de intercambio de información; imágenes de satélite; y datos publicados por los Estados[1]. Las investigaciones en fuentes abiertas digitales son investigaciones en las que se utiliza información digitales de fuentes abiertas. Para facilitar la lectura, en el Protocolo se hablará en lo sucesivo de "información de fuentes abiertas" para referirse a la información digital procedente de dichas fuentes y de "investigaciones en fuentes abiertas" para referirse a las investigaciones digitales de ese tipo.

2. Aunque la utilización de información de fuentes abiertas en las investigaciones no es nueva, el volumen y la diversidad de las fuentes abiertas se han multiplicado con el uso cada vez mayor de Internet y otros recursos digitales para intercambiar información, y en particular con la proliferación de las redes sociales. El Protocolo es una respuesta tanto a las complejidades que surgen cuando se trabaja con información digital como a las dificultades especiales que conlleva la evaluación de las fuentes y la verificación de la información encontrada en foros abiertos en línea.

3. Si bien en un número cada vez mayor de investigaciones sobre infracciones del derecho penal internacional y el derecho internacional de los derechos humanos se utiliza Internet para facilitar el trabajo, no existen actualmente referencias, directrices o normas universales para las investigaciones en fuentes abiertas. Con el Protocolo se trata de colmar esa laguna estableciendo principios y prácticas que ayuden a las personas que investigan a realizar su trabajo con profesionalidad y faciliten, en su caso, la preservación de la información de fuentes abiertas por si pudiera utilizarla algún mecanismo judicial.

4. El Protocolo se centra específicamente en las investigaciones en fuentes abiertas efectuadas con el fin de que se haga justicia y se establezca la rendición de cuentas a nivel internacional en general, en ámbitos como: las iniciativas de documentación, preservación, recogida de pruebas y determinación de los hechos sobre violaciones de derechos humanos; las comisiones de investigación y misiones de determinación de los hechos[2]; otros tipos de investigaciones e indagaciones establecidas por mandato internacional[3]; los procesos de verdad y reconciliación; litigios civiles; y juicios penales, incluidos los procedimientos penales internacionales. Dado que las investigaciones en fuentes abiertas pueden contribuir a diferentes tipos de iniciativas destinadas a

1 Esta lista no es exhaustiva.

2 Las comisiones de investigación y las misiones de determinación de los hechos son órganos que pueden ser creados por Gobiernos u organizaciones internacionales para indagar sobre diversas cuestiones. Las comisiones de investigación o las misiones de determinación de los hechos informan sobre los hechos comprobados, extraen conclusiones jurídicas y formulan recomendaciones. Aunque las conclusiones de las comisiones de investigación o misiones de determinación de los hechos internacionales no son jurídicamente vinculantes, pueden ser muy influyentes. Sin embargo, las conclusiones de las comisiones nacionales de investigación pueden ser vinculantes en algunas jurisdicciones. Para más información sobre las comisiones de investigación y las misiones de determinación de los hechos internacionales, véase Consejo de Derechos Humanos, "Comisiones de investigación, misiones de determinación de los hechos y otras investigaciones". Disponible en www.ohchr.org/es/HRBodies/HRC/Pages/COIs.aspx.

3 Véase, por ejemplo, el informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos sobre la situación de los derechos humanos en la República Bolivariana de Venezuela (A/HRC/41/18), presentado de conformidad con la resolución 39/1 del Consejo de Derechos Humanos. Véase también la resolución 41/2 del Consejo, en la que este solicitó a la Alta Comisionada que preparara un informe sobre la situación de los derechos humanos en Filipinas.

establecer rendición de cuentas[4], la metodología y los requisitos de documentación descritos en el Protocolo pueden ser más rigurosos que los empleados tradicionalmente en otros campos, como el periodismo y la defensa de los derechos humanos. Cualquiera que sea el objetivo de la investigación, la observancia de los principios metodológicos establecidos en el Protocolo —que se apoyan en normas jurídicas comunes— garantizará a las personas que investigan en fuentes abiertas la alta calidad de su trabajo e incrementará la posibilidad de que la información recolectada sea utilizada en cortes, tribunales y otros procesos judiciales.

5. Además, el Protocolo establece normas para investigar violaciones del derecho internacional —incluidas las violaciones de derechos humanos— y violaciones del derecho penal internacional, como los crímenes de guerra, crímenes de lesa humanidad y genocidio, pero también puede utilizarse como guía en otros tipos de investigaciones, como aquellas realizadas para tribunales nacionales o municipales.

6. En última instancia, el Protocolo pretende ayudar a las personas que investigan en fuentes abiertas a realizar su trabajo aplicando una metodología profesional que sea ampliamente conforme con los requisitos legales y las normas éticas. Con él también se busca ayudar a quienes utilizan el resultado de la investigación (juristas, tribunales y otras instancias decisorias) a comprender y evaluar mejor las técnicas de investigación en fuentes abiertas. El Protocolo también pretende ser un recurso para especialistas en la materia y una herramienta de formación y enseñanza para quienes deseen aprender a realizar investigaciones en fuentes abiertas sobre presuntas violaciones del derecho internacional[5].

A. Objetivo

7. Si bien el personal investigador lleva mucho tiempo recurriendo a la información de fuentes abiertas, su utilización sistemática se aceleró a principios y mediados del siglo XX, cuando se extraía información de emisiones de radio y periódicos impresos extranjeros[6]. Con la introducción de la World Wide Web en la década de 1990, preludio de la popularización de las redes sociales y los teléfonos inteligentes en la de 2000, la cantidad y la calidad de la información de fuentes abiertas han evolucionado drásticamente. Hoy en día, cualquier persona que tenga un teléfono inteligente y acceso a Internet puede crear y distribuir contenidos digitales en todo el mundo, aunque con distintos grados de calidad, veracidad y transparencia. El creciente volumen de datos y la velocidad con que estos se transmiten y divulgan, han creado nuevas oportunidades para que la personas que investigan en fuentes abiertas recopilen y analicen información sobre crímenes internacionales y violaciones de derechos humanos. Ahora bien, las personas creadoras de contenido también son ahora capaces de difundir desinformación y manipular datos digitales con relativa facilidad. Con el Protocolo se intenta dar una respuesta a esta nueva realidad y a la complejidad inherente a estas oportunidades y dificultades.

8. La información de fuentes abiertas es útil en todo tipo de investigaciones, pero desempeña una función especialmente crítica en las investigaciones relativas al derecho penal internacional y al derecho internacional de los derechos humanos. Esto se debe a una serie de razones. En primer lugar, las investigaciones establecidas por mandato internacional, como las realizadas por las comisiones de investigación y las misiones de determinación

[4] Por ejemplo, la misión internacional independiente de investigación sobre Myanmar utilizó información de fuentes abiertas, junto con fuentes de primera mano y otra información, en su proceso de verificación y en sus observaciones y conclusiones. El informe final de la misión de investigación (A/HRC/42/50) fue uno de los factores que condujeron a la creación, por el Consejo de Derechos Humanos, del Mecanismo Independiente de Investigación para Myanmar, al que se encomendó el mandato de realizar investigaciones judiciales. Además, se ordenó a la misión de investigación que entregara al Mecanismo Independiente de Investigación para Myanmar la información que había recogido, incluidos los resultados de sus investigaciones en fuentes abiertas. Los informes de la misión de investigación también se utilizaron en la causa que Gambia presentó contra Myanmar ante la Corte Internacional de Justicia por la violación de la Convención para la Prevención y la Sanción del Delito de Genocidio. Esto demuestra que la información recogida con una finalidad puede acabar contribuyendo a otro proceso judicial.

[5] El Protocolo también proporciona una serie de modelos para las investigaciones en fuentes abiertas, así como un glosario (véase el cap. VIII).

[6] Nikita Mehandru y Alexa Koenig, "ICTs, social media, & the future of human rights", *Duke Law & Technology Review*, vol. 17, núm. 1, pág. 129.

de hechos de las Naciones Unidas, o las autorizadas por la Corte Penal Internacional, dependen de los procesos legales y políticos que permiten que las mismas sucedan[7]. Por lo tanto, a menudo se llevan a cabo mucho tiempo después de que ocurran los hechos. En segundo lugar, muchas investigaciones internacionales no tienen acceso al lugar físico en que ocurrieron los hechos investigados, por ejemplo cuando el Estado se niega a cooperar o a permitir dicho acceso. En tercer lugar, aun cuando los equipos de investigación pueden acceder a la región o territorio, a veces su acceso físico al lugar en cuestión es limitado, o no pueden realizar investigaciones *in situ* ni entrevistas en persona por motivos de seguridad. Por último, en la mayoría de esas investigaciones, las personas que las realizan no tienen plena facultad para hacer cumplir la ley en los territorios en que se cometieron los presuntos delitos o infracciones, por lo que les puede resultar imposible recoger la información necesaria. Aun en los casos en que se cuenta con la cooperación del Estado, el levantamiento de pruebas en un país extranjero puede ser un proceso arduo, ralentizado por onerosos trámites burocráticos. Todos estos factores demuestran por qué las técnicas de investigación en fuentes abiertas, que pueden llevarse a cabo a distancia y en el momento en que ocurren los hechos, son tan potentes como necesarias.

9. El Protocolo está destinado a un grupo diverso de personas que investigan en diferentes contextos con mandatos, facultades y recursos diversos. Por lo tanto, adopta un enfoque flexible, es decir, no se pretende que todas esas personas realicen su trabajo de forma idéntica, sino que adapten las metodologías a su entorno de trabajo concreto. Además, dado que las tecnologías, herramientas y técnicas que ayudan a las investigaciones en fuentes abiertas evolucionan constantemente, el Protocolo no se centra en tecnologías, plataformas, sitios web, programas computacionales o fuentes concretas, que pueden cambiar con el tiempo, sino en los principios y procedimientos subyacentes que deben guiar las investigaciones en fuentes abiertas.

10. El Protocolo está diseñado para estandarizar procedimientos y proporcionar orientaciones metodológicas a las distintas investigaciones, instituciones y jurisdicciones para ayudar a las personas que realizan investigaciones en fuentes abiertas a comprender la importancia de:

    a) Rastrear la procedencia de los contenidos en línea y atribuirlos a su fuente original, siempre que sea posible;

    b) Evaluar la credibilidad y fiabilidad de las fuentes en línea;

    c) Verificar los contenidos en línea y evaluar su veracidad y su fiabilidad;

    d) Actuar de conformidad con los requisitos legales y las normas éticas;

    e) Minimizar cualquier riesgo de daño para las personas investigadoras, sus organizaciones y otras partes;

    f) Contribuir a la protección de los derechos humanos de las fuentes, incluido el derecho a la privacidad.

B. Público

11. El Protocolo está destinado a las personas y organizaciones que identifican, recogen, preservan o analizan información de fuentes abiertas digitales para investigar crímenes internacionales o violaciones de derechos humanos con el fin de que se haga justicia y se atribuyan responsabilidades legales. Se trata de personas investigadoras, juristas, archivistas y analistas que trabajan para tribunales penales internacionales, regionales e híbridos; dependencias nacionales dedicadas a los crímenes de guerra; comisiones de investigación; misiones de determinación de hechos; mecanismos de investigación independientes; organizaciones internacionales; mecanismos de justicia transicional; y organizaciones no gubernamentales (ONG). Otras personas a las que el Protocolo podría resultarles útil son aquellas que trabajan para diversos mecanismos internacionales y regionales que llevan a cabo investigaciones judiciales y cuasijudiciales en fuentes abiertas sobre violaciones del derecho

[7] Han establecido comisiones de investigación y misiones de determinación de los hechos de las Naciones Unidas, entre otros, el Consejo de Seguridad, la Asamblea General, el Consejo de Derechos Humanos y el Secretario General. En el caso de la Corte Penal Internacional, la Fiscalía puede iniciar investigaciones a petición de los Estados partes o del Consejo de Seguridad, o por iniciativa propia y con la autorización de los magistrados y magistradas de la Corte.

internacional[8]. El Protocolo también puede ser instructivo para activistas digitales como las organizaciones locales, así como para investigadores e investigadoras independientes quienes suelen ser los primeros en publicar hallazgos basados en información de fuentes abiertas, y cuyo trabajo suele tener un papel crucial en la instauración de investigaciones de fuentes abiertas formalmente establecidas. El público destinatario también incluye a las personas y organizaciones que ayudan a víctimas a presentar demandas contra los autores particulares o los Estados. El Protocolo también puede ser de ayuda en general para quienes extraen conclusiones fácticas o jurídicas de las investigaciones en fuentes abiertas, permitiéndoles evaluar mejor el contenido de las investigaciones en que se funden o que evalúen.

12. Otras partes posiblemente interesadas en el Protocolo son los proveedores de servicios digitales, como las plataformas de redes sociales, que almacenan grandes volúmenes de datos y pueden desempeñar un papel clave en su preservación, así también como para quienes crean programas computacionales para reforzar técnicas y procesos de investigación en fuentes abiertas.

C. Definiciones

13. Con el fin de proporcionar normas y orientaciones prácticas para las investigaciones en fuentes abiertas, las personas que realizan dichas investigaciones deben interpretar una serie de términos específicos de manera uniforme. En esta sección se aclaran los principales términos utilizados en el Protocolo y se hace distinción entre términos que suelen confundirse[9].

1. Información de fuentes abiertas e información de fuentes cerradas

14. La información de fuentes abiertas es la información al alcance del público que cualquier particular puede observar, adquirir o solicitar sin necesidad de tener una categoría jurídica especial y sin acceder a ella ilegalmente. La información de fuentes cerradas es información de acceso restringido o protegido por ley[10] pero que puede obtenerse legalmente por procesos privados, como procedimientos judiciales, o ser ofrecida de forma voluntaria. A pesar de esta sencilla definición, el determinar lo que constituye información de fuentes abiertas es más complicado de lo que parece inicialmente en el contexto de contenidos en línea. En Internet hay un volumen creciente de datos que se han hecho públicos sin el consentimiento de sus propietarios, como la información que ha sido pirateada, filtrada, divulgada por fallos de seguridad o publicada sin permiso por terceros. Aunque esta información está al alcance del público y, por lo tanto, técnicamente se considera de fuentes abiertas, puede haber restricciones legales y éticas respecto de ciertos tipos de uso final. Además, hay información digital que solo está al alcance de personas con formación y conocimientos técnicos especializados, mismas que pueden acceder a redes y datos inaccesibles o de acceso muy poco probable para cualquier persona[11]. Un ejemplo de ello es la información que solo puede obtenerse en la web oscura, es decir, la parte de Internet a la que solo se puede acceder con determinados programas, como el navegador Tor[12]. Aunque la web oscura ofrece anonimato y, por ello, ha atraído diversas actividades ilegales, el uso del navegador Tor y la búsqueda de información en la web oscura es legal en la mayoría de los países. El Protocolo incluye esta información en la categoría de información "de fuentes abiertas" siempre que no se acceda a ella sin autorización. La diferencia más clara entre

8 Véanse, por ejemplo, las comunicaciones y los informes relativos a visitas de los procedimientos especiales del Consejo de Derechos Humanos. Disponibles en www.ohchr.org/es/hrbodies/sp/pages/welcomepage.aspx. Véase también la labor de los comités de sanciones creados por el Consejo de Seguridad. Disponible en www.un.org/securitycouncil/es/content/repertoire/sanctions-and-other-committees.

9 Para una lista más completa de términos y definiciones pertinentes, véase el cap. VIIII.

10 Por ejemplo, información reservada o confidencial.

11 Algunos actos pueden infringir las condiciones de utilización de un sitio web pero no ser ilegales en sí mismos. Por ejemplo, si un usuario de un sitio web incumple las condiciones de utilización para raspar datos *(scraping)*, incurre en un comportamiento no autorizado y puede resultar vetado de dicho sitio web.

12 Se llama "web oscura" a la parte de Internet a la que solo se puede acceder con programas computacionales especializados. El navegador Tor es uno de esos programas.

ambos conceptos reside en el hecho de que para acceder a la información de fuentes abiertas no es necesario interactuar ni solicitar información a ningún usuario de Internet[13]. La información que se obtiene de otros usuarios de Internet comunicándose previamente con ellos se considera información de fuentes cerradas.

15. La información de fuentes abiertas digitales[14] es información en línea de fuentes abiertas a la que se puede acceder, por ejemplo, en sitios web públicos, bases de datos de Internet o plataformas de redes sociales. A continuación se describen diferentes formas de obtener información de fuentes abiertas.

2. Obtención de información de fuentes abiertas digitales

a) Observar

16. El contenido de muchas plataformas se puede obtener simplemente visitando el sitio en cuestión con cualquier navegador gratuito. Para acceder a otro tipo de plataformas en línea y ver sus contenidos, los usuarios deben conectarse o registrarse. Estos contenidos se consideran información de fuentes abiertas siempre que los procesos mencionados estén abiertos a todos los usuarios ubicados en jurisdicciones en las que el acceso sea legal, y no se infrinjan controles de privacidad o de seguridad al acceder al sitio o al verlos. Sin embargo, hay algunos contenidos que entran dentro de esta definición pero no pueden considerarse información de fuentes abiertas, por ejemplo la información reservada, confidencial o protegida legalmente de alguna otra manera. En estos casos, aunque cualquier particular puede observar la información, su uso como medio de prueba en un procedimiento judicial puede estar restringido. La utilización de ese tipo de contenidos también puede presentar problemas éticos o metodológicos, como la imposibilidad de atribuirlos o verificarlos.

b) Adquirir

17. Diversas fuentes de datos útiles para las investigaciones en fuentes abiertas se encuentran en plataformas que exigen un pago previo o emplean un modelo combinado de acceso gratuito y de pago en el que para acceder a más funcionalidades y datos se ha de pagar. En ese sentido, cada vez son más las empresas que agregan datos públicos y ofrecen servicios gratuitos y de pago para acceder a esas informaciones. Gran parte de la información útil para las investigaciones en fuentes abiertas está en bases de datos y plataformas a las que solo se puede acceder pagando. A los efectos del Protocolo, la información de fuentes abiertas incluye los servicios de pago que están al alcance de cualquier particular, pero no los servicios cuyo acceso está limitado a determinados grupos, como las fuerzas del orden o los investigadores e investigadoras con licencias particulares.

c) Solicitar

18. En este contexto, por "solicitar" se entiende el pedido de información pública que cualquier persona pueda hacer a organismos del Estado en virtud de las leyes de transparencia o de acceso a la información. No aplica a los pedidos dirigidos a individuos, empresas u organizaciones para que entreguen voluntariamente su información, sino que se limita a los que se dirigen a entidades del Estado que tienen la obligación legal de responder por igual a todas las personas. Las investigaciones en fuentes abiertas pueden dar lugar a otras actividades de investigación en línea, como contactos con fuentes externas utilizando servicios de mensajería, salas de chat, foros o el correo electrónico. Este tipo de contactos escapa al ámbito de la investigación en fuentes abiertas a que se refiere el Protocolo.

3. Inteligencia de fuentes abiertas

19. La inteligencia de fuentes abiertas es una subcategoría de información de fuentes abiertas que se recoge y utiliza con el objetivo específico de ayudar a la formulación de políticas y a la toma de decisiones, casi siempre en un contexto militar o político. Mientras que la información de fuentes abiertas incluye toda la información al alcance del público que cualquiera puede

[13] Aunque la adquisición de información de una base de datos privada o la presentación de una solicitud de información a un organismo público requieren cierto grado de interacción en línea, a menudo se trata de un proceso automatizado, distinto del tipo de interacción con otros usuarios de Internet aquí descrito.

[14] En el Protocolo, la información de fuentes abiertas también puede denominarse "contenidos en línea", "material en línea" o "datos en línea".

obtener legalmente, la inteligencia con fuentes abiertas es un subconjunto de esa información "que se recoge, aprovecha y difunde de manera oportuna a un público concreto con el fin de atender una necesidad de inteligencia específica"[15]. En el contexto de las violaciones del derecho penal internacional y el derecho internacional de los derechos humanos, la inteligencia de fuentes abiertas se utiliza como información secundaria para la toma de decisiones —por ejemplo, las relacionadas con la seguridad, como la protección de las personas testigos y de los miembros del equipo que hacen trabajo de campo, o para rastrear a personas sospechosas— más que para las funciones de recogida de información relacionadas con los procesos de investigación, como el establecimiento de los elementos de los distintos crímenes.

4. Investigación con fuentes abiertas

20. Por "investigación con fuentes abiertas" se entiende el uso de información de fuentes abiertas para recoger información y pruebas.

5. Medios de prueba de fuentes abiertas

21. Debe distinguirse entre "evidencia" e "información"[16]. En general, las evidencias se definen en todas las jurisdicciones como aquella utilizada en una investigación o presentada en audiencias judiciales como los juicios para establecer hechos. La evidencia de fuentes abiertas es un tipo de información de fuentes abiertas con valor probatorio que puede ser admitida para establecer hechos en un procedimiento judicial. Es importante no hablar erróneamente o excesivamente de evidencia al referirse a la "información" en general.

6. Información de fuentes abiertas frente a *software* de código abierto

22. La expresión inglesa *open source* se aplica a menudo al *software* o código que se puede usar y republicar libremente, sin restricciones de derechos de autor, patentes u otros obstáculos legales. El *software* de código abierto se crea con un código fuente para que cualquier persona con acceso a este pueda inspeccionar, modificar y mejorar[17]. Normalmente, quien utiliza el software no puede ver dicho código, pero las personas con conocimientos de programación pueden modificarlo y adaptarlo. El *software* de código abierto *(open-source software)* es distinto de la información de fuentes abiertas *(open source information)*, aunque las personas que investigan en fuentes abiertas utilizan con frecuencia *software* y herramientas de código abierto para encontrar, recoger, preservar y analizar información de fuentes abiertas.

7. Credibilidad frente a fiabilidad

23. Cuando en los juicios penales internacionales se presentan pruebas testimoniales, la autoridad judicial evalúa la "credibilidad de la persona testigo" y la "fiabilidad de su testimonio"[18]. Las orientaciones publicadas por las comisiones de investigación y misiones de determinación de los hechos de las Naciones Unidas y otras investigaciones similares disponen que "la persona entrevistadora deberá evaluar la credibilidad y la fiabilidad de la persona entrevistada"[19]. Además, "la evaluación tendrá en cuenta la pertinencia de la información para el objetivo de la investigación. También examinará la fiabilidad de la fuente y la validez o veracidad de la información"[20]. El Protocolo utiliza estos términos de la siguiente manera:

    a) Por "credibilidad" se entiende la cualidad de una persona que puede o merece ser creída;

15 National Open Source Enterprise, Intelligence Community Directive No. 301, 111 de julio de 2006, pág. 8 (se omite la nota a pie de página).

16 Federica D'Alessandra y otros (eds.), *Handbook on Civil Society Documentation of Serious Human Rights Violations: Principles & Best Practices* (La Haya, Public International Law and Policy Group, 2016), pág. 17.

17 Véase Opensource.com, "¿Qué es el código abierto?".

18 Corte Penal Internacional, *Prosecutor v. Bosco Ntaganda*, causa núm. ICC-01/04-02/06, fallo del 8 de julio de 2019, párr. 53.

19 ACNUDH, *Comisiones de investigación y misiones de determinación de los hechos en derechos humanos y derecho internacional humanitario: Guía y practica* (Nueva York y Ginebra, 2015), pág. 52. Disponible en www.ohchr.org/sites/default/files/Documents/Publications/CoI_Guidance_and_Practice_sp.pdf.

20 *Ibid.*, pág. 59.

b) Por "fiabilidad" se entiende la capacidad para actuar de forma congruente, fidedigna o como se espera;

c) Por "veracidad" o "validez" se entiende la exactitud, rigor o conformidad con los hechos.

II

PRINCIPIOS

RESUMEN DEL CAPÍTULO

- Los principios profesionales relacionados con las investigaciones en fuentes abiertas digitales implican que los investigadores e investigadoras deben ser responsables, competentes y objetivos y que deben efectuar su trabajo de acuerdo a la ley y teniendo en cuenta las cuestiones relacionadas con la seguridad.
- Las personas que investigan en fuentes abiertas también deben tener en cuenta los métodos que usan en todas las etapas de su investigación. Los principios metodológicos pertinentes incluyen, como mínimo, la exactitud, la minimización de los datos, la preservación de los datos y la seguridad por diseño.
- Por último, todos los investigadores e investigadoras deben guiarse por una serie de consideraciones éticas. Estas incluyen, como mínimo, la protección de la dignidad de todas las personas que participan o están implicadas en una investigación, así como la humildad, la inclusividad, la independencia y la transparencia.

24. Aunque las tecnologías, herramientas y técnicas utilizadas en las investigaciones en fuentes abiertas cambiarán, ciertos principios metodológicos y éticos generales deberían perdurar. La definición de estos principios es un paso importante hacia la profesionalización del campo de las investigaciones con fuentes abiertas. Los siguientes principios son fundamentales para garantizar la calidad de las investigaciones con fuentes abiertas, lo que a su vez reforzará su credibilidad, fiabilidad y utilidad potencial para establecer la responsabilidad y minimizar los posibles daños a las diversas partes interesadas.

A. Principios profesionales

1. Responsabilidad

25. Las personas que investigan en fuentes abiertas deben ser responsables de sus actos, lo que a menudo puede conseguirse mediante una documentación clara, el mantenimiento de registros y la supervisión. La transparencia en los métodos y procedimientos de una investigación es un elemento esencial para garantizar la responsabilidad. Por ello, en la medida de lo posible y razonable, los investigadores e investigadoras en fuentes abiertas deben dejar constancia de sus actividades. Las etapas de una investigación en fuentes abiertas —desde la identificación del material pertinente hasta la recogida, el análisis y la presentación de la información— deben documentarse de forma coherente y clara. Todas las personas que participan en la recogida o el tratamiento de información digital deben ser conscientes de la posibilidad de que su metodología sea cuestionada, lo que incluye la posibilidad de que sean llamadas a declarar en un juicio. La documentación de las investigaciones en fuentes abiertas puede realizarse manualmente o con los procesos automatizados proporcionados por diversos programas computacionales. Siempre que la documentación sea coherente y suficientemente completa, pueden utilizarse métodos manuales o automáticos. Los procesos automatizados y los programas computacionales deben ser entendidos por quienes los utilizan y poder ser explicados ante un tribunal tanto por ellos como por las personas que los crearon. Además, los investigadores e investigadoras en fuentes abiertas deben dejar constancia de todas las herramientas o programas que utilicen durante su trabajo.

2. Competencia

26. Las personas que investigan en fuentes abiertas deben tener la formación y los conocimientos técnicos adecuados. Deben ejecutar las actividades en línea de manera profesional y ética, evitando apropiarse del trabajo de otras; nombrando a todas las personas que participan en una investigación (cuando sea seguro hacerlo y cuando lo deseen esas personas); y comunicando los datos con exactitud, lo que incluye reconocer las lagunas que existan en los contenidos en línea. Tanto investigadores e investigadoras como los procesos de investigación en fuentes abiertas también deben permanecer flexibles, estar al día de las novedades en la materia y adoptar las nuevas tecnologías y técnicas según convenga. Además, las organizaciones y equipos de investigación deben contar con mecanismos para garantizar que los procedimientos se aplican y observan de forma coherente.

3. Objetividad

27. La objetividad es un principio fundamental que se aplica a todas las investigaciones, sean en línea o en el mundo real. Las personas que investigan en fuentes abiertas deben ser conscientes de que los sesgos personales, culturales y estructurales pueden afectar su trabajo y que deben tomar contramedidas para garantizar la objetividad. En ese sentido, deben asegurarse de que realizan sus investigaciones de forma objetiva, elaborando varias hipótesis de trabajo y no favoreciendo ninguna teoría en particular para explicar el caso que investigan. La objetividad es especialmente importante para las investigaciones en fuentes abiertas realizadas en línea, debido a la forma en que la información está estructurada y se presenta en Internet. Aun realizando la misma consulta se pueden obtener resultados muy diferentes en función del navegador, el motor de búsqueda, los términos de búsqueda y la sintaxis que se utilicen. Los sesgos inherentes a la arquitectura de Internet y a los algoritmos empleados por los motores de búsqueda y los sitios web pueden disminuir la objetividad de los resultados de

la búsqueda[21]. Estos también pueden resultar influidos por una serie de factores técnicos, como el dispositivo utilizado y su ubicación, y las búsquedas y actividades realizadas anteriormente en Internet por el usuario. Las personas que investigan en fuentes abiertas deben contrarrestar esos sesgos aplicando metodologías para que los resultados de las búsquedas sean lo más diversos posible, por ejemplo, ejecutando múltiples consultas de búsqueda y utilizando distintos motores de búsqueda y navegadores[22]. Deben ser conscientes de que los resultados de las búsquedas también pueden estar influidos por otros factores, entre ellos los causados por la discrepancia en el entorno digital, es decir, el hecho de que pueda haber menos información en línea sobre ciertos grupos o segmentos de la sociedad[23]. Por último, deben esforzarse siempre por conocer sus propios sesgos, que pueden ser conscientes o subconscientes, y contrarrestarlos[24].

4. Legalidad

28. Las investigaciones en fuentes abiertas deben cumplir la legislación aplicable, lo que significa que quienes las realizan debe tener un conocimiento básico de las leyes que se aplican a su trabajo. En particular, deben conocer las leyes relativas a la protección de los datos y al derecho a la privacidad, que está protegido por el derecho internacional de los derechos humanos[25]. Aunque la información esté al alcance del público, ello no significa que pueda recogerse y utilizarse sin consecuencias en lo que a la privacidad se refiere. Las personas que investigan en fuentes abiertas deben evaluar las consecuencias de sus actos para la privacidad, que pueden ser contrarias a las expectativas razonables de privacidad de una persona en diferentes espacios digitales. También deben tener presente el efecto mosaico, es decir, el hecho de que los datos públicos, aun habiéndose convertido en anónimos, pueden ser reidentificados si se publican o combinan

21 Véase Safiya Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York, New York University Press, 2018); Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor* (Nueva York, Picador, 2019).

22 Véase, por ejemplo, "How to conduct discovery using open source methods", en *Digital Witness, Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig y Daragh Murray (eds.) (Oxford, Oxford University Press, 2020) (donde se analizan las formas en que la selección del motor de búsqueda y los términos de búsqueda pueden crear un sesgo en los resultados de las investigaciones en fuentes abiertas).

23 Véase, por ejemplo, Alexa Koenig y Ulic Egan, "Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes", en *Technologies of Human Rights Representation*, James Dawes y Alexandra S. Moore (eds.) (de próxima publicación) (donde se analiza el hecho de que la relativa falta de acceso de las mujeres a los teléfonos inteligentes y el uso de un lenguaje en clave en Internet por las sobrevivientes de la violencia sexual y la violencia de género pueden reducir la cantidad y la accesibilidad de la información de fuentes abiertas relacionada con esos delitos, así como el hecho de que la prevalencia de los hombres en los puestos relacionados con la tecnología y en las investigaciones de los crímenes de guerra puede reducir la probabilidad de que los procesos de detección automatizados o manuales produzcan información de fuentes abiertas sobre los crímenes con una dimensión de género). Para más información sobre los sesgos, véase el cap. II.C, sobre los principios éticos, y el cap. V.B, sobre la evaluación del panorama digital.

24 Véase, por ejemplo, Forensic Science Regulator, *Cognitive Bias Effects Relevant to Forensic Science Investigations, FSR-G-217* (Birmingham, Reino Unido, 2015) (donde se analizan diversas categorías de sesgos cognitivos que pueden reducir la calidad de la investigación, como el sesgo de expectativa, el sesgo de confirmación, el efecto de anclaje, el sesgo contextual y los efectos de rol y reconstrucción); Wayne A. Wallace, *The Effect of Confirmation Bias on Criminal Investigative Decision Making* (Minneapolis, Walden University ScholarWorks, 2015) (donde se explica el sesgo de confirmación como un proceso por el cual las personas que investigan buscan o dan credibilidad a la información que confirma la teoría que favorecen sobre un caso "al tiempo que pasan por alto o tratan de justificar la información que la contradice"); Michael Pittaro, "Implicit bias within the criminal justice system", Psychology Today, 21 de noviembre de 2018 (donde se tratan los sesgos que pueden influir en las investigaciones criminales en general y se describen técnicas conocidas para contrarrestar los sesgos); Jon S. Byrd, "Confirmation bias, ethics, and mistakes in forensics", Forensic Pathways, 21 de marzo de 2020 (donde se analizan diversos errores cognitivos y éticos que pueden distorsionar el análisis forense, así como distintas técnicas para evitar esos errores). Véase también Yvonne McDermott, Daragh Murray y Alexa Koenig, "Digital accountability symposium: whose stories get told, and by whom? Representativeness in open source human rights investigations", Opinio Juris, 19 de diciembre de 2019 (donde se postula que los métodos de las investigaciones en fuentes abiertas pueden incidir negativamente en "los tipos de delitos que sacan a la luz, las víctimas y los testigos que tienen la oportunidad de hacerse oír y la manera en que se articulan los relatos sobre las violaciones de derechos humanos en masa"); y el proyecto titulado "The future of human rights investigations: using open source intelligence to transform the documentation and discovery of human rights violations", dirigido por Yvonne McDermott.

25 El artículo 12 de la Declaración Universal de Derechos Humanos dispone que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques. El Pacto Internacional de Derechos Civiles y Políticos establece en su artículo 17 que nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación. También prevé, en el artículo 17, que toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.

suficientes conjuntos de datos con información similar o complementaria[26]. Además, deben ser conscientes de que, en algunas jurisdicciones, la observación continua y persistente de una persona en línea, o la recolección sistemática y la preservación de sus datos personales más allá de cierto tiempo, pueden requerir permisos y salvaguardias adicionales, debido a las mayores consecuencias de esas actividades para la privacidad[27].

5. Conciencia de la seguridad

29. Mientras que la seguridad por diseño[28] se refiere a la arquitectura y la infraestructura de una investigación y de las actividades secundarias, el principio de conciencia de la seguridad se centra en las consideraciones que las personas que investigan deben tener en cuenta durante su trabajo, siendo conscientes en particular de su comportamiento en línea. Todas las personas que realizan investigaciones en línea deben tomar conciencia básica de la seguridad relacionada con sus actividades para minimizar su rastro digital y conocer los riesgos potenciales. Las organizaciones que realizan investigaciones en fuentes abiertas deben asegurarse de que sus equipos reciban capacitación sobre seguridad informática/digital para que comprendan los riesgos que podrían enfrentar y conozcan los tres pilares fundamentales de la seguridad de la información: a) confidencialidad (solo se debe permitir el acceso a los datos a los usuarios autorizados); b) integridad (se debe impedir que los datos sean manipulados o alterados por usuarios no autorizados); y c) disponibilidad (se debe garantizar que los sistemas y datos estén al alcance de los usuarios autorizados cuando los necesiten). La capacitación también debe centrarse en la estructura de gobernanza de Internet. Antes de comenzar las actividades de investigación en línea deben realizarse evaluaciones de las amenazas y riesgos que deben revisarse periódicamente y modificarse si se considera necesario. La seguridad es responsabilidad de todos, no solo de las dependencias de tecnología de la información o de las personas encargadas de gestionar los riesgos de seguridad.

B. Principios metodológicos

1. Exactitud

30. El imperativo metodológico y ético de garantizar la exactitud —y, por ende, la calidad— de las investigaciones, obliga a estas a basarse únicamente en material creíble. Las personas que investigan en fuentes abiertas deben tratar de ser lo más veraces y precisas posible en el curso de sus investigaciones y al presentar cualquier resultado, especialmente al reconocer deficiencias de los datos subyacentes o de su argumentación en general. Muchas veces, la exactitud puede mejorarse empleando y poniendo a prueba más de una hipótesis de trabajo o sometiendo los resultados a revisión por pares; ambas opciones pueden minimizar las posibilidades de que los datos se seleccionen, interpreten o presenten de manera sesgada. Las conclusiones analíticas no deben exagerarse o sobredimensionarse. Usando un lenguaje claro, objetivo y basado en los hechos, además evitando usar lenguaje emotivo, se protege la objetividad real y supuesta de una investigación y de sus resultados.

---

[26] El concepto del efecto mosaico se deriva de la teoría del mosaico de la recogida de inteligencia, según la cual hay fragmentos dispares de información que, aunque por separado tengan poca utilidad, se vuelven importantes cuando se combinan con otros tipos de información (Pozen 2005). Aplicado a los datos de uso público, el concepto del efecto mosaico sugiere que incluso los datos convertidos en anónimos, que pueden parecer inocuos por separado, pueden ser reidentificados si se publican suficientes conjuntos de datos con información similar o complementaria". Véase John Czajka y otros, *Minimizing Disclosure Risk in HHS Open Data Initiatives* (Washington, D. C., Mathematica Policy Research, 2014), apéndice E, pág. E-7. Disponible en https://aspe.hhs.gov/system/files/pdf/77196/rpt_Disclosure.pdf. Véase también David E. Pozen, "The mosaic theory, national security, and the Freedom of Information Act", *Yale Law Journal*, vol. 115, núm. 3 (diciembre de 2005), págs. 628 a 679.

[27] Por ejemplo, en el Reino Unido de Gran Bretaña e Irlanda del Norte, la ley dispone que "los datos personales tratados para... fines policiales no deben preservarse más tiempo del necesario para el objeto en cuestión" (capítulo 12 de la Ley de Protección de Datos de 2018, parte 3, cap. 3, art. 39, párr. 1). En virtud del Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), los datos personales solo pueden ser recogidos con "fines determinados, explícitos y legítimos", deben limitarse a la información necesaria en relación con los fines para los que son recogidos y deben permanecer identificables solo durante el tiempo necesario a los efectos de la recogida (arts. 5 y 6).

[28] Véase el párr. 33.

2. Minimización de datos

31. El principio de la minimización de datos prescribe que solo debe recogerse y tratarse información digital si: a) lo justifica un fin expresable; b) es necesario para lograr ese fin; y c) actuar de ese modo guarda proporción con la capacidad de alcanzar ese fin[29]. En el contexto de las investigaciones con fuentes abiertas, solo deben recogerse los contenidos en línea relevantes para una investigación concreta. Este principio favorece la recolección manual y pormenorizada frente a la recolección masiva y automatizada, aunque cabe señalar que esta última puede ser adecuada en algunos casos. La aplicación de este principio a la recolección de contenidos en línea contribuye a evitar la recolección excesiva, lo cual es importante por varias razones. La recolección excesiva —que debe tenerse en cuenta especialmente cuando se utilizan procesos de recolección automatizada— puede crear vulnerabilidades de seguridad o exacerbar las existentes[30], en particular si hace que el equipo de investigación no sea consciente de los tipos de información que posee. La recolección excesiva también puede plantear problemas de privacidad y protección de datos cuando un proceso automatizado no distingue según el tipo de contenido. Por último, el evitar la recolección excesiva presenta ciertas ventajas prácticas como minimizar los costos de almacenamiento y prevenir los cuellos de botella en las fases siguientes del ciclo de investigación, como la revisión, el análisis y, en caso de que la investigación llegue a un procedimiento judicial, la entrega.

3. Preservación

32. Es igual importante evitar la insuficiente recolección como la excesiva recolección de información relevante, en particular en el contexto de la información en línea, cuya permanencia y disponibilidad es muchas veces precaria. El principio de preservación tiene por objeto evitar la recolección insuficiente, de modo que no se pierda el material pertinente y potencialmente probatorio. Puede ocurrir que las plataformas de redes sociales, por ejemplo, eliminen contenidos que incumplan sus condiciones de utilización aunque dichos contenidos puedan ser valiosos para las investigaciones. A menos que se haga rápidamente una solicitud de preservación a la plataforma o que el equipo de investigación preserve los contenidos de otra manera, dicha información puede perderse para siempre. Además, los usuarios pueden optar por suprimir o editar sus propios contenidos, por lo que esa información que antes era pública deja de estar disponible. Adicionalmente, la información que se encuentra en Internet puede descontextualizarse, perderse, eliminarse o corromperse fácilmente. Para que el material digital siga siendo accesible y puedan utilizarlo futuros mecanismos judiciales, es necesario preservarlo activa y cuidadosamente tanto a corto como a largo plazo[31].

4. Seguridad por diseño

33. El principio de la seguridad por diseño requiere que, en la medida de lo posible, la información digital y las operaciones en línea sean seguras por defecto. Las organizaciones que realizan investigaciones con fuentes abiertas en línea deben invertir en medidas técnicas y estructurales adecuadas y aplicarlas para que, por defecto, las infraestructuras —tanto el *hardware* como el *software*— estén debidamente anonimizadas y no sean atribuibles cuando su personal investigador actúe en línea. Todos los dispositivos deben contar con *software* actualizado para protegerlos de los programas malintencionados y tener una configuración de privacidad y seguridad adecuada. Las medidas de seguridad deben estar activas antes de que comiencen las actividades de investigación en línea, y supervisarse y actualizarse continuamente, además de modificarse cuando sea necesario. Para comprobar que los sistemas de seguridad funcionan según lo previsto, las organizaciones, los equipos de investigación o las personas investigadoras pueden disponer el ponerlos a prueba continua, incluida la realización de pruebas de penetración[32].

---

29 El Protocolo derivó el principio de la minimización de datos del Reglamento General de Protección de Datos de la Unión Europea, pero lo adaptó al contexto de la investigación en fuentes abiertas (véase el art. 5 del Reglamento).

30 Véase el cap. IV, sobre la seguridad, donde se dan más ejemplos de vulnerabilidades de seguridad.

31 Para más información, véase el cap. VI.D, sobre la preservación.

32 Una prueba de penetración es un ciberataque simulado que ha sido autorizado para poner a prueba la seguridad de un sistema.

C. Principios éticos

1. Dignidad

34. Las investigaciones deben realizarse teniendo en cuenta las cuestiones subyacentes relacionadas con la dignidad, especialmente los intereses protegidos por el derecho internacional de los derechos humanos. Por ejemplo, las personas que realizan la investigación deben observar el principio de no discriminación, que puede incidir en lo que se investiga, en quién investiga o en a quién se atribuye la investigación, e integrar salvaguardias para proteger la seguridad digital, física y psicosocial de las personas testigos o sobrevivientes, sus pares, las personas acusadas y otras que puedan verse afectadas negativamente. La observancia del principio de dignidad también puede incidir en la información que se divulga públicamente sobre una investigación, tanto por escrito como por cualquier medio visual, por ejemplo, no mostrando todo el sufrimiento o la violencia si no es necesario hacerlo. Este principio garantiza que las investigaciones en fuentes abiertas se guíen por las normas de derechos humanos para actuar de manera ética.

2. Humildad

35. Las personas que realizan investigaciones en fuentes abiertas deben ser humildes, lo que entraña reconocer sus propias limitaciones y ser conscientes de lo que no saben. Es posible que para comprender e interpretar correctamente determinada información de fuentes abiertas necesiten formación especializada o consultar a especialistas. La humildad también significa asumir la responsabilidad con los errores. Cuando se descubre que se ha cometido un error, este debe ser corregido o comunicado a quienes puedan minimizar el daño resultante. Lo ideal sería que exista un mecanismo para notificar los errores y para que se publiquen correcciones, especialmente en el caso de las investigaciones que son públicas y de amplia difusión.

3. Inclusividad

36. Las personas que realizan investigaciones en fuentes abiertas deben velar por que estas integren una diversidad de perspectivas y experiencias. Entre los factores que pueden influir en la inclusividad general de una investigación en línea se encuentran su alcance geográfico, las infracciones o crímenes internacionales que se investigan y el hecho de que se tenga o no conciencia de la naturaleza desigual de la información en línea con respecto a los diferentes segmentos de la sociedad[33]. Los equipos de investigación también deben ser diversos, lo que incluye tener un equilibrio de género. Además, el principio de inclusividad, junto con el principio de dignidad, puede incidir en el material que se decide recoger y utilizar en una investigación y en la forma en que se presenta a los diferentes públicos.

4. Independencia

37. Las personas que realizan investigaciones en fuentes abiertas deben protegerse a sí mismas y a sus investigaciones de toda influencia inapropiada. Deben identificar y evitar cualquier conflicto de intereses real o supuesto y establecer salvaguardias para mitigar los conflictos que no puedan evitarse. La transparencia del proceso, los métodos y la financiación puede ayudar a evaluar la independencia y proteger la independencia real y supuesta de una investigación.

5. Transparencia

38. Mientras que el principio de responsabilidad exige transparencia en los métodos y resultados de la investigación, el principio ético de la transparencia se refiere a la forma en que los investigadores e investigadoras en fuentes abiertas se comportan en línea y de cara al exterior. Esto significa que se debe evitar toda tergiversación[34]. Aunque el anonimato y la no atribución —que pueden incluir el uso de identidades virtuales[35]— pueden ser importantes por motivos de seguridad, los investigadores e investigadoras deben ser conscientes de las posibles ramificaciones

33 Véase el cap. V.B, sobre la evaluación del panorama digital.

34 Por ejemplo, tratar de entrar en grupos cerrados o de conectar con personas en las redes sociales proporcionando información falsa.

35 Para más información sobre las identidades virtuales, véase el cap. IV.C, dedicado a las consideraciones relacionadas con la infraestructura.

negativas de la tergiversación, como el daño a la reputación y la credibilidad de una investigación, equipo u organización, o la contaminación de la información recogida. La obtención de información mediante la tergiversación puede violar el derecho a la privacidad de una persona o mancillar una investigación, especialmente si la tergiversación es ilegal en la jurisdicción o jurisdicciones correspondientes.

III

MARCO JURÍDICO

RESUMEN DEL CAPÍTULO

- Para decidir qué información recolectar y cúal es la mejor manera de hacerlo es fundamental determinar qué leyes se aplican. Estas variarán en función del objetivo de la investigación, de la identidad de las personas investigadoras e investigadas, y de las jurisdicciones en que se encuentran estas, los datos y los procesos legales.
- Al preservar el material digital de forma que se mantenga su autenticidad y se documente la cadena de custodia, aumentar la probabilidad de que sea admitido como medio de prueba en tribunales.
- Según el tipo de investigación y su objetivo final (por ejemplo, un procedimiento penal o civil, un proceso de justicia transicional, etc.), se aplica un umbral probatorio diferente.
- La violación del derecho a la privacidad de una persona podría provocar la no admisión de los medios de prueba obtenidos.

39. Las personas que realizan investigaciones de fuentes abiertas deben comprender los marcos jurídicos en que actúan. En concreto, deben conocer la legislación aplicable a sus investigaciones y los marcos jurídicos de las jurisdicciones en que llevan a cabo actividades de investigación. El conocimiento de las leyes sustantivas aplicables a las investigaciones —incluidos los elementos de las posibles infracciones[36] o crímenes, así como los modos de responsabilidad[37], puede aumentar su eficacia y la probabilidad de que la información recogida y las conclusiones analíticas extraídas puedan utilizarse en mecanismos de justicia y establecimiento de la responsabilidad. Del mismo modo, el conocimiento de las leyes procesales y las normas relativas a los medios de prueba en las jurisdicciones correspondientes permitirá a las personas investigadoras realizar su trabajo de conformidad con los requisitos para el uso de información de fuentes abiertas en los procedimientos judiciales.

40. En el caso de las investigaciones penales internacionales, el marco jurídico será prescrito por los instrumentos que rigen el tribunal, la corte o el sistema judicial correspondiente[38]. En el caso de las investigaciones establecidas por mandato internacional, como las comisiones de investigación, el mecanismo que establece la investigación prescribirá, entre otros elementos, la legislación aplicable y el alcance geográfico y temporal de la investigación[39]. En el caso de otras investigaciones, como las realizadas por ONG, la propia entidad investigadora determina a veces su propio marco jurídico[40].

41. Este capítulo pretende ayudar a las personas que realizan investigaciones en fuentes abiertas a conocer y comprender mejor los posibles usos finales de su trabajo y adaptar así sus técnicas de investigación. Puesto que las leyes aplicables varían según la jurisdicción, el tipo de investigación y la autoridad legal de la entidad investigadora, las siguientes secciones ofrecen una visión general de las principales consideraciones que se han de tener en cuenta al investigar posibles violaciones del derecho internacional. Se recomienda que, en la medida de lo posible, los equipos investigadores reciban asesoramiento especializado de juristas que conozcan bien las jurisdicciones correspondientes y el asunto en cuestión.

---

36 Por ejemplo, si se investigan casos de discurso de odio e incitación a la violencia, los investigadores e investigadoras deben comprender el tipo de conducta que alcanza el alto umbral del artículo 20, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos. Véase el Plan de Acción de Rabat sobre la prohibición de la apología del odio nacional, racial o religioso que constituye incitación a la discriminación, la hostilidad o la violencia (A/HRC/22/17/Add.4, apéndice), párrs. 11 y 29, y su prueba de umbral basada en los derechos humanos, publicada en 32 idiomas. Disponible en www.ohchr.org/es/freedom-of-expression. En relación con el discurso de odio, véase la Estrategia y Plan de Acción de las Naciones Unidas para la Lucha contra el Discurso de Odio (2019). Disponible en www.un.org/en/genocideprevention/documents/advising-and-mobilizing/Action_plan_on_hate_speech_ES.pdf.

37 En el derecho penal, los autores pueden ser declarados responsables con arreglo a una serie de modos de responsabilidad definidos por la ley correspondiente. Estos modos incluyen la autoría directa e indirecta, la coautoría, la complicidad y la responsabilidad de mando. Véase Jérôme de Hemptinne, Robert Roth y Elies van Sliedregt (eds.), *Modes of Liability in International Criminal Law* (Cambridge, Reino Unido, Cambridge University Press, 2019).

38 Véase, por ejemplo, Corte Penal Internacional, Rules of Procedure and Evidence (2013); Tribunal Internacional para la ex-Yugoslavia, Rules of Procedure and Evidence (8 de julio de 2015); Tribunal Penal Internacional para Rwanda, Rules of Procedure and Evidence (13 de mayo de 2015); Tribunal Especial Residual para Sierra Leona, Rules of Procedure and Evidence (30 de noviembre de 2018); Tribunal Especial para el Líbano, Rules of Procedure and Evidence (10 de abril de 2019); Salas Especiales de los Tribunales de Camboya, Internal Rules (3 de agosto de 2011).

39 Por ejemplo, la misión internacional independiente de determinación de los hechos sobre la República Bolivariana de Venezuela, que se estableció en septiembre de 2019, tiene el mandato de investigar las ejecuciones extrajudiciales, las desapariciones forzadas, las detenciones arbitrarias y las torturas y otros tratos crueles, inhumanos o degradantes cometidos desde 2014 y de presentar un informe con sus conclusiones al Consejo (resolución 42/25 del Consejo de Derechos Humanos, párr. 24). La Comisión Internacional Independiente de Investigación sobre la República Árabe Siria, creada en 2011, tiene el mandato de investigar todas las presuntas violaciones de las normas internacionales de derechos humanos cometidas desde marzo de 2011 en la República Árabe Siria, determinar los hechos y circunstancias que puedan constituir infracciones de esas normas y los crímenes cometidos y, siempre que sea posible, identificar a los autores (resolución S-17/1 del Consejo de Derechos Humanos, párr. 13). El equipo de expertos internacionales enviado a la región de Kasái de la República Democrática del Congo en 2017 tenía la misión de recoger y custodiar información en relación con las presuntas vulneraciones y conculcaciones de los derechos humanos y las vulneraciones del derecho humanitario internacional en los Kasáis, y remitir a las autoridades judiciales de la República Democrática del Congo las conclusiones de esa investigación (resolución 35/33 del Consejo de Derechos Humanos, párr. 10).

40 Algunas organizaciones, ONG incluidas, tienen su propia metodología interna que les exige centrarse en un área concreta del derecho, como la tortura o la violencia sexual y la violencia de género, lo que también servirá de orientación para el enfoque de las investigaciones.

A. Derecho internacional público

42. El Protocolo se centra en tres categorías del derecho internacional público que se superponen: el derecho internacional humanitario, el derecho internacional de los derechos humanos y el derecho penal internacional. Las tres categorías se refuerzan mutuamente, como demuestra el que la aplicabilidad del derecho internacional humanitario o del derecho penal internacional no exime a los Estados de cumplir sus obligaciones en virtud del derecho internacional de los derechos humanos. A continuación se ofrece una visión general de cada una de esas áreas, señalándose las fuentes del derecho y distinguiéndo entre las tres para que las personas que realizan investigaciones en fuentes abiertas sepan las referencias que deben orientar su trabajo.

1. Derecho internacional humanitario

43. El derecho internacional humanitario, o "derecho de los conflictos armados", regula la conducción de las hostilidades y resuelve las cuestiones humanitarias que surgen en el contexto de esos conflictos, que pueden ser de carácter internacional o no internacional[41]. El derecho internacional humanitario se activa cuando estalla un conflicto armado y permanece activo hasta que se alcanza la paz, aunque estas delimitaciones no siempre son concretas o fáciles de interpretar[42]. Las principales fuentes del derecho internacional humanitario son los Convenios de La Haya de 1899 y 1907[43], los Convenios de Ginebra del 12 de agosto de 1949[44] y sus Protocolos Adicionales de 1977[45], así como varios tratados que regulan el empleo de ciertos tipos de armas[46]. El derecho consuetudinario es otra fuente importante del derecho internacional humanitario, ya que colma las lagunas no abordadas por los tratados. El derecho internacional humanitario consuetudinario es vinculante para todas las partes de un conflicto y es especialmente relevante para los conflictos armados no internacionales, ya que sus normas relacionadas con estos son más detalladas que las establecidas en los tratados

41 La distinción entre conflicto armado internacional y no internacional se basa en dos factores: la estructura y la condición de las partes implicadas. En los conflictos armados internacionales participan Estados soberanos. En cambio, en los conflictos armados no internacionales participan Estados y grupos armados organizados. Véase Andrew Clapham, Paola Gaeta y Marco Sassòli (eds.), *The 1949 Geneva Conventions, A Commentary* (Oxford, Oxford University Press, 2015), caps. 1 y 19.

42 Mientras que el momento en que comienza un conflicto internacional es relativamente claro, ya que lo desencadena cualquier uso de la fuerza entre dos Estados, el inicio de un conflicto armado no internacional no es tan fácil de determinar. Solo se habla de "conflicto armado no internacional" cuando el grupo o los grupos armados en cuestión están suficientemente organizados y el nivel de violencia alcanza cierta intensidad, dos factores que requieren un análisis detallado de los hechos en cada caso. Véase Sylvain Vité, "Typology of armed conflicts in international humanitarian law: legal concepts and actual situations", *Revista Internacional de la Cruz Roja*, vol. 91, núm. 873 (marzo de 2009), págs. 72 y 76 a 77. También hay discrepancias en cuanto al momento en que termina un conflicto armado y se alcanza la paz. Aunque la firma de un acuerdo de alto el fuego o de paz puede contribuir a determinar que el conflicto armado ha terminado, ese tipo de acuerdos no son determinantes. Se han propuesto varios criterios para establecer que un conflicto armado ha terminado, como el hecho de que se haya llegado a un cese general de las operaciones militares después de alcanzarse una conclusión general de paz, la existencia de un acuerdo pacífico y el cese de los criterios que permitieron determinar la existencia del conflicto. Véase Nathalie Weizmann, "The end of armed conflict, the end of participation in armed conflict, and the end of hostilities: implications for the detention operations under the 2001 AUMF", *Columbia Human Rights Law Review*, vol. 47, núm. 3 (2016), págs. 221 a 224.

43 Respectivamente, Convención relativa a las Leyes y Costumbres de la Guerra Terrestre (Segunda Convención de La Haya) y Convención relativa a las Leyes y Costumbres de la Guerra Terrestre (Cuarta Convención de La Haya).

44 Véase el Convenio de Ginebra del 12 de agosto de 1949 para Aliviar la Suerte que Corren los Heridos y los Enfermos de las Fuerzas Armadas en Campaña (Primer Convenio de Ginebra); el Convenio de Ginebra del 12 de agosto de 1949 para Aliviar la Suerte que Corren los Heridos, los Enfermos y los Náufragos de las Fuerzas Armadas en el Mar (Segundo Convenio de Ginebra); el Convenio de Ginebra relativo al Trato debido a los Prisioneros de Guerra (Tercer Convenio de Ginebra); y el Convenio de Ginebra relativo a la Protección debida a las Personas Civiles en Tiempo de Guerra (Cuarto Convenio de Ginebra).

45 Véase el Protocolo Adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la Protección de las Víctimas de los Conflictos Armados Internacionales (Protocolo I); y el Protocolo Adicional a los Convenios de Ginebra del 12 de agosto de 1949 relativo a la Protección de las Víctimas de los Conflictos Armados Sin Carácter Internacional (Protocolo II).

46 Véase, por ejemplo, la Convención sobre la Prohibición del Desarrollo, la Producción y el Almacenamiento de Armas Bacteriológicas (Biológicas) y Toxínicas y sobre Su Destrucción; la Convención sobre Prohibiciones o Restricciones del Empleo de Ciertas Armas Convencionales que Puedan Considerarse Excesivamente Nocivas o de Efectos Indiscriminados; la Convención sobre la Prohibición del Desarrollo, la Producción, el Almacenamiento y el Empleo de Armas Químicas y sobre Su Destrucción; la Convención sobre la Prohibición del Empleo, Almacenamiento, Producción y Transferencia de Minas Antipersonal y sobre su Destrucción; y la Convención sobre Municiones en Racimo. Véase también Comité Internacional de la Cruz Roja (CICR), "Weapons", 30 de noviembre de 2011. Disponible en www.icrc.org/en/document/weapons.

de derecho internacional humanitario[47]. Hasta principios de la década de 1990, los principales mecanismos de aplicación del derecho internacional humanitario eran los tribunales militares nacionales, en los que los Estados juzgaban a sus propios soldados y oficiales. Con la aparición de los tribunales penales internacionales, ciertas violaciones graves del derecho internacional humanitario fueron codificadas en los estatutos fundacionales de los tribunales como crímenes de guerra[48], proporcionando una nueva vía para hacer cumplir el derecho internacional humanitario a nivel internacional. Algunos Estados también han codificado los crímenes de guerra en su legislación nacional[49], de modo que pueden ser juzgados en sus sistemas judiciales ordinarios, en contraposición a los tribunales militares. Las causas juzgadas por esos tribunales nacionales pueden referirse a hechos ocurridos en el país del conflicto o, cada vez más, en otros países, con arreglo al principio de la jurisdicción universal[50]. Varios Estados han establecido dependencias especializadas en los crímenes de guerra para enjuiciar esos casos. Los tribunales penales internacionales y los tribunales nacionales contribuyen al creciente corpus de jurisprudencia sobre el derecho internacional humanitario, que también sirve como importante fuente de derecho, cuyas normas pueden ser vinculantes en función de la jurisdicción.

2. Derecho internacional de los derechos humanos

44. En virtud del derecho internacional, los Estados tienen la obligación y el deber de respetar, proteger y cumplir los derechos humanos. La Declaración Universal de Derechos Humanos, aprobada en 1948, constituye la base del derecho internacional de los derechos humanos. Aunque es una aspiración y no obliga jurídicamente a los declarantes, algunos de sus artículos forman parte del derecho internacional consuetudinario[51]. También ha inspirado dos pactos y un amplio conjunto de tratados de derechos humanos[52]. Los Estados solo están obligados por los pactos y tratados que han firmado y ratificado, a menos que las normas que contienen esos documentos hayan alcanzado la categoría de derecho internacional

47 Véase CICR, "Customary international humanitarian law", 29 de octubre de 2010. Disponible en www.icrc.org/en/document/customary-international-humanitarian-law-0. Véase también CICR, "Nuestra bienvenida a la base de datos sobre DIH consuetudinario". Disponible en https://ihl-databases.icrc.org/customary-ihl/spa/docs/home.

48 Por ejemplo, el artículo 8 del Estatuto de Roma de la Corte Penal Internacional codifica el derecho internacional humanitario en su definición de los crímenes de guerra.

49 Véase, por ejemplo: Australia (Ley de Crímenes de Guerra de 1945, enmendada, art. 7); Bosnia y Herzegovina (Código Penal, arts. 171 a 184); Kenya (Ley de Crímenes Internacionales de 2008, art. 6, párrs. 1 c) y 2 a 4); Nueva Zelandia (Ley de Crímenes Internacionales y de la Corte Penal Internacional de 2000, art. 11); Sudáfrica (Ley de Aplicación de los Convenios de Ginebra de 2012).

50 En virtud de la "jurisdicción universal", un tribunal nacional puede enjuiciar a individuos por crímenes graves de derecho internacional —como los crímenes de lesa humanidad, los crímenes de guerra, el genocidio y la tortura— que hayan sido cometidos fuera de las fronteras del Estado, basándose en el principio de que tales crímenes perjudican a la comunidad internacional y al propio orden internacional, que los Estados pueden proteger actuando por su cuenta. Véase International Justice Resource Center, "Universal jurisdiction". Disponible en https://ijrcenter.org/cases-before-national-courts/domestic-exercise-of-universal-jurisdiction.

51 Numerosos países, autoridades de las Naciones Unidas y especialistas han afirmado que la mayoría de los artículos de la Declaración Universal de Derechos Humanos, si no todos, constituyen derecho internacional consuetudinario. En concreto, se acepta que las prohibiciones de la esclavitud, la privación arbitraria de la vida, la tortura, la detención arbitraria y la discriminación racial codificadas en la Declaración Universal de Derechos Humanos constituyen derecho internacional consuetudinario. Véase Hurst Hannum, "The status of the Universal Declaration of Human Rights in national and international law", *Georgia Journal of International and Comparative Law*, vol. 25, núm. 1 (1996), págs. 322 a 332 y 341 a 346.

52 Véase la Convención Internacional sobre la Eliminación de todas las Formas de Discriminación Racial; el Pacto Internacional de Derechos Civiles y Políticos; el Pacto Internacional de Derechos Económicos, Sociales y Culturales; la Convención sobre la Eliminación de Todas las Formas de Discriminación contra la Mujer; la Convención contra la Tortura y Otros Tratos o Penas Crueles, Inhumanos o Degradantes; y la Convención sobre los Derechos del Niño. Para más información sobre los principales tratados de derechos humanos de las Naciones Unidas, véase ACNUDH, "Los principales instrumentos internacionales de derechos humanos y sus órganos de control". Disponible en www.ohchr.org/es/core-international-human-rights-instruments-and-their-monitoring-bodies.

consuetudinario[53]. El derecho internacional de los derechos humanos también se ha integrado en los estatutos de muchos tribunales penales internacionales. Además, hay varias cortes regionales de derechos humanos establecidas por convenciones internacionales con el mandato de juzgar asuntos contra Estados parte en dichas convenciones por las violaciones del derecho internacional de los derechos humanos, entre ellos la Corte Africana de Derechos Humanos y de los Pueblos[54], el Tribunal Europeo de Derechos Humanos[55] y la Corte Interamericana de Derechos Humanos[56]. Existen otros órganos de derechos humanos a nivel regional, como la Comisión Africana de Derechos Humanos y de los Pueblos, el Comité Europeo de Derechos Sociales y la Comisión Interamericana de Derechos Humanos, que siguen estableciendo jurisprudencia sobre el derecho internacional de los derechos humanos.

45. Las organizaciones internacionales también desempeñan un papel fundamental en la elaboración y el establecimiento de normas de derecho internacional consuetudinario de los derechos humanos[57]. La Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), así como otras entidades internacionales, publican informes temáticos sobre áreas del derecho que contribuyen al establecimiento de normas y al desarrollo del derecho indicativo. Los órganos creados en virtud de tratados de derechos humanos[58] elaboran informes[59], jurisprudencia[60] y otras orientaciones, como observaciones generales y recomendaciones generales[61], que desarrollan los artículos de sus respectivos tratados y contribuyen a que se comprendan mejor. Del mismo modo, los procedimientos especiales del Consejo de Derechos Humanos participan en la evolución de las normas del derecho internacional de los derechos humanos[62], al igual que otros mecanismos, como las misiones de

53 Por "derecho internacional consuetudinario" se entienden las obligaciones internacionales derivadas de las prácticas internacionales arraigadas, a diferencia de las obligaciones derivadas de las convenciones y tratados formales escritos. Es el resultado de una práctica general y constante que los Estados siguen porque sienten que tienen la obligación jurídica. Uno de los componentes fundamentales del derecho internacional consuetudinario es el *ius cogens*, es decir, una serie de principios fundamentales e imperativos del derecho internacional. Véase, por ejemplo, Legal Information Institute, "Customary international law" y "Jus cogens", Facultad de Derecho de la Universidad Cornell. Disponible en www.law.cornell.edu/wex.

54 Establecida en virtud de la Carta Africana de Derechos Humanos y de los Pueblos (Carta de Banjul).

55 Creado en virtud del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Convenio Europeo de Derechos Humanos).

56 Creada en virtud de la Convención Americana sobre Derechos Humanos (Pacto de San José de Costa Rica).

57 Entre esas organizaciones internacionales se encuentran la Corte Penal Internacional, la Organización Internacional para las Migraciones y la Organización para la Prohibición de las Armas Químicas, así como mecanismos de derechos humanos como los procedimientos especiales y las comisiones de investigación del Consejo de Derechos Humanos o sus equivalentes. Los procedimientos especiales ejercen su mandato en relación con todos los Estados Miembros de las Naciones Unidas; no dependen de la ratificación de un tratado concreto. Existen diferencias en las normas jurídicas y en los procedimientos de estos mecanismos de derechos humanos, así como en los métodos y normas de recogida de información. Por ejemplo, el principal método de trabajo del Grupo de Trabajo sobre la Detención Arbitraria consiste en recibir información sobre casos individuales de las personas afectadas, sus familiares o representantes, Gobiernos, ONG e instituciones nacionales. A continuación, el Grupo de Trabajo investiga los casos denunciados en las comunicaciones, en ocasiones visitando el país. Véase A/HRC/36/38 para consultar la versión más reciente de los métodos de trabajo del Grupo de Trabajo. Las comisiones de investigación, por el contrario, son creadas por el Consejo de Derechos Humanos para un fin concreto, y normalmente inician sus propias investigaciones de acuerdo con lo establecido en su mandato, a menudo realizando visitas a los países, durante las cuales, entre otras cosas, entrevistan a testigos. Véase, por ejemplo, el mandato de la Comisión de Investigación sobre Burundi. Disponible en www.ohchr.org/Documents/HRBodies/HRCouncil/CoIBurundi/TermsofreferenceCOIBurundiENGL.pdf.

58 Véase, por ejemplo, ACNUDH, "Vídeos sobre los órganos de tratados". Disponible en www.ohchr.org/es/treaty-bodies/videos-about-treaty-bodies.

59 Los informes pueden adoptar la forma de observaciones finales, mediante las cuales un órgano de tratado examina los informes presentados por los Estados partes y otros actores interesados en relación con el cumplimiento de las obligaciones que incumben al Estado en virtud de un tratado concreto. Algunos órganos de tratados también pueden publicar informes sobre investigaciones. Véase, por ejemplo, Comité para la Eliminación de la Discriminación contra la Mujer, "Procedimiento de investigación". Disponible en www.ohchr.org/es/treaty-bodies/cedaw/inquiry-procedure.

60 Los órganos de tratados emiten dictámenes sobre las denuncias individuales presentadas por particulares. Véase, en general, ACNUDH, "Órganos de tratados de derechos humanos – Comunicaciones de particulares". Disponible en www.ohchr.org/es/treaty-bodies/human-rights-treaty-bodies-individual-communications.

61 Véase ACNUDH, "Observaciones generales Órganos de los Tratados". Disponible en www.ohchr.org/es/treaty-bodies/general-comments.

62 Véase, en general, ACNUDH, "Procedimientos Especiales del Consejo de Derechos Humanos". Disponible en www.ohchr.org/es/special-procedures-human-rights-council.

determinación de los hechos y las comisiones de investigación.

46. De manera semejante al derecho internacional humanitario, el derecho internacional de los derechos humanos ha pasado a formar parte del marco jurídico de muchos países que, como resultado de tradición jurídicas monistas, por lo que aplican directamente las obligaciones internacionales en el ámbito nacional, o bien que integran directamente el derecho internacional en la legislación nacional o a través de la aplicación del principio de la jurisdicción universal, con lo que se ha establecido un volumen considerable de jurisprudencia sobre dicho derecho[63].

3. Derecho penal internacional

47. El derecho penal internacional se aplica tanto en tiempos de paz como durante conflictos armados, al imponer responsabilidad penal a aquellas personas que cometen crímenes de derecho internacional, como los crímenes de guerra, crímenes de lesa humanidad y genocidio[64]. Estos crímenes se denominan a veces colectivamente "crímenes atroces"[65] o "graves crímenes internacionales", y fueron codificados en gran medida en el Estatuto de Roma, que se considera en general un reflejo del derecho penal internacional consuetudinario. El derecho penal internacional también incluye algunos crímenes que no están codificados en el Estatuto de Roma, como el terrorismo[66]. En ocasiones puede haber cierto superposición entre el derecho penal internacional y el ámbito conexo del derecho penal transnacional, que penaliza actos transfronterizos como la trata de personas y el tráfico de drogas, armas y otras mercancías ilícitas[67]. A diferencia del derecho internacional humanitario y del derecho internacional de los derechos humanos, el derecho penal internacional se centra en la responsabilidad penal individual más que en la responsabilidad del Estado. Las causas de derecho penal internacional pueden ser juzgadas en tribunales penales nacionales, tribunales penales híbridos[68], cortes o tribunales penales internacionales[69], incluida la Corte Penal Internacional, o tribunales nacionales que ejercen la jurisdicción universal. Las fuentes del derecho penal internacional incluyen los documentos constitutivos de las cortes y tribunales (por ejemplo, las resoluciones del Consejo de Seguridad, los estatutos, las reglas de procedimiento y prueba, y los reglamentos de los tribunales) y la legislación nacional de los Estados cuyos tribunales ejercen su jurisdicción sobre los crímenes internacionales. Otra fuente importante del derecho penal internacional es la jurisprudencia, que puede ser vinculante o indicativa, en función de la jurisdicción[70].

B. Competencia y establecimiento de la responsabilidad

48. La competencia es un término jurídico que se refiere a la autoridad otorgada a una entidad jurídica, como un tribunal o corte, para prescribir, juzgar y hacer cumplir una ley. La justicia y el establecimiento de la responsabilidad se definen de manera general en el Protocolo para referirse a diferentes tipos de procesos judiciales y no judiciales.

---

63 Amnistía Internacional, *Universal Jurisdiction: A Preliminary Survey of Legislation Around the World – 2012 Update* (Londres, 2012), págs. 1 y 2.

64 Robert Cryer, Darryl Robinson y Sergey Vasiliev, *An Introduction to International Criminal Law and Procedure*, 4ª ed. (Cambridge, Reino Unido, Cambridge University Press, 2019), cap. 15.

65 Aunque el término "depuración étnica" no está incluido en el Estatuto de Roma y no está definido como crimen independiente en el derecho internacional, se ha considerado que pertenece a la categoría de "crímenes atroces". En este contexto, véase Naciones Unidas, "Marco de análisis para crímenes atroces: una herramienta para la prevención", pág. 1. Disponible en www.un.org/es/preventgenocide/adviser/pdf/Framework%20of%20Analysis%20for%20Atrocity%20Crimes_SP.pdf.

66 Véase la resolución 1757 (2007) del Consejo de Seguridad, anexo, Apéndice (Estatuto del Tribunal Especial para el Líbano), art. 2.

67 Cryer, Robinson y Vasiliev, *An Introduction to International Criminal Law and Procedure*, cap. 15.

68 En este término se engloban, por ejemplo, las Salas Especiales de los Tribunales de Camboya, el Tribunal Especial para Sierra Leona, el Tribunal Especial para el Líbano, las Salas Especializadas y la Fiscalía Especializada de Kosovo y el Tribunal Penal Especial de la República Centroafricana.

69 Este término incluye la Corte Penal Internacional (permanente) y el Tribunal Internacional para la ex-Yugoslavia, el Tribunal Penal Internacional para Rwanda y el Mecanismo Residual Internacional de los Tribunales Penales *(ad hoc)*.

70 Véase Rosa Theofanis, "The doctrine of res judicata in international criminal law", *International Criminal Law Review*, vol. 3, núm. 3 (2003).

El establecimiento de la responsabilidad por la comisión de crímenes internacionales y violaciones del derecho internacional de los derechos humanos o del derecho internacional humanitario puede ser el resultado de procesos judiciales, que pueden ser de naturaleza penal, civil o administrativa, así como de procesos no vinculantes jurídicamente, como los informes de las investigaciones internacionales de derechos humanos, incluidas las comisiones de investigación y las misiones de determinación de hechos, incluyendo también otros mecanismos de justicia transicional, como las iniciativas que se centran en la búsqueda de la verdad. Siempre que sea posible, las personas que investigan deben esforzarse por tener en cuenta todas las jurisdicciones en que se puede tratar de establecer responsabilidades.

49. Las personas que realizan investigaciones en fuentes abiertas deben determinar qué mecanismos de rendición de cuentas pueden ser de interés para su trabajo y qué instancias podrían admitir las pruebas recogidas para establecer los hechos. Sin embargo, esto no es siempre claro o puede ser imposible de determinar en las primeras fases de las investigaciones internacionales, especialmente si el Estado en que se cometieron los crímenes no cuenta con un sistema judicial que funcione o cuando la comunidad internacional aún no está plenamente dispuesta a investigar el asunto. Además, en ocasiones no es posible prever todas las jurisdicciones que podrían ser relevantes en el futuro. Cuando las personas que investigan en fuentes abiertas no conocen el mecanismo o la jurisdicción específica, deben esforzarse por recolectar y preservar la información para maximizar su utilización en el mayor número de jurisdicciones potencialmente relevantes. Si conocen los requisitos particulares de la instancia en que finalmente se juzgará el caso, deben adaptar sus procesos a dichos requisitos.

50. La competencia jurisdiccional puede establecerse de las siguientes maneras:

a) La jurisdicción territorial es la autoridad de un tribunal o corte para conocer de las causas relacionadas con hechos ocurridos en un territorio definido. En el caso de los tribunales internacionales, la jurisdicción territorial suele limitarse a los territorios de los Estados que han ratificado el tratado constitutivo;

b) La jurisdicción temporal es la autoridad de un tribunal o corte para conocer de las causas en que los presuntos hechos tuvieron lugar durante un período determinado;

c) La competencia por razón de la persona es la autoridad de un tribunal o corte para tomar decisiones respecto de una de las partes en el procedimiento;

d) La competencia por razón de la materia es la autoridad de un tribunal o corte para conocer de un tipo particular de causas relacionadas con una materia específica;

e) La competencia o jurisdicción universal es la jurisdicción que ejerce un tribunal sobre una persona acusada, cualquiera que sea el lugar en que se haya cometido el presunto delito, y cualesquiera que sean la nacionalidad de dicha persona, su país de residencia o cualquier otra relación con la entidad acusadora.

C. Facultades y deberes investigativos

51. Las facultades formales para investigar son las que la ley confiere a una entidad específica para investigar dentro de una jurisdicción determinada. Al igual que los límites de la autoridad judicial, las entidades judiciales o fiscales solo pueden realizar investigaciones en la medida en que estén autorizadas para ello por la ley[71]. Las facultades para investigar pueden incluir la capacidad de hacer comparecer a testigos, ordenar la entrega de documentación y ejecutar órdenes de allanamiento. Las entidades investigadoras pueden estar obligadas por ley a seguir procedimientos estrictos o, en algunos casos, pueden elegir sus propios procedimientos[72].

52. La mayoría de las demás personas que investigan violaciones del derecho internacional no suelen estar dotadas de facultades para investigar ni de medios ejecutables para la recolección de pruebas, como citaciones u órdenes de

[71] Véase Justia, "Agency investigations". Disponible en www.justia.com/administrative-law/agency-investigations.

[72] *Ibid.*

allanamiento. Por lo tanto, en muchos casos dependen totalmente de la información de fuentes abiertas y de la información proporcionada voluntariamente, como documentos, archivos digitales y "testimonios de testigos".

53. En general, las facultades para investigar van acompañadas de deberes definidos[73]. Aunque algunas personas investigadoras pueden no tener facultades policiales o alguna otra autoridad legal, se recomienda que, en la medida de lo posible, todas ellas traten de cumplir con los principales deberes de las entidades investigadoras legales, al objeto de garantizar la calidad de las investigaciones. Los deberes y obligaciones comunes de las entidades investigadoras judiciales y fiscales incluyen el deber de investigar las circunstancias incriminatorias y eximentes, el deber de proteger a las personas testigos, el deber de preservar las pruebas, el deber de garantizar la equidad del procedimiento y la obligación de respetar los derechos de las personas acusadas.

54. En juicios penales, las fiscalías o procadurías también estás obligadas a revelar tanto información como medios de prueba a la defensa[74]. Esto incluye no solo los medios de prueba admitidos en el juicio, sino también cualquier información recogida mediante una investigación que sea incriminatoria o eximente, incluida la información relacionada con la credibilidad de las personas testigos[75]. Existen algunas excepciones relacionadas con información reservada o información que podría poner en peligro a una persona. Los tribunales pueden ordenar que no se revele la identidad de una víctima o testigo que pueda correr peligro por dicha revelación, pero esa posibilidad nunca está garantizada[76]. Muchas jurisdicciones penales tienen normas de revelación que obligan a fiscales o procuradores a que entreguen a la defensa toda la información que sea potencialmente exculpatoria[77]. Las personas que realizan investigaciones en fuentes abiertas sobre cualquier caso que tenga la más mínima posibilidad de acabar en los tribunales deben tener en cuenta estas obligaciones de revelación al realizar su trabajo[78]. Existen otras razones por las que la posibilidad de que se tenga que revelar la información es importante para la investigación. Por ejemplo, si la acusación está obligada a examinar todo el material recolectado en una investigación, se debe actuar con cautela al recoger datos de forma masiva, ya que el examen de un gran volumen de información puede resultar excesivamente oneroso o incluso imposible. Esto también es importante para la preservación y almacenamiento de la información recogida, que debe por ello etiquetarse adecuadamente para ayudar significativamente a quienes deban recuperar y examinar el material posteriormente.

---

73 Por ejemplo, el artículo 54 del Estatuto de Roma define las funciones y atribuciones de la Fiscalía con respecto a las investigaciones, y establece su capacidad para, entre otras cosas, llevar a cabo investigaciones, reunir y examinar pruebas, interrogar a víctimas y testigos y cooperar con Estados y organizaciones internacionales.

74 Véase, por ejemplo, Tribunal Internacional para la ex-Yugoslavia, Rules of Procedure and Evidence, regla 66 A); Tribunal Penal Internacional para Rwanda, Rules of Procedure and Evidence, regla 66 A); Tribunal Especial para el Líbano, Rules of Procedure and Evidence, regla 110 A).

75 Véase, por ejemplo, Corte Penal Internacional, Rules of Procedure and Evidence, reglas 76 a 84; Tribunal Internacional para la ex-Yugoslavia, Rules of Procedure and Evidence, regla 66 A) ii); Tribunal Penal Internacional para Rwanda, Rules of Procedure and Evidence, regla 66 A) ii); Tribunal Especial para Sierra Leona, Rules of Procedure and Evidence, regla 66 A) ii); Tribunal Especial para el Líbano, Rules of Procedure and Evidence, regla 110 A) ii); Salas Especiales de Delitos Graves de Timor Oriental, Transitional Rules of Criminal Procedure, regla 24.4.

76 Véase, por ejemplo, Corte Penal Internacional, Rules of Procedure and Evidence, regla 81, párrafo 4; Tribunal Internacional para la ex-Yugoslavia, Rules of Procedure and Evidence, regla 69; Tribunal Penal Internacional para Rwanda, Rules of Procedure and Evidence, regla 69; Tribunal Especial para Sierra Leona, Rules of Procedure and Evidence, regla 69; Tribunal Especial para el Líbano, Rules of Procedure and Evidence, reglas 115 y 116; Salas Especiales de Delitos Graves de Timor Oriental, Transitional Rules of Criminal Procedure, regla 24.6.

77 Véase, por ejemplo, Tribunal Internacional para la ex-Yugoslavia, Rules of Procedure and Evidence, regla 68; Tribunal Penal Internacional para Rwanda, Rules of Procedure and Evidence, regla 68; Tribunal Especial para Sierra Leona, Rules of Procedure and Evidence, regla 68; Tribunal Especial para el Líbano, Rules of Procedure and Evidence, regla 113; Estatuto de Roma de la Corte Penal Internacional, art. 67, párr. 2; Salas Especiales de Delitos Graves de Timor Oriental, Transitional Rules of Criminal Procedure, regla 24.4 c). Las pruebas exculpatorias son aquellas que pueden eximir de responsabilidad a una persona acusada. En los Estados Unidos, la doctrina Brady es una norma de revelación de información previa al juicio establecida por el Tribunal Supremo que obliga a la acusación en una causa penal a revelar a la defensa todos los medios de prueba con carácter exculpatorio. Véase *Brady v. Maryland*, 378 U.S. 83 (1963).

78 Dado que las obligaciones de revelación pueden entrañar que se deba entregar a la defensa una parte o la totalidad del material recogido, la capacidad de las personas investigadoras en fuentes abiertas para proteger las identidades y otra información comprometedora puede resultar anulada.

D. Reglas de procedimiento y prueba

55. En el contexto de una investigación judicial, la principal tarea de los investigadores e investigadoras de fuentes abiertas es recoger información que sea pertinente y auténtica, de modo que pueda utilizarse para extraer conclusiones fácticas y jurídicas. Especialmente en los tribunales y cortes internacionales, se debe procurar que los medios de prueba de fuentes abiertas que se recolecten sean admisibles, pertinentes, fiables y probatorios. Las investigaciones penales se distinguen de las investigaciones realizadas con otros fines por el mayor grado de prueba exigido[79] y por contar con reglas de procedimiento y prueba más estrictas, como el estándar de admisibilidad de las mismas, al objeto de proteger las garantías procesales y el derecho a un juicio imparcial de las personas acusadas[80]. Aunque el umbral de admisibilidad de los medios de prueba en las cortes y tribunales penales internacionales es en general, más bajo que el de tribunales nacionales, los métodos de recolección de pruebas inciden no obstante en el peso que da la autoridad judicial a las mismas. Esto es cierto en todas las jurisdicciones. En esta época marcada por la proliferación de la información digital, así como de informaciones erróneas y desinformación[81], es crucial que las personas investigadoras sean capaces de determinar si la información de fuentes abiertas es auténtica y de establecer o refutar su veracidad con suficiente exactitud[82].

56. En el caso de los procedimientos judiciales, la admisibilidad se refiere a un material presentado dentro del procedimiento que puede constar en acta como medio de prueba. En general, los tribunales penales internacionales evalúan la admisibilidad de los materiales presentados atendiendo a tres factores: a) relevancia; b) valor probatorio; y c) valor probatorio ponderado frente a cualquier efecto perjudicial para la equidad del juicio[83]. El elemento se considera relevante si aumenta o disminuye la probabilidad de un hecho, mientras que el valor probatorio se refiere a si el elemento ayuda a probar o refutar un hecho del caso. En el caso de las investigaciones no judiciales, se aplica una evaluación similar a la de la admisibilidad. Cada fragmento de información debe ser evaluado para verificar su fiabilidad, relevancia y valor probatorio y determinar si debe ser utilizado, y cómo, para extraer las conclusiones jurídicas o fácticas[84].

57. Por "peso" se entiende el valor que se atribuye a un elemento y el grado en que, en última instancia, se utilizará para extraer una conclusión jurídica o fáctica. La ponderación o determinación del peso debe ser una evaluación holística que depende, en parte, del resto de la información que pueda respaldar, corroborar o contradecir el hecho en cuestión. En muchos procedimientos judiciales, la admisibilidad y el peso se evalúan por separado. En otros contextos, en situaciones en las que la admisibilidad de las pruebas no sea relevante, los investigadores e investigadoras de derechos humanos aplicarán

79 Por ejemplo, mientras que los tribunales internacionales suelen aplicar el criterio de derecho penal según el cual los hechos deben quedar demostrados "más allá de toda duda razonable", las comisiones de investigación y otros órganos similares han tendido a apoyarse más en el criterio menos estricto de los "motivos razonables para creer" al fundamentar sus conclusiones. Para más información, véase ACNUDH, *Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice*, págs. 62 y 63.

80 Corte Penal Internacional, *Prosecutor v. Jean-Pierre Bemba*, causa núm. ICC-01/05-01/08 A, Judgment on the Appeal of Mr Jean-Pierre Bemba Gombo against Trial Chamber III's "Judgment pursuant to Article 74 of the Statute", 8 de junio de 2018, Sala de Apelaciones, voto particular de la Magistrada Van den Wyngaert y del Magistrado Morrison, párr. 5.

81 La información errónea es una información que es falsa pero que no tiene la intención de causar daño. Por ejemplo, las personas que no saben que una información es falsa pueden difundirla en las redes sociales con la intención de ayudar. La desinformación es una información falsa que se crea o difunde deliberadamente con el propósito expreso de causar daño. Los productores de desinformación suelen tener móviles políticos, económicos, psicológicos o sociales. Véase Claire Wardle, "Information disorder: the essential glossary" (Cambridge (Massachusetts), Shorenstein Center on Media, Politics and Public Policy, 2018). Disponible en https://firstdraftnews.org/wp-content/uploads/2018/07/infoDisorder_glossary.pdf?x32994.

82 *Ibid.*

83 Con arreglo al Estatuto de Roma (arts. 64, párr. 9 a), y 69, párr. 4), la Sala de Primera Instancia de la Corte Penal Internacional "podrá, a petición de una de las partes o de oficio, [...] decidir sobre la admisibilidad o pertinencia de las pruebas [...] teniendo en cuenta, entre otras cosas, su valor probatorio y cualquier perjuicio que pueda suponer para un juicio justo o para la justa evaluación del testimonio de un testigo, de conformidad con las Reglas de Procedimiento y Prueba".

84 Véase, por ejemplo, ACNUDH, *Commissions of Inquiry and Fact-Finding Missions on International Human Rights and Humanitarian Law: Guidance and Practice*, en particular el cap. IV.C, sobre la recogida y evaluación de la información.

un enfoque similar para evaluar el peso que debe atribuirse a la información.

58. Las reglas de procedimiento y prueba aplicables a los procedimientos penales internacionales pueden encontrarse en los instrumentos constitutivos de cada tribunal, más comúnmente en sus reglas de procedimiento y prueba. La jurisprudencia proporciona más orientación. En función de la naturaleza de una investigación, puede valer la pena ponerse en contacto con juristas con experiencia para obtener asesoramiento, sobre todo si con la investigación se pretende contribuir a un procedimiento judicial.

59. La información de fuentes abiertas puede ser una combinación de pruebas documentales y testimoniales. Por ejemplo, un video de una persona haciendo declaraciones tendrá que ser autenticado y las declaraciones hechas en él tendrán que ser verificadas por separado[85]. Por lo tanto, los medios de autenticación del material digital ya sea como documento, como evaluación de su fiabilidad y admisibilidad o prueba testimonial podrían ser relevantes. Las personas investigadoras deben estar conscientes de la forma en que se trata cada categoría probatoria en la jurisdicción correspondiente. En muchos casos, las pruebas documentales pueden admitirse aunque no se conozca la identidad del autor o este no se encuentre en condiciones de testificar. También pueden ser admisibles sin tener que presentar el documento por conducto de un testigo que pueda autenticarlo, siempre que la parte que lo presenta pueda demostrar con claridad y especificidad dónde y cómo ese documento encaja en el caso[86].

60. En las situaciones en que la responsabilidad de los delitos e infracciones se atribuye a quienes están en un nivel superior en la cadena de mando, la información recogida no solo puede utilizarse para establecer la "base del delito" (véase más abajo), sino que también puede ser relevante para probar el modo de responsabilidad[87] del presunto autor o autores individuales[88]. Una persona puede ser considerada responsable cuando cada uno de los elementos del delito o infracción, incluidos los actos materiales *(actus reus)* y el estado mental del acusado *(mens rea)*, se demuestran según el criterio de prueba aplicable. Para tomar esa decisión, se debe examinar la información presentada con respecto a cada elemento de la violación o delito. Las personas que investigan deben saber qué delitos o infracciones pueden alegarse, los elementos de cada uno, a quién se acusa de haberlos cometido y con arreglo a qué supuesto de responsabilidad. En los casos de

85 Véase Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley, "Digital fingerprints: using electronic evidence to advance prosecutions at the International Criminal Court" (Berkeley, 2014). Disponible en www.law.berkeley.edu/files/HRC/Digital_fingerprints_interior_cover2.pdf. Las pruebas "de oídas" son informaciones de las que la persona que declara como testigo no tiene conocimiento directo. En algunas jurisdicciones, las pruebas de oídas son inadmisibles a menos que cumplan los criterios de una excepción concreta. En otras, son admisibles pero se les da poca importancia porque no pueden ser probadas adecuadamente durante el examen de la persona testigo por la acusación o por la defensa. Según la Organización para la Seguridad y la Cooperación en Europa, "mientras que las pruebas de oídas no suelen ser admisibles en las jurisdicciones de *common law*, salvo en circunstancias especiales, no existe ninguna prohibición de las pruebas de oídas en las jurisdicciones de derecho civil ni en los tribunales internacionales". Véase Organización para la Seguridad y la Cooperación en Europa, Misión en Bosnia y Herzegovina, *Investigation Manual for War Crimes, Crimes Against Humanity and Genocide in Bosnia and Herzegovina* (Sarajevo, 2013), pág. 26. Disponible en www.osce.org/bih/281491?download=true. A pesar de esta falta de obstáculos en las jurisdicciones de derecho civil y en los tribunales internacionales, por regla general, las pruebas de oídas se consideran una categoría de pruebas indirectas especialmente poco fiable y las autoridades judiciales suelen darles relativamente poca importancia.

86 Véase, por ejemplo, Tribunal Internacional para la ex-Yugoslavia, *Prosecutor v. Pavle Strugar*, causa núm. IT-01-42-T, Decision on the Admissibility of Certain Documents, 26 de mayo de 2004, Segunda Sala de Primera Instancia, y *Prosecutor v. Milan Milutinović et al.*, causa núm. IT-05-87-T, Decision on Prosecution Motion to Admit Documentary Evidence, 10 de octubre de 2006, Sala de Primera Instancia; Tribunal Penal Internacional para Rwanda, *Prosecutor v. Edouard Karemera et al.*, causa núm. ICTR-98-44-T, Decision on Joseph Nzirorera's Motion to Admit Documents from the Bar Table: Public Statements and Minutes, 14 de abril de 2009, Tercera Sala de Primera Instancia; Corte Penal Internacional, *Prosecutor v. Thomas Lubanga Dyilo*, causa núm. ICC-01/04/-01/06, Decision on the Admission of Material from the "Bar Table", 24 de junio de 2009; Tribunal Internacional para la ex-Yugoslavia, *Prosecutor v. Radovan Karadžić*, causa núm. IT-95-5/18-PT, Order on Prosecution Request for Clarification and Proposal concerning Guidelines for the Conduct of Trial, 20 de octubre de 2009, Sala de Primera Instancia, y *Prosecutor v. Radovan Karadžić*, causa núm. IT-95-5/18-T, Decision on the Prosecution's First Bar Table Motion, 13 de abril de 2010, Sala de Primera Instancia; Corte Penal Internacional, *Prosecutor v. Germain Katanga and Mathieu Ngudjolo Chui*, causa núm. ICC-01/04-01/07, Decision on the Prosecutor's Bar Table Motions, 17 de diciembre de 2010, Segunda Sala de Primera Instancia.

87 Cryer, Robinson y Vasiliev, *An Introduction to International Criminal Law and Procedure*, cap. 15.

88 Véase ACNUDH, *Who's Responsible? Attributing Individual Responsibility for Violations of International Human Rights and Humanitarian Law in United Nations Commissions of Inquiry, Fact-Finding Missions and Other Investigations* (Nueva York y Ginebra, 2018). Disponible en www.ohchr.org/sites/default/files/Documents/Publications/AttributingIndividualResponsibility.pdf.

derecho penal internacional, se suele distinguir entre las "pruebas basadas en el delito" y las "pruebas de vinculación". Las diferencias entre ambos conceptos son las siguientes:

a) Las pruebas basadas en el delito son pruebas de los delitos en que se fundamentan los cargos, como la información sobre quién, qué, dónde y cuándo[89]. Por ejemplo, si se acusa al presunto autor de un asesinato de cometer un crimen de lesa humanidad, cualquier información que demuestre que hubo un asesinato se considera una prueba basada en el delito;

b) Las pruebas de vinculación son los medios que demuestran la responsabilidad del presunto autor de los delitos cometidos, que son especialmente importantes si el autor no cometió directamente el delito[90]. Es decir, son las pruebas que conectan a la parte responsable con el delito. Por ejemplo, en los casos en que se alega que un superior no impidió o castigó presuntas infracciones de las que tenía conocimiento, las pruebas de vinculación son las que demuestran ese conocimiento o el hecho de que el superior tenía el "control efectivo" del autor directo.

E. El derecho a la privacidad y a la protección de datos

61. El derecho a la privacidad es un derecho humano fundamental[91]. Uno de sus elementos importantes es el derecho a la protección de los datos personales, que se ha articulado en diversas leyes de protección de datos[92]. En particular, las leyes de protección de datos y privacidad son cada vez más relevantes para las investigaciones que utilizan la tecnología digital de la información y las comunicaciones (TIC). A continuación se ofrece un breve resumen de los conceptos del derecho humano internacional a la privacidad y del marco global relativo a la protección de datos, la seguridad de los datos y el intercambio de datos que deben conocer los investigadores e investigadoras en fuentes abiertas. En el entorno digital, la privacidad informativa, que engloba la información que existe o puede obtenerse sobre una persona, es de especial importancia[93].

62. Las personas que realizan investigaciones en fuentes abiertas deben respetar los derechos humanos y tener especialmente presente el derecho a la privacidad, que entra con frecuencia en juego en el contexto de la información digital. Por ejemplo, la violación del derecho a la privacidad es uno de los pocos motivos por los que los magistrados y magistradas pueden excluir pruebas en la Corte Penal Internacional[94]. La privacidad sustenta y protege la dignidad humana y otros valores fundamentales, como la libertad de asociación y la libertad de expresión. El Tribunal Europeo de Derechos Humanos ofrece algunas de las interpretaciones más rigurosas de las leyes de privacidad, con una jurisprudencia en rápido crecimiento sobre las cuestiones de los derechos digitales. Las violaciones de estos derechos fundamentales darán lugar inevitablemente a impugnaciones de la defensa en los procedimientos penales y podrían incluso dar lugar a demandas civiles contra la parte investigadora. Además de las leyes de privacidad, numerosas leyes y reglamentos de

89 Kelly Matheson, *Video as Evidence Field Guide* (WITNESS, 2016), pág. 42. Disponible en https://vae.witness.org/video-as-evidence-field-guide.

90 *Ibid.*

91 El derecho a la privacidad está incluido en numerosos instrumentos de derechos humanos y en los estatutos constitucionales de más de 130 países. Véanse, por ejemplo, la Declaración Americana de los Derechos y Deberes del Hombre, art. V; el Convenio Europeo de Derechos Humanos, art. 8; la Convención Americana sobre Derechos Humanos, art. 11; la Convención sobre los Derechos del Niño, art. 16; la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de Sus Familiares, art. 14; la Carta Africana sobre los Derechos y el Bienestar del Niño, art. 10; la Carta Árabe de Derechos Humanos, arts. 16 y 21; y la Declaración de Derechos Humanos de la Asociación de Naciones de Asia Sudoriental, art. 21. Véase también Privacy International, "What is privacy?", 23 de octubre de 2017. Disponible ent https://privacyinternational.org/explainer/56/what-privacy.

92 Existen leyes de protección de datos en más de 100 países y en numerosos instrumentos internacionales y regionales. Véase, por ejemplo, Organización de Cooperación y Desarrollo Económicos, Directrices sobre la protección de la vida privada y la transmisión transfronteriza de datos personales; Consejo de Europa, Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; Carta de los Derechos Fundamentales de la Unión Europea; Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico; y Ley Complementaria sobre la Protección de los Datos Personales en la Comunidad Económica de los Estados de África Occidental.

93 Véase, en general, A/HRC/39/29, párr. 5.

94 Véase el Estatuto de Roma, art. 69, párr. 7.

protección de datos contribuyen a garantizar la seguridad de los datos personales. En particular, las personas que realizan investigaciones en fuentes abiertas deben tener presente el Reglamento 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos), y su enfoque de la protección de los datos personales, ya que este instrumento ha establecido un umbral alto y otros Estados están estudiando la posibilidad de aprobar uno similar[95]. Sin embargo, las normativas de protección de datos difieren de un país a otro, con variaciones significativas e incluso a veces con normas directamente opuestas. Las personas que investigan en fuentes abiertas deben consultar a juristas con experiencia para conocer bien las leyes y reglamentos de protección de datos aplicables en las jurisdicciones en que trabajan.

63. Por último, las personas que realizan investigaciones con fuentes abiertas deben ser conscientes de la prohibición general del acceso no autorizado a datos y redes. Por ejemplo, no pueden utilizar una contraseña filtrada en un conjunto de datos divulgados sin permiso para acceder a material restringido, ni tampoco acceder a información restringida sin autorización, mediante el engaño u otras formas de ingeniería social[96].

F. Otras consideraciones jurídicas pertinentes

64. Existen otras leyes pueden ser relevantes en el curso de las investigaciones en fuentes abiertas. A continuación se ofrece una lista no exhaustiva de algunas de las consideraciones jurídicas que deben tener presentes las personas que investigan en fuentes abiertas.

1. Incumplimiento de los términos y condiciones

65. Algunas técnicas habituales de investigación en fuentes abiertas incumplen los términos y condiciones de determinados sitios web o plataformas. Por ejemplo, el raspado de datos o el uso de una identidad virtual (no la propia identidad real) infringen las condiciones de utilización de las plataformas y, en particular, de las plataformas de redes sociales[97]. Incumplir los términos y condiciones constituye un incumplimiento de contrato. Los investigadores e investigadoras deben verificar si con ello también cometen un acto ilegal en las jurisdicciones en que trabajan. La necesidad de observar los principios de seguridad al usar una identidad virtual debe sopesarse con los posibles daños derivados del incumplimiento de contrato en tales circunstancias, cuya consecuencia más común es la inhabilitación del acceso del usuario a la plataforma. Sin embargo, si bien el uso de una identidad virtual es necesario cuando se hace simplemente para tareas de búsqueda y seguimiento en fuentes abiertas, como se ha señalado anteriormente, no debe utilizarse una identidad virtual para intentar acceder a contenidos revelados en redes sociales que estén sujetos a controles de acceso restrictivos; o como pretexto para obtener información directamente de una persona adoptando una identidad falsa. Ese comportamiento pondría a la persona investigadora fuera del ámbito de

[95] El Reglamento establece que las personas físicas tienen derechos relacionados con la protección de los datos personales, la protección del tratamiento de los datos personales y la libre circulación de datos personales dentro de la Unión Europea. El Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y, en particular, su Protocolo de 2018 prevén derechos similares. El Convenio vincula no solo a los Estados miembros del Consejo de Europa, sino también a otros Estados.

[96] Según el Instituto Nacional de Normas y Tecnología de los Estados Unidos, la ingeniería social es "el acto de engañar a una persona para que revele información confidencial asociándose con ella para ganar su confianza" (Paul A. Grassi, Michael E. Garcia y James L. Fenton, *Digital Identity Guidelines* (Gaithersburg (Maryland), Instituto Nacional de Normas y Tecnología, 2017), pág. 54. Véase también Michael Workman, "Gaining access with social engineering: an empirical study of the threat", *Information Systems Security*, vol. 16, núm. 6 (2007). Para más información sobre el acceso no autorizado y mediante el engaño, véase el párr. 65. Para más información sobre el camuflaje de usuarios, véase el párr. 107.

[97] Por ejemplo, las condiciones del servicio de Facebook obligan a los usuarios a "usar el mismo nombre que utiliza[n] en [su] vida diaria", "proporcionar información exacta sobre [ellos/ellas]" y "crear solo una cuenta (propia) y usar la biografía para fines personales". Véase https://es-es.facebook.com/legal/terms. La suplantación de identidad infringe las reglas y políticas de Twitter. Véase "Política relativa a las identidades engañosas y que inducen a error" en https//help.twitter.com/es/rules-and-policies/twitter-impersonation-and-deceptive-identities-policy.

la investigación en fuentes abiertas, violaría los principios éticos[98] y podría infringir la ley[99].

2. Leyes de propiedad intelectual

66. Las personas que investigan deben saber qué permisos de propiedad intelectual pueden necesitar para publicar, distribuir o utilizar legalmente la información que han recolectado en el curso de una investigación. Las leyes pertinentes varían de una jurisdicción a otra, aunque la mayoría de las jurisdicciones proporcionan (como mínimo) algún tipo de protección de derechos de autor a quienes crean contenido, como video, fotografías o textos compartidos en línea. El "creador o creadora" suele definirse como la persona que realmente creó el material —por ejemplo, tomando la foto, grabando el video o escribiendo el texto original—; y no la persona que lo sube a Internet, aunque puede tratarse de la misma persona. Es posible que el usuario final tenga que obtener el consentimiento del creador o creadora para el uso propuesto con el fin de evitar una violación de los derechos de autor (por ejemplo, si se utiliza el contenido en un informe público o un artículo periodístico) —el hecho de contar con el consentimiento de la persona que sube el contenido, si no es la misma que lo creó, no suele ser suficiente para evitar el incumplimiento de la ley. Esta es una razón más para intentar localizar la fuente original de cada contenido que los investigadores e investigadoras obtengan. Algunas jurisdicciones (aunque no todas) prevén excepciones a la necesidad de obtener el consentimiento explícito —a menudo denominadas excepciones de "uso justo" o "uso equitativo"— cuando los videos, fotografías, textos o informaciones se utilizan para determinados fines de interés social, como la educación, la labor policial o el periodismo. Sin embargo, estas excepciones, cuando son aplicables, suelen definirse de manera bastante limitada, por lo que nunca debe darse por sentado que un uso concreto entra dentro de esa excepción sin realizar antes un examen minucioso. Algunos mecanismos que a veces pueden minimizar la probabilidad o el alcance de la infracción incluyen proporcionar un enlace al contenido original en un informe digital sin eliminarlo de su fuente original; acreditar al creador o creadora; y utilizar solo una pequeña parte del contenido original, aunque, una vez más, esto depende del contexto específico y de la jurisdicción. La información sujeta a una licencia Creative Commons u otras licencias de libre acceso puede tener una amplia variedad de usos permitidos sin costo alguno. Sin embargo, si el contenido está sujeto a estas licencias libres, es importante cumplir las condiciones de la licencia y no tratarlo como si no hubiera necesidad alguna de permiso.

98 Para más información sobre la tergiversación, véase el cap. II.C, sobre los principios éticos.

99 Véase el cap. III.E, sobre el derecho a la privacidad y a la protección de datos.

IV

SEGURIDAD

RESUMEN DEL CAPÍTULO

- Todas las personas participantes son responsables de garantizar la seguridad de una investigación y de aquellas a quienes afecta, no solo las que trabajan en la tecnología de la información.
- Las consideraciones de seguridad deben ser de dos tipos: a) las relacionadas con la infraestructura, como el *hardware*, el *software* y las redes; y b) las relacionadas con el comportamiento, incluido el de los investigadores e investigadoras y el de todas las personas con las que interactúan.
- Deben realizarse evaluaciones de seguridad en tres niveles: la organización, la investigación o caso específico, y las actividades o tareas específicas.
- Deben diseñarse medidas de protección para mitigar los riesgos y amenazas identificadas en una evaluación de riesgos de la investigación.
- Las evaluaciones de seguridad deben tener en cuenta todos los tipos de daños, incluidos los digitales, económicos, legales, físicos, psicosociales y reputacionales.
- Algunas de las mayores vulnerabilidades de las investigaciones en fuentes abiertas están relacionadas con las conexiones a Internet o direcciones IP, los dispositivos, sus características, y el comportamiento de los usuarios.
- Los investigadores e investigadoras y las entidades de investigación deben recibir capacitación sobre seguridad continua y aplicar medidas de protección que evolucionen a la par de las amenazas o vulnerabilidades.

67. Este capítulo contiene una visión general de las consideraciones de seguridad, tanto en línea como en el mundo real, relacionadas con las investigaciones en fuentes abiertas. Preparándose, invirtiendo y centrándose adecuadamente en la evaluación de las amenazas y la mitigación de riesgos, las personas que realizan investigaciones en fuentes abiertas podrán minimizar el riesgo de infligir daños a personas, datos y otros elementos. La infraestructura de seguridad, que incluye el *hardware*, el *software* y los protocolos de comportamiento de los usuarios, debe estar funcionando, en la medida de lo posible, antes de comenzar la investigación, evaluarse periódicamente y actualizarse cuando sea necesario. El tamaño y los recursos de una organización pueden influir en la viabilidad de determinadas medidas de protección; por ello, este capítulo contiene normas flexibles que deben adaptarse en función de las necesidades específicas de una organización y la investigación correspondiente. Las organizaciones que realizan investigaciones de alto riesgo —como las investigaciones con víctimas especialmente vulnerables o cuando los presuntos autores son agentes estatales o son identificados individualmente— deben contratar servicios de profesionales con experiencia de ciberseguridad. Además, para que el marco de seguridad sea sólido, debe incluir algún tipo de mecanismo de auditoría independiente y una formación continua para que los usuarios puedan estar al día de los nuevos avances tecnológicos y las mejores prácticas.

A. Estándares mínimos

68. Dado que la infraestructura de seguridad y las mejores prácticas de comportamiento de los usuarios cambian constantemente, el Protocolo ofrece principios generales para ayudar a los investigadores e investigadoras con fuentes abiertas a reflexionar sobre la seguridad. Los equipos de investigación deben ser responsables de su propia seguridad, evaluando el riesgo que crea su conducta y poniendo en marcha medidas adecuadas de mitigación de riesgos y protección. Aunque es necesario adoptar un enfoque personalizado e individualizado de la seguridad, hay algunas normas mínimas que los investigadores e investigadoras con fuentes abiertas deben aplicar siempre a su trabajo para cumplir con los principios de seguridad, a saber:

a) Deben evitar revelar elementos identificables sobre ellos mismos, su organización o cualquier asociado o fuente, a menos que sea un objetivo u obligación de la investigación. Por lo tanto, deben mantener el anonimato en línea y asegurarse de que, en la mayor medida posible, sus actividades en línea no sean atribuibles;

b) Deben realizar sus actividades en línea conscientes de que podrían ser observadas y analizadas por terceros. Por lo tanto, deben actuar de manera coherente con su identidad virtual y de forma que no revelen su identidad o los objetivos de su investigación, ni pongan en peligro a sus fuentes humanas o a otras partes;

c) Deben ser conscientes de que la sobrexplotación de una única fuente de información en línea, como un sitio específico, puede aumentar el riesgo de ser observados y analizados por terceros. Por lo tanto, deben adoptar prácticas para minimizar esta probabilidad, como diversificar las fuentes digitales;

d) Deben evitar pautas de comportamiento identificables o previsibles, como patrones de búsqueda repetitivos en dispositivos identificables, que podrían ayudar a terceros a identificar los objetivos de la investigación, así como convertirse ellos mismos en objetivos más fáciles para los ataques de *phishing* y otras formas de ingeniería social[100];

e) Deben mantener sus tareas profesionales separadas de sus actividades personales en línea. No deben utilizar sus cuentas personales en línea y, en la medida de lo posible, sus dispositivos personales para las investigaciones profesionales, y nunca

[100] Más abajo se explican los ataques de *phishing* y de ingeniería social.

deben utilizar los dispositivos profesionales para sus actividades personales en línea[101];

f) Cuando realicen varias investigaciones al mismo tiempo, no deben entremezclarlas. Por lo tanto, deben mantener diferentes horas de inicio y fin para cada actividad de investigación, mantener los datos y la documentación de cada investigación en lugares separados y utilizar diferentes identidades virtuales, si procede[102];

g) Deben utilizar sistemas o entornos técnicos que estén diseñados para minimizar su vulnerabilidad a la posible introducción de *software* hostil o malintencionado u otras influencias perturbadoras que puedan encontrarse durante las actividades.

B. Evaluaciones de seguridad

69. Para establecer un marco de seguridad adecuado y eficaz, las personas que realizan investigaciones en fuentes abiertas deben comprender los conceptos clave de la ciberseguridad y la gestión de riesgos. También deben ser capaces de identificar los bienes que necesitan ser protegidos y los daños potenciales, y evaluar las posibles amenazas, riesgos y vulnerabilidades.

70. El riesgo es la posibilidad de que una amenaza explote una vulnerabilidad, causando la pérdida, daño o destrucción de un bien. Cada uno de estos términos se define más abajo. Dado que las investigaciones con fuentes abiertas realizadas en Internet implican métodos de recolección de información diferentes a los de las investigaciones tradicionales, dan lugar a tipos de riesgos distintos. La identificación y evaluación de estos riesgos es una parte esencial de la planeación y preparación de una investigación. Los riesgos frecuentes en las investigaciones con fuentes abiertas incluyen: los conocimientos y capacidades tecnológicas del objetivo de la investigación, o de las entidades que apoyan al objetivo, que podrían evadir o despistar a las personas que realizan la investigación; los problemas en la configuración técnica del entorno en línea que se utiliza para la investigación, que podrían provocar la exposición de información y con ello comprometer la investigación; la utilización de *software* o códigos malintencionados que podrían comprometer los sistemas computacionales, las actividades, la identidad o los datos recogidos por la investigación; o herramientas técnicas, como rastreadores, *cookies*, balizas y análisis, que podrían comprometer las actividades de investigación.

71. En la siguiente sección se explican los términos clave y su aplicación a las investigaciones en fuentes abiertas, proporcionando así una hoja de ruta para llevar a cabo una evaluación de amenazas y riesgos.

1. Bienes

72. Un bien es todo lo que necesita ser protegido, incluidas las personas[103], las instalaciones y la información. En el contexto de las investigaciones en fuentes abiertas, las personas que requieren protección pueden ser los investigadores o investigadoras, o los equipos de investigación —incluidas las personas con las que trabajen (colegas internos y asociados externos, tanto locales como los que trabajan en el terreno)—, los autores o las fuentes de información, las personas testigos o víctimas, los presuntos autores de las infracciones y los transeúntes. Por instalaciones se entienden todos los elementos tangibles e intangibles a los que se puede asignar un valor[104]. Los bienes tangibles incluyen los edificios, el material y los documentos, mientras que los bienes intangibles incluyen la reputación y la información protegida por derechos de autor, como los datos digitales, los metadatos, las bases de datos, el código de *software* y los registros.

2. Daños

73. Los daños son los perjuicios físicos o mentales que sufren los bienes o la destrucción de los

[101] Si no se puede evitar el uso de material personal, se deben realizar las investigaciones profesionales y las actividades personales en entornos en línea separados, por ejemplo, utilizando una máquina virtual para las investigaciones.

[102] Además de minimizar el riesgo de confundir las investigaciones, estas prácticas ayudarán a preservar la cadena de custodia.

[103] Únicamente se habla de bienes para referirse a personas en el contexto de la realización de evaluaciones de seguridad.

[104] Véase Threat Analysis Group, "Threat, vulnerability, risk – commonly mixed up terms". Disponible en www.threatanalysis.com/2010/05/03/threat-vulnerability-risk-commonly-mixed-up-terms.

mismos. Puede tratarse de daños digitales, económicos, jurídicos, físicos, psicosociales o reputacionales.

a) Daños digitales

74. Los daños digitales son los perjuicios a cualquier información o infraestructura digitales. Pueden incluir la destrucción, manipulación o pérdida de acceso a los datos, o la interrupción de los servicios de los sistemas y plataformas computacionales.

b) Daños económicos

75. Los daños económicos pueden derivarse de varias fuentes, como los daños jurídicos y reputacionales ligados a una investigación. Pueden sufrir estos daños tanto las personas que realizan la investigación, como los objetivos y transeúntes. Además, pueden producirse daños económicos cuando no se evalúan adecuadamente los costos a largo plazo de una investigación.

c) Daños jurídicos

76. Los investigadores e investigadoras de fuentes abiertas pueden incurrir en responsabilidad legal por el proceso o los resultados de su trabajo. Deben ser conscientes de las limitaciones legales de su trabajo y de las ramificaciones jurídicas de sus actos, con el fin de minimizar el riesgo de responsabilidad jurídica para ellos mismos o para terceros. Las investigaciones también pueden provocar daños jurídicos a los sujetos de dichas investigaciones, e incluso a los transeúntes, que pueden verse implicados en actos ilícitos descubiertos en el curso de la investigación[105].

d) Daños físicos

77. Los daños físicos pueden incluir perjuicios a personas o bienes. Aunque las personas que realizan investigaciones con fuentes abiertas suelen trabajar desde una oficina o desde el domicilio, y no sobre el terreno, los daños físicos deben evaluarse como una posible consecuencia de las actividades en línea. Todo lo que se hace en el ciberespacio puede acarrear consecuencias en el mundo real, de las que los investigadores e investigadoras deben ser conscientes y para las que deben prepararse. Por ejemplo, las personas que realizan investigaciones en fuentes abiertas deben ser conscientes de las personas —sean colegas, usuarios en línea en los países donde sucedieron los hechos, u otras— que pueden estar en entornos inseguros y correr el riesgo de sufrir daños físicos como consecuencia de las actividades en línea de la investigación. Los investigadores e investigadoras en línea tienen el deber ético —y en algunos casos legal— de cuidar a los demás[106] para garantizar que quienes corren riesgo de sufrir daños físicos no se vean expuestos a un peligro mayor a causa de sus actividades. Los riesgos físicos deben incluirse en una evaluación completa de las amenazas antes de comenzar el trabajo y reevaluarse a lo largo de toda la investigación.

e) Daños psicosociales

78. Los daños psicosociales pueden incluir desde la angustia psicológica hasta el trauma, y pueden afectar a cualquier miembro de un equipo de investigación o a las personas que participan o se ven afectadas por una investigación, incluidos los sujetos de la investigación y transeúntes. Además de la importancia moral y ética de protegerse a uno mismo y a los demás de los daños psicológicos, los seres humanos pueden ser a veces el eslabón más vulnerable en el funcionamiento de una organización. Un ser humano que sufra daños psicosociales puede ser especialmente vulnerable, creando nuevas oportunidades para que los actores generadores de amenazas las exploten u otros riesgos para la seguridad física y digital, especialmente si los efectos psicológicos negativos dan lugar a un funcionamiento comprometido, como un cumplimiento más laxo de lo habitual de los protocolos de seguridad. Es sabido que el ver grandes cantidades de videos violentos y descarnados es especialmente difícil de procesar, y puede dar lugar a angustia psicológica o a un trauma que puede requerir tratamiento profesional. Los signos de trauma secundario pueden incluir cambios en el comportamiento, cambios de humor, cambios en los hábitos alimenticios o de bebida, incapacidad para dormir, deseo de dormir más de lo habitual

[105] Véanse también los caps. IV.E y IV.F para más información sobre las consideraciones jurídicas pertinentes.

[106] Estatuto de Roma, art. 54, párr. 1 b).

o pesadillas[107]. Las estrategias para mitigar el daño psicosocial se describen en la sección sobre la preparación y creación de un plan de resiliencia y autocuidado[108].

f) Daños reputacionales

79. En el contexto de las investigaciones en fuentes abiertas, los daños reputacionales pueden ser más graves para los investigadores e investigadoras o para sus organizaciones, por ejemplo, si publican información errónea, incumplen los principios éticos o producen contenidos problemáticos. Los daños reputacionales también pueden afectar a los sujetos de las investigaciones, que pueden ser estigmatizados por su supuesto comportamiento una vez que este se hace público. Esto puede ser especialmente preocupante cuando se hacen acusaciones contra personas u organizaciones que luego resultan ser falsas.

3. Medidas de protección

80. Las medidas de protección son las realizados para prevenir o minimizar las vulnerabilidades y pueden incluir medidas físicas, tecnológicas y normativas. La protección física puede incluir la existencia de cerraduras en los edificios, salas o armarios en que se almacena el material confidencial. Las medidas tecnológicas pueden incluir el uso de contraseñas, el cifrado y la autenticación de dos pasos en los dispositivos, o los controles de acceso a los sistemas de datos. Las medidas normativas incluyen las reglas, leyes y mecanismos de aplicación internos y externos, como las reglas que prohíben el envío de productos de trabajo internos desde un correo electrónico de trabajo a un correo electrónico personal o las políticas que prohíben el uso de cuentas personales de redes sociales en la computadora del trabajo.

4. Amenazas

81. Una amenaza es algo contra lo que hay que proteger los bienes en cuestión. Dicho de otro modo, es cualquier cosa que pueda explotar una vulnerabilidad, intencionada o accidentalmente, y obtener, dañar o destruir un bien. Las amenazas pueden ser internas o externas a una organización o investigación, y pueden ser ejecutadas por individuos, grupos, instituciones o redes. Las personas que realizan investigaciones en fuentes abiertas deben ser conscientes de las siguientes amenazas, entre otras.

a) Ataques de denegación de servicio distribuida

82. Los ataques de denegación de servicio distribuida son ciberataques diseñados para interrumpir la capacidad de la entidad objeto del ataque para acceder a una máquina o red. Debe establecerse un sistema para mitigar estos ataques contra los bienes de cara al público, como los sitios web y otros portales accesibles a distancia. Además, debe establecerse un sistema para registrar dichos incidentes y utilizarlo en caso de ataque para registrar las acciones y actores correspondientes.

b) Ataques de *phishing*

83. El *phishing* es el intento fraudulento de obtener información confidencial, como nombres de usuario, contraseñas y datos de tarjetas de crédito, haciéndose pasar por una entidad de confianza en una comunicación electrónica[109]. En ocasiones se utilizan estafas telefónicas o de *phishing* para obtener información confidencial o para acosar a las personas que investigan. Las cuentas personales suelen correr más riesgo que las profesionales, por lo que su uso puede poner en peligro las investigaciones o el producto del trabajo.

---

[107] Véase Dart Center for Journalism and Trauma, "Working with traumatic imagery", 12 de agosto de 2014 (disponible en https://dartcenter.org/content/working-with-traumatic-imagery); Sam Dubberley, Elizabeth Griffin y Haluk Mert Bal, *Making Secondary Trauma a Primary Issue: A Study of Eyewitness Media and Vicarious Trauma on the Digital Frontline* (Eyewitness Media Hub, 2015) (disponible en http://eyewitnessmediahub.com/research/vicarious-trauma); Sam Dubberley y Michele Grant, "Journalism and vicarious trauma: a guide for journalists, editors and news organisations" (First Draft News, 2017) (disponible en https://firstdraftnews.org/wp-content/uploads/2017/04/vicarioustrauma.pdf); Center for Human Rights and Global Justice, "Human rights resilience project launches new website", 21 de mayo de 2018 (disponible en https://chrgj.org/2018/05/21/human-rights-resilience-project-launches-resources-for-resilience-website); Keramet Reiter y Alexa Koenig, "Reiter and Koenig on challenges and strategies for researching trauma", Palgrave MacMillan (disponible en www.palgrave.com/gp/blogs/social-sciences/reiter-and-koenig-on-researching-trauma).

[108] Véase el cap. V.D para más información sobre el autocuidado.

[109] Véase Phishing.org, "What is phishing?". Disponible en www.phishing.org/what-is-phishing.

c) Ataques de intermediario

84. Los ataques de intermediario *(man-in-the-middle)* son un tipo de ciberataque en el que actores malintencionados se insertan en las conversaciones entre dos partes, se hacen pasar por alguna y acceden a la información que estaban tratando de enviarse[110]. Los ataques de intermediario permiten al actor malintencionado interceptar, enviar y recibir datos destinados a otra persona, o no destinados a ser enviados en absoluto, sin que ninguna de las partes externas lo sepa hasta que sea demasiado tarde[111].

d) Ingeniería social

85. La ingeniería social es la manipulación psicológica de las personas para conseguir que realicen una acción potencialmente dañina, como revelar información confidencial. Hay muchos ejemplos diferentes de ingeniería social, como la suplantación de identidad dirigida *(spear phishing)*[112]. Dado que las tácticas de ingeniería social no dejan de adaptarse y evolucionar, los investigadores e investigadoras deben recibir formación continua para detectar y evitar las tácticas de ingeniería social identificadas.

e) *Malware*

86. El *malware*, abreviatura en inglés de *software* malintencionado, son los programas computacionales diseñados para infiltrarse y dañar las computadoras sin el consentimiento del usuario. Hay varios tipos de *malware*, como el *spyware* (programas espía) y el *ransomware* (programas secuestradores).

5. Actores generadores de amenazas

87. Los actores generadores de amenazas o actores malintencionados son personas o entidades responsables de un hecho o incidente que afecta, o podría afectar la seguridad de otra entidad o actor. En las investigaciones de violaciones del derecho penal internacional y el derecho internacional de los derechos humanos, los actores generadores de amenazas pueden ser los presuntos autores, o las personas objeto de una investigación, Gobiernos incluidos, o quienes los apoyan. Es importante que los investigadores e investigadoras de fuentes abiertas identifiquen a los posibles actores generadores de amenazas y comprendan sus capacidades y la probabilidad de que lancen ataques.

6. Vulnerabilidades

88. Una vulnerabilidad es un punto débil o una brecha en las medidas de protección, que puede existir tanto en el ámbito digital como en el mundo real. En actividades en línea, las vulnerabilidades pueden incluir un punto débil en las medidas de protección de la seguridad que podría ser explotada para acceder sin autorización a un bien; defectos de seguridad en el *software*; diseños poco seguros; y usuarios y códigos con más privilegios de los necesarios. En el resto de las actividades, también pueden incluir puntos débiles en las personas, como un miembro del equipo que sea susceptible de ser chantajeado o coaccionado, o que pueda volverse vulnerable por ver demasiado material descarnado, o a causa de otras condiciones de trabajo difíciles[113]. Pueden crearse nuevas vulnerabilidades si la persona objeto de la investigación se entera de que está siendo investigada o si se revela el alcance de la investigación. Por último, las vulnerabilidades de seguridad pueden derivarse de amenazas externas, como nuevos programas malintencionados y virus, que los investigadores e investigadoras deben tener presentes. Estas vulnerabilidades deben tenerse en cuenta en los planes de seguridad y evaluaciones de riesgos.

89. Las personas que investigan en fuentes abiertas también deben ser conscientes de las siguientes vulnerabilidades en línea.

a) *Cookies*

90. Una *cookie* es un pequeño archivo que suele enviarse desde un sitio web y que se almacena en la memoria de la computadora del usuario o se graba en el disco de esta para que lo utilice

[110] Véase Veracode, "Man in the middle (MITM) attack". Disponible en www.veracode.com/security/man-middle-attack.

[111] *Ibid.*

[112] La suplantación de identidad dirigida es la práctica fraudulenta de enviar correos electrónicos aparentemente de un remitente conocido o de confianza con el fin de inducir a las personas que los reciben a revelar información confidencial.

[113] Véase el cap. V.D para más información sobre la resiliencia y el autocuidado.

el navegador. Las cookies son muchas veces necesarias para que un sitio web funcione correctamente, por ejemplo, al ofrecer la posibilidad de almacenar las preferencias del usuario en el sitio web y sus datos de identidad, evitando que tenga que volver a introducir los datos cada vez que lo visite. Las *cookies* se han programado de forma que pueden recoger y almacenar un volumen considerable de datos importantes —a menudo confidenciales— sobre los visitantes y sus visitas. Algunas se han convertido en herramientas centralizadas que pueden utilizarse para recoger datos con los que construir una imagen de los intereses y hábitos de navegación de un usuario. Una *cookie* puede estar presente en una computadora hasta que expire o sea eliminada por el usuario.

b) Rastreadores

91. Los rastreadores son *cookies* que aprovechan la capacidad de los navegadores de registrar las páginas web que se han visitado, criterios de búsqueda que se han introducido, etc. Los rastreadores son *cookies* persistentes que mantienen un registro continuo del comportamiento de los visitantes de un sitio web. En su forma más simple, asignan una identidad única al navegador de un usuario y luego vinculan esa identidad a toda la actividad de navegación y búsqueda posterior (criterios de búsqueda, páginas visitadas, secuencia de páginas visitadas, etc.). Esto permite al propietario del rastreador vincular las visitas anteriores y posteriores a un sitio web (o conjunto de sitios web asociados) para construir una imagen detallada de los usuarios y sus hábitos de navegación. Los rastreadores se incorporan a menudo en los anuncios, que se distribuyen a su vez en distintos sitios web, lo que ofrece al rastreador muchas más posibilidades de seguir la actividad y el comportamiento del usuario. Incluso la visita a un sitio web "de confianza" puede dar lugar a la instalación de rastreadores en la computadora del usuario y al control de sus actividades posteriores en Internet.

c) Balizas

92. Las balizas son mecanismos utilizados para controlar la actividad y el comportamiento del usuario. Están formadas por un elemento pequeño y discreto (a menudo invisible) colocado en una página web (algo tan pequeño como un solo píxel transparente) que, al ser mostrado por un navegador, da lugar a que se envíe a un tercero información sobre ese navegador y la computadora que lo usa. Las balizas pueden utilizarse junto con las *cookies* para activar la recogida y transmisión de datos y para identificar a cada usuario y registrar sus hábitos de navegación. Las balizas están estrechamente relacionadas con las redes sociales, cuya razón de ser es la identificación de las relaciones y las redes del usuario. Por último, las balizas pueden utilizarse en correos electrónicos que usan HTML para recoger información sobre la identidad del usuario y acceder a las *cookies* que se hayan almacenado previamente en la computadora.

d) Otros códigos y secuencias de comandos

93. Cada vez son más los sitios web que utilizan pequeños fragmentos de código que se descargan en el navegador del visitante y que tienen la capacidad de almacenar información sobre la visita. Este código puede influir en la apariencia del sitio web, en la forma en que este reacciona a las entradas de texto y en la forma en que el navegador responde al sitio web. El código también puede almacenar datos confidenciales sobre las credenciales de los visitantes, sus actividades, etc. La recogida de datos puede ser persistente, y podrían enviarse estos datos a terceros.

C. Consideraciones relacionadas con la infraestructura

94. Por infraestructura se entienden las estructuras, instalaciones y sistemas —*software* y *hardware* incluidos— que son necesarios para realizar investigaciones con fuentes abiertas. La infraestructura debe proporcionar e incorporar suficientes medidas de seguridad para proteger y preservar los bienes y datos de una organización. Para reforzar la infraestructura, deben adoptarse medidas de mitigación que garanticen continuidad en caso de que se produzca cualquiera de las siguientes situaciones:

a) Interrupción o pérdida de la conexión a Internet;

b) Interrupción o pérdida de acceso a los datos almacenados;

c) Pérdida, corrupción o destrucción de datos;

d) Interrupción o pérdida de servicios de *software*;

e) Daños en el *hardware* o pérdida del mismo;

f) Acceso no autorizado a dispositivos;

g) Acceso no autorizado a una red;

h) Eliminación o manipulación accidental de datos;

i) Destrucción o manipulación intencionada de datos;

j) Filtración o secuestro de datos.

95. La arquitectura necesaria viene definida por la magnitud de las actividades de investigación en línea que se van a realizar, la naturaleza de la investigación y el sujeto investigado, así como los fondos disponibles para construir, mantener y modificar la infraestructura según sea necesario.

1. Infraestructura

96. La infraestructura utilizada para realizar investigaciones en fuentes abiertas incluirá, como mínimo, los siguientes componentes, además de otras características relacionadas con las estrategias de investigación concretas que se utilicen.

a) Dispositivos

97. Para acceder a los contenidos en línea, los investigadores e investigadoras en fuentes abiertas deben disponer de dispositivos como computadoras de escritorio, computadoras portátiles, tabletas o teléfonos inteligentes. El *hardware* y los dispositivos deben estar protegidos por contraseña, tener activado el cifrado de todo el disco y, si es posible, utilizar la autenticación de dos pasos[114]. En todos los dispositivos se deben realizar copias de seguridad de los datos periódicamente. Cuando no se utilice, el *hardware* debe almacenarse de forma segura, restringiendo el acceso al usuario y personal autorizado. Los dispositivos personales no deben utilizarse para actividades relacionadas con el trabajo. Asimismo, los dispositivos relacionados con la investigación no deben utilizarse para actividades personales, debido al riesgo de vincular las redes sociales personales con las identidades virtuales cultivadas para una investigación[115].

b) Conexión a Internet

98. Lo ideal es que se disponga de una conexión a Internet robusta, estable y privada, y evitar el uso de redes Wi-Fi públicas. Aunque las redes Wi-Fi públicas y gratuitas —incluidas las redes semiprivadas, como las que proporcionan los hoteles o los cibercafés— son una opción cómoda, ofrecen muy poca seguridad y son vulnerables a numerosas amenazas, la mayor de las cuales es la posibilidad de que un pirata computacional *(hacker)* se sitúe entre el usuario y el punto de conexión. El uso de un punto de acceso personal protegido por contraseña requiere sin duda una inversión económica, pero es esencial para realizar actividades de investigación en línea de forma segura. Además, aunque no siempre esté controlada por la persona investigadora, es preferible tener una conexión a Internet robusta y estable, tanto por su funcionalidad como por su seguridad. Si se utiliza una red privada virtual (VPN) en una conexión inestable, se debe emplear un mecanismo a prueba de fallos para garantizar que la dirección IP no quede a la vista si la conexión se interrumpe.

c) Navegadores web

99. Una de las principales herramientas de las investigaciones en línea son los navegadores web, que se utilizan para consultar, buscar y acceder a sitios web publicados en Internet. Los navegadores actúan como la principal interfaz entre los investigadores e investigadoras e Internet, pero a menudo se pasan por alto como fuente de riesgo. Los navegadores modernos se modifican continuamente y tienen una amplia gama de funcionalidades incorporadas para adaptarlos a una multitud de necesidades. Los navegadores son también un objetivo clave

[114] La autenticación multifactorial es un elemento de seguridad que obliga al usuario a presentar dos tipos de credenciales para acceder a una cuenta, por ejemplo, una contraseña y una huella dactilar o una tarjeta inteligente. Véase Estados Unidos, Instituto Nacional de Normas y Tecnología, "Back to basics: multi-factor authentication (MFA)". Disponible en www.nist.gov/itl/applied-cybersecurity/tig/back-basics-multi-factor-authentication.

[115] Esta recomendación puede ser difícil de cumplir durante los viajes, cuando se lleva el dispositivo de trabajo pero se quiere o necesita realizar actividades personales fuera del horario de trabajo. Por lo tanto, las organizaciones que realizan investigaciones en fuentes abiertas deben establecer políticas de viaje razonables.

para quienes desean vigilar a un adversario o lanzar ataques contra él, ya que se puede hacer un uso indebido de las funcionalidades y se pueden añadir otras con relativa facilidad. Los navegadores tienen acceso simultáneo a Internet y a la computadora y, en consecuencia, a información potencialmente identificable sobre el usuario. La filtración de datos mediante un navegador puede revelar datos suficientes para alertar al sujeto de una investigación. Los navegadores modernos tienen varias funcionalidades incorporadas y se les pueden añadir muchas otras, conocidas como complementos, que pueden filtrar datos individual o colectivamente, lo que puede provocar que se identifique una investigación, a un investigador o investigadora, una línea de investigación y las actividades de búsqueda realizadas. Los navegadores también son capaces, por defecto, de descargar y ejecutar código computacional derivado de un sitio web. La presencia o la función del código computacional pueden no ser evidentes para quienes investigan, y sin embargo el código puede ser capaz de alterar el contenido digital que se les muestra, acceder a la funcionalidad y a los datos de sus computadoras e incluso hacer que estas se comporten de una manera diferente a la prevista. Los investigadores e investigadoras en fuentes abiertas deben tratar de minimizar estos riesgos asegurándose de que utilizan navegadores seguros y actualizados que se revisan periódicamente, así como programas computacionales adecuados y complementos instalados que mitiguen algunos de los riesgos descritos[116].

2. Medidas de seguridad

100. Estos elementos esenciales de la infraestructura pueden utilizarse para identificar a los usuarios y su ubicación. Con objeto de observar el principio de anonimato y no atribución, las personas que investigan deben emplear las siguientes estrategias para camuflar sus conexiones a Internet. Estas estrategias ocultan la ubicación y la dirección IP y camuflan la máquina, ocultando sus características identificativas, el sistema operativo y el navegador.

a) Camuflaje de conexión

101. Una dirección IP puede revelar información que podría utilizarse para atacar la infraestructura de una organización. Los investigadores e investigadoras en fuentes abiertas deben tratar de utilizar VPN, servidores intermediarios *(proxies)* u otros programas para ocultar la dirección IP de sus computadoras, de manera que la dirección IP que se revele a Internet no esté vinculada a esas personas ni a su organización. Las VPN también crean un canal cifrado para las comunicaciones entre la computadora de la persona que investiga y el servidor de la VPN, de manera que cualquier red o nodo por el que pase la conexión solo verá datos cifrados, lo que proporciona una capa adicional de protección. Sin embargo, el uso de ciertas VPN está bloqueado por algunos países y sitios web, y puede señalar las actividades de investigación como potencialmente sospechosas para terceros. Normalmente, las VPN permiten a los investigadores e investigadoras utilizar varias direcciones IP con la posibilidad de cambiar rápidamente de una a otra cuando sea necesario. Las direcciones IP no deben reflejar ubicaciones de un solo país, sino que deben dividirse en distintos lugares de todo el mundo.

b) Camuflaje mediante una máquina

102. Para ocultar ciertos elementos que podrían utilizarse para identificar a los usuarios, los investigadores e investigadoras pueden utilizar máquinas virtuales, que son programas computacionales o sistemas operativos que se comportan como computadoras distintas. Al usar una máquina virtual se crea básicamente una nueva computadora dentro de la computadora, un entorno completamente separado del resto de esta. Las máquinas virtuales también son capaces de realizar tareas como ejecutar aplicaciones y programas como si fueran una computadora completamente distinta[117], haciendo que la persona que la utiliza aparezca como un individuo diferente en línea. Las máquinas virtuales permiten a las personas que investigan disponer de un sistema para variar el navegador, el agente

[116] Para más información actualizada sobre los navegadores y otras medidas de seguridad operacional, véase el sitio web del Centro de Recursos de Seguridad Computacional del Instituto Nacional de Normas y Tecnología de los Estados Unidos (https://csrc.nist.gov).

[117] Véase Techopedia, "Virtual machine (VM)", 21 de mayo de 2020. Disponible en www.techopedia.com/definition/4805/virtual-machine-vm.

de usuario, el *software*, los puertos abiertos, el sistema operativo y otra información sobre la máquina para aparecer como un individuo diferente cada vez que se conectan. En circunstancias óptimas, la máquina virtual oculta la máquina real que se está utilizando. Las máquinas virtuales pueden ser destruidas y recreadas, restauradas en un punto anterior, configuradas de diferentes maneras, replicadas para nuevos casos o preservadas para cuando se necesiten en el futuro. Como alternativa, los investigadores pueden adoptar el enfoque más oneroso, pero también relativamente eficaz, de variar su apariencia manualmente, utilizando diferentes navegadores cada vez que se conectan a Internet, cambiando la configuración para limitar la unicidad de las huellas digitales de sus máquinas y utilizando complementos que impidan el rastreo.

3. Otras infraestructuras

103. Antes de comenzar su trabajo, las personas investigadoras deben estudiar la opción de utilizar otras infraestructuras para proteger sus redes e infraestructuras, incluidos los siguientes sistemas:

a) Sistemas de copia de seguridad;

b) Sistemas de registro para supervisar las actividades y controlar las acciones de los usuarios;

c) Sistemas de almacenamiento separados y lugares de almacenamiento adecuados para reunir el material digital identificado durante las búsquedas. Con objeto de proteger los datos frente a todo agente externo, las organizaciones deben contar con plataformas (como depósitos de pruebas, bases de datos u otros sistemas de gestión de la información) que se mantengan separadas de las redes principales. Las plataformas deben tener dos partes principales: una conectada a Internet y la otra desconectada. En algunos casos, puede ser conveniente retirar los datos de las infraestructuras conectadas a Internet a una red o depósito más seguro lo antes posible para que la información pueda ser revisada sin riesgos.

D. Consideraciones relacionadas con la persona usuaria

104. Uno de los puntos más débiles de cualquier marco de seguridad es el usuario. Incluso con una infraestructura perfecta, los principios de seguridad no se respetarán si no se adapta el comportamiento de los usuarios mediante formación periódica y supervisión. La seguridad es responsabilidad de todos. Los investigadores e investigadoras no deben realizar actividades que puedan poner en peligro datos o personas sin una formación adecuada sobre la manera de mitigar esos riesgos. Deben estar capacitados para saber evaluar qué comportamiento es el adecuado en las diferentes actividades en línea.

105. El anonimato puede ayudar a minimizar los daños en las situaciones en que un agente generador de amenazas intente rastrear el origen de la actividad hasta la red o el usuario[118]. Cualquier actividad en línea es vulnerable a ser rastreada por terceros; por lo tanto, las personas que investigan deben asumir dicha amenaza cuando realicen actividades en línea. Los objetos más comúnmente rastreados son la dirección IP, el navegador y la resolución de pantalla (utilizados para identificar el dispositivo), así como el tiempo de navegación y la actividad en los sitios web (como los términos de búsqueda introducidos o las páginas visitadas). Los agentes generadores de amenazas pueden intentar identificar el origen de la actividad en línea. En ese caso, deben ser dirigidos lejos de la verdadera ubicación o identidad de la persona o entidad investigadora. Esto puede hacerse tomando medidas para que en Internet parezca que el acceso se realizó desde otro lugar, utilizando para ello una VPN, por ejemplo, creando y utilizando identidades virtuales[119].

106. Ocultando la conexión y la máquina que se utiliza en una investigación en línea se consigue una protección importante, pero esta puede resultar mermada si un usuario se revela identificándose en un sitio web o, por ejemplo, utilizando información personal para registrarse o iniciar sesión en una plataforma de redes sociales u otra cuenta privada. Los

[118] Rastrear es descubrir el punto de origen de alguien o algo siguiendo un rastro de información o una serie de hechos hacia atrás.

[119] Para más información sobre las identidades virtuales, véanse también los caps. II.C, III.F y IV.A y C.

investigadores e investigadoras nunca deben utilizar sus cuentas personales para investigar ni acceder a cuentas personales en un navegador que se utilice para realizar investigaciones en fuentes abiertas. Algunas cuentas requieren el uso de fotografías, números de teléfono o correos electrónicos para poder crearlas. Nunca deben utilizarse fotografías, número de teléfonos, correos electrónicos o datos que sean personales o atribuibles a las personas que investigan o a otras personas.

Camuflaje del usuario

107. Una identidad virtual[120] es una identidad o perfil en línea falso que puede utilizarse para realizar actividades de investigación seguras en plataformas de redes sociales y otras plataformas digitales abiertas que requieren que los usuarios inicien sesión para acceder al contenido. El concepto también puede aplicarse a una cuenta virtual o a un servicio de correo electrónico o de mensajería, una base de datos, un producto o una aplicación que utiliza una identidad en línea falsa en lugar de la identidad real. Desde el punto de vista de la seguridad, los investigadores e investigadoras deben crear y utilizar identidades virtuales en sus actividades de investigación en línea con material de fuentes abiertas. Así se aseguran de que, si un agente generador de amenazas intenta rastrear las actividades en línea de ese perfil, encontrará información consistente y convincente basada en la identidad virtual que no revele información real sobre la persona o entidad investigadora, o información sobre el contenido u objetivo de la investigación. Esta es también una importante medida de seguridad para proteger a quienes colaboren con la investigación. Los perfiles y cuentas virtuales y las actividades que se realizan con ellos deben planearse[121]. Además, se debe mantener un registro de la información utilizada para crear las cuentas y de las actividades realizadas, de manera que puedan explicarse posteriormente si es necesario, por ejemplo en un juicio[122].

[120] Al utilizar identidades virtuales se debe sopesar la necesidad de seguridad con el principio ético de la transparencia. Véase el cap. II.C, sobre los principios éticos.

[121] Véase el cap. V.C, sobre el plan de investigación en línea.

[122] Véase el cap. VI.D, sobre la preservación.

V

PREPARACIÓN

RESUMEN DEL CAPÍTULO

- La preparación y la planificación estratégica son fundamentales para una investigación exhaustiva y segura.
- La preparación incluye tres procesos: a) la evaluación de las amenazas y riesgos, así como un plan para mitigarlos; b) la evaluación del panorama informativo; y c) la elaboración de un plan de investigación. Estos procesos pueden solaparse o repetirse durante la investigación.
- La preparación incluye la elaboración de un plan para lidiar con los posibles efectos psicosociales negativos de la investigación, como los que puede causar la visión de material descarnado o potencialmente traumático.
- La preparación incluye la elaboración de un plan para manejar la información recogida durante la investigación: cuándo y en qué condiciones debe ser eliminada, cómo y en qué condiciones puede ser compartida y quién debe tener acceso a ella.
- La preparación debe incluir una evaluación del *software* y otras herramientas potencialmente útiles. Los investigadores e investigadoras deben comprender las ventajas y desventajas de los recursos comerciales, creados *ad hoc* y de código abierto.

108. Las personas que realizan investigaciones con fuentes abiertas no deben comenzar sus actividades de investigación en línea sino después de haber tomado una serie de medidas preparatorias. Estas deben incluir la realización de una evaluación de los riesgos y amenazas digitales y otra del panorama digital[123]. A continuación, los investigadores e investigadoras deben elaborar planes de investigación en línea basados en esas evaluaciones. Cada una de estas actividades se explica en detalle en este capítulo.

109. También es importante que la organización establezca políticas sobre la preservación, la eliminación, el acceso y el intercambio de datos antes de recoger y preservar la información, como se explica más abajo.

A. Evaluación de los riesgos y amenazas digitales

110. La valoración de las posibles amenazas y la adopción de una estrategia para gestionar el riesgo —físico, digital o psicosocial— garantizan el cumplimiento de los principios éticos y el principio de seguridad. Al comienzo de la investigación debe realizarse una evaluación de los riesgos y amenazas digitales, identificando las amenazas generales y específicas del caso que puedan surgir como consecuencia de las actividades en línea, en particular las visitas a los sitios web identificados, el monitoreo continuo de fuentes específicas o el raspado de datos de las plataformas de redes sociales. La evaluación debe incluir elementos analíticos de amenazas tradicionales, como la identificación de todos los posibles agentes generadores de amenazas, la valoración de los intereses y capacidades de dichos agentes así como la probabilidad de ataque, el estudio de las vulnerabilidades y el establecimiento de medidas de protección para minimizar esas vulnerabilidades. En estas evaluaciones deben participar especialistas en seguridad, en particular si tienen experiencia en ciberseguridad[124]. La evaluación debe revisarse periódicamente y actualizarse si es necesario. Además, puede ser necesario realizar otras evaluaciones en el caso de determinados tipos de actividades en línea, o si se identifican nuevos agentes potencialmente generadores de amenazas[125].

B. Evaluación del panorama digital

111. Las personas que investigan en fuentes abiertas deben comprender el entorno digital de la situación investigada. Los tipos de datos digitales disponibles dependen del tipo de tecnología disponible y utilizada, así como de quién la utiliza. Para ello es necesario identificar las plataformas en línea, los servicios de comunicación, las plataformas de redes sociales, las tecnologías móviles y las aplicaciones móviles más utilizadas en la región geográfica investigada. Por ejemplo, en las investigaciones de crímenes de guerra, se deben conocer los tipos de transporte, las TIC y los medios digitales utilizados por todas las partes implicadas en el conflicto armado, así como por los transeúntes u otras personas testigos, para saber qué tipos de información es más probable que se haya obtenido y distribuido en línea.

112. Los investigadores e investigadoras deben examinar las categorías de personas que utilizan o tienen acceso a cada una de esas tecnologías dentro de esa región geográfica. A este respecto, deben ser conscientes de que los contenidos digitales generados por usuarios y al alcance del público —incluidos los mensajes en las redes sociales y la información compartida en las plataformas digitales— tal vez no revelen del mismo modo todas las infracciones cometidas contra todos los individuos y grupos. Esto se debe a que el uso de las tecnologías digitales

[123] Véase el anexo II, sobre el modelo de evaluación de los riesgos y amenazas digitales, y el anexo III, sobre el modelo de evaluación del panorama digital.

[124] Para más información general sobre las amenazas y los riesgos en las investigaciones en fuentes abiertas, véase el cap. IV, sobre la seguridad.

[125] Véase el anexo II, sobre el modelo de evaluación de los riesgos y amenazas digitales.

puede ser diferente en función de, entre otras características, el género[126], la etnia, la religión, las creencias, la edad, la situación socioeconómica, la pertenencia a una minoría racial, lingüística[127], étnica o religiosa, la identidad indígena, la situación migratoria y la ubicación geográfica[128]. Este desequilibrio puede deberse a la falta de acceso a dispositivos, instalaciones o recursos[129], que impide que determinadas personas puedan crear o subir a Internet información sobre los problemas o infracciones que les conciernen. Otro factor que se debe tener en cuenta es que esas personas, entre otras, tal vez no hayan tenido acceso a la educación en igualdad de condiciones y, por lo tanto, tengan menos habilidades técnicas. Como consecuencia de la intersección de distintas formas de discriminación, algunos segmentos de la sociedad pueden ser doblemente invisibles en línea. Por ejemplo, es posible que la información sobre las mujeres y niñas que pertenecen a uno de los grupos marginados mencionados esté aún menos representada en la información de fuentes abiertas. Estos factores pueden traducirse en que esas personas no son las que crean contenidos o están representadas en ellos, sesgando así los resultados de cualquier investigación en línea.

113. Además, el acceso desigual a la tecnología de todos los segmentos de la sociedad también puede crear una imagen sesgada no solo de qué personas aparecen representadas en los contenidos en línea, sino también de los tipos de infracciones de que se informa en línea, en particular en los contenidos generados por los usuarios. Por ejemplo, cuando una mujer comparte el teléfono celular de alguno de sus familiares varones, o comparte una cuenta con otras personas, tal vez no hable de temas delicados, como la violencia sexual y la violencia de género, o de cuestiones relacionadas con la salud sexual y reproductiva. Además, los contenidos generados por usuarios que aparecen en las redes sociales, incluidas las fotografías y videos, tienden a mostrar más algunas infracciones que otras. Por ejemplo, los actos de violencia sexual y violencia de género, muchas veces cometidos en privado, pueden ser más difíciles de mostrar que las fotografías de desahucios, por ejemplo.

114. Aunque algunos de estos factores pueden mitigarse tratando de acceder a una pluralidad de tipos de información en línea —no solo a contenidos generados por los usuarios—, hay que tener en cuenta los mismos factores al analizar otros tipos de información de fuentes abiertas. Por ejemplo, cuando accedan a datos y estadísticas generadas por las autoridades, los investigadores e investigadoras siempre deben examinar si los datos han representado con precisión a todos los segmentos y todos los aspectos de la sociedad[130]. Puede evaluarse una serie de cuestiones y tecnologías clave, en función de lo que sea relevante para la investigación sobre la base de su alcance geográfico y temporal. Las investigaciones deben tener en cuenta el género, la edad, las disparidades geográficas y socioeconómicas, y otros datos demográficos relevantes. El objetivo de esta evaluación es comprender mejor las situaciones investigadas y, gracias a ello, diseñar estrategias de investigación en línea eficaces, así como obligar a las personas investigadoras a tener presentes de antemano los posibles sesgos de los datos disponibles en línea. Todas estas categorías tal vez no sean relevantes para todas las investigaciones, por lo que se debe adaptar la evaluación del panorama digital a las circunstancias del caso[131]. En el anexo III figura una lista completa de las

[126] Por ejemplo, las mujeres, las niñas y las personas lesbianas, gais, bisexuales, transgénero e intersexuales tal vez no tengan acceso al teléfono celular de la familia o no lo posean. Para más información sobre lo que se ha denominado "brecha digital de género", véase A/HRC/35/9. Véase también la resolución 32/13 del Consejo de Derechos Humanos, y Araba Sey y Nancy Hafkin (eds.), *Taking Stock: Data and Evidence on Gender Equality in Digital Access, Skills, and Leadership* (Macao, China, EQUALS Global Partnership y Universidad de las Naciones Unidas, 2019). Disponible en www.itu.int/en/action/gender-equality/Documents/EQUALS%20Research%20Report%202019.pdf.

[127] Las personas pertenecientes a minorías lingüísticas, por ejemplo, pueden encontrarse con barreras para acceder al espacio en línea, que suele utilizar la lengua dominante. Sin embargo, algunas minorías lingüísticas también tienen su propio espacio en línea en su propia lengua. Por lo tanto, tal vez se deban realizar búsquedas en las lenguas minoritarias (incluidas las lenguas indígenas).

[128] Por ejemplo, en las zonas rurales, la conectividad a Internet puede ser menor.

[129] Por ejemplo, no tener acceso físico a una conexión rápida a Internet o no poder adquirir un dispositivo o pagar la cuota de acceso.

[130] Véase, en general, ACNUDH, "Enfoque de datos basados en derechos humanos: que nadie se quede atrás en la Agenda 2030 para el Desarrollo Sostenible" (Ginebra, 2018). Disponible en www.ohchr.org/sites/default/files/Documents/Issues/HRIndicators/GuidanceNoteonApproachtoData_SP.pdf.

[131] Véase el modelo en el anexo III.

categorías de información que pueden incluirse en una evaluación del panorama digital.

C. Plan de investigación en línea

115. Antes de comenzar una investigación en fuentes abiertas, debe crearse un plan de investigación en línea[132] que incluya: a) la estrategia general de investigación; y b) las actividades específicas de la investigación en línea. Si las investigaciones en línea forman parte de una investigación más amplia en la que se utilizan técnicas tradicionales, como la toma de declaraciones a testigos o la recogida de pruebas físicas, el plan de investigación en línea debe integrarse en el plan de investigación principal. En el plan de investigación se debe integrar una perspectiva de género para garantizar que la investigación tenga en cuenta todas las cuestiones de género y las diferencias de acceso a la tecnología[133]. El plan de investigación en línea debe tratar los siguientes elementos.

1. Objetivos y actividades previstas

116. El plan debe exponer los objetivos y prioridades de la investigación en fuentes abiertas, la estrategia propuesta para cumplir estos objetivos y los plazos previstos para ello.

2. Estrategia de gestión de riesgos

117. El plan debe incorporar las principales conclusiones de la evaluación de los riesgos y amenazas digitales mencionada anteriormente, como las posibles ciberamenazas, junto con una estrategia para gestionar el riesgo que incluya la manera de identificar las fallas o ataques, así como de reaccionar y recuperarse de ellos.

3. Mapeo de otras entidades y oportunidades de cooperación

118. Es conveniente mapear a otras entidades que puedan estar realizando investigaciones similares o coincidentes para determinar si sus respectivas actividades podrían afectarse y para explorar posibles asociaciones y oportunidades de colaboración. En concreto, se puede tratar de identificar a archivistas digitales, periodistas u otros grupos o individuos que estén preservando contenidos en línea que puedan ser relevantes para la investigación. Este ejercicio también debe tener en cuenta los posibles sesgos y las limitaciones de otras entidades, que pueden dar lugar a conclusiones de terceros que no representen plenamente las complejidad de una situación determinada, o excluyan a ciertos grupos debido al sesgo inherente de la esfera digital si no se tiene este en cuenta, como se ha señalado más arriba. Si se forman este tipo de asociaciones, conviene firmar un acuerdo por escrito sobre el intercambio de información.

4. Recursos

119. El plan debe identificar los recursos necesarios para realizar las actividades planeadas (personal, formación, herramientas y material). Al evaluar las necesidades de personal, puede determinarse el número de personas necesarias para llevar a cabo las tareas, sus competencias, la inclusividad y diversidad de los miembros del equipo y las necesidades de formación adicionales. También puede valorarse la infraestructura necesaria —*hardware* y *software*— y los costos de la preservación del material digital a largo plazo. El plan también debe garantizar que haya recursos dedicados al bienestar psicológico del personal investigador teniendo en cuenta las cuestiones de género, especialmente en el caso de las investigaciones en fuentes abiertas que manejen contenidos descarnados o en que haya miembros del equipo u otras partes implicadas que puedan correr particularmente peligro de sufrir represalias si su identidad o su privacidad resultan comprometidas[134].

[132] Véase el anexo I, sobre el modelo de plan de investigación en línea.

[133] Para más información sobre la integración de la perspectiva de género, véase *Integración de la perspectiva de género en las investigaciones en derechos humanos: guía y práctica* (publicación de las Naciones Unidas, núm. de venta 19.XIV.2).

[134] Por ejemplo, los miembros de la investigación pueden ser objeto de discurso de odio o acoso en línea y esos ataques pueden tener un componente de género (por ejemplo, si son mujeres o pertenecen a la comunidad lesbiana, gai, bisexual, transgénero, *queer* e intersexual, pueden correr un mayor riesgo de sufrir discurso de odio en línea, *doxing* (revelación pública de información personal privada), amenazas de violación y otras amenazas violentas de carácter sexual o basadas en el género). Véase, por ejemplo, Amnistía Internacional, "Toxic Twitter – a toxic place for women". Disponible en www.amnesty.org/en/latest/research/2018/03/online-violence-against-women-chapter-1/.

5. Funciones y responsabilidades

120. Si se trabaja en equipo o con entidades asociadas externas, las funciones y responsabilidades de cada persona participante en la investigación en fuentes abiertas deben estar bien definidas, teniendo en cuenta la necesidad de coordinar las actividades para evitar la duplicación de tareas y de recogida de datos. Además, en esta sección del plan se debe determinar qué áreas de especialización pueden ser necesarias para la investigación y si se necesitará consultar o contratar a una persona con esos conocimientos especializados si no hay ninguna en el equipo existente. Las áreas de especialización pueden incluir la ciencia forense digital, el análisis de imágenes satelitales y la ciencia de los datos. En algunas de esas áreas podría ser necesario actuar para encontrar a especialistas que aporten diversidad en materia de género y con respecto a otras características, con el fin de garantizar la inclusividad y diversidad del equipo de investigación y análisis.

6. Documentación

121. Las investigaciones en fuentes abiertas deben documentarse de forma que puedan gestionarse de forma eficaz y se cumpla el principio de responsabilidad. En caso de procedimiento judicial, esa documentación permitirá al personal investigador demostrar que las pruebas recogidas son pertinentes y tienen valor probatorio, así como explicar los pasos dados, o no dados, durante las actividades en línea, y la razón para ello. Tanto si se trata de una tarea propia como de una asignada por un supervisor o supervisora, el sistema debe contar con un mecanismo de creación de tareas para determinadas actividades de investigación —incluidas las actividades en línea—, como la presentación de solicitudes para investigar a una persona concreta u otras consultas. En los resultados de las tareas, incluidos los informes, se deben documentar las metodologías y técnicas utilizadas. En los informes se debe separar la información operacional que tal vez sea necesario mantener confidencial para proteger las fuentes y los métodos de una investigación, de la información obtenida por la investigación que deba ser revelada durante los procedimientos judiciales.

122. El plan de investigación en línea debe revisarse periódicamente y modificarse en caso necesario. Véase en el anexo I el ejemplo de plan de investigación en línea.

D. Plan de resiliencia y autocuidado

123. Aunque no se realicen entrevistas en persona ni se visiten personalmente los lugares donde se haya cometido el crimen, las particularidades de la investigación digital pueden obligar a los investigadores e investigadoras con fuentes abiertas a ver, recopilar y analizar cantidades significativas de información digital descarnada o traumática, que podría provocarles un trauma secundario, entre otros problemas. Esas personas deben conocer los principios del autocuidado[135], y quienes dirigen su trabajo deben establecer un entorno que otorgue importancia al autocuidado y a la sensibilidad cultural y de género. Esto debe instituirse en la fase preparatoria de la investigación, elaborando un plan para fomentar la resiliencia y mitigar los efectos psicosociales negativos de la investigación, que pueden ser diferentes según el género, la cultura y la edad. Dicho plan es esencial por motivos éticos, puesto que se deben promover y respetar los derechos humanos de cada miembro del equipo de investigación. También es esencial para maximizar la seguridad física y digital. Incluso con la formación adecuada, una persona estresada puede representar una vulnerabilidad para la seguridad del equipo y de la información, así como para la calidad del trabajo. Deben asignarse tiempo y recursos específicos para garantizar la correcta ejecución del plan, en particular cuando se prevea que la investigación en línea podría obligar a los miembros del equipo a ver grandes cantidades de imágenes descarnadas, con contenidos violentos o traumáticos. Existen distintas estrategias para mitigar el posible impacto negativo de los contenidos descarnados en quienes los ven, pero suelen dividirse en tres

[135] Para más información sobre la importancia del autocuidado para quienes trabajan en el ámbito de las investigaciones de derechos humanos, véase ACNUDH, *Manual on Human Rights Monitoring* (Ginebra, 2011), cap. 12, sobre el trauma y el autocuidado, págs. 20 a 39. Disponible en www.ohchr.org/Documents/Publications/Chapter12-MHRM.pdf.

categorías: conciencia individual, tácticas para minimizar la exposición y apoyo colectivo.

124. En primer lugar, los investigadores e investigadoras deben conocer sus propios comportamientos habituales y los de los demás miembros de su equipo, en particular los patrones de trabajo, recreación, sueño y alimentación, para poder detectar cualquier alteración y atajarla. En ese sentido puede ayudar trabajar en grupos de dos, ya que la otra persona puede advertir más fácilmente los cambios de comportamiento que a veces no se pueden o no se quieren reconocer en primera persona. Los miembros del equipo deben tener presentes y respetar las diferencias en las respuestas de cada persona al material descarnado o de otro tipo que pueda provocar una emoción fuerte, y saber que dichas diferencias pueden variar entre individuos, géneros y grupos culturales, así como a lo largo del tiempo para algunas personas, debido al grado de estrés al que están sometidas y a otros factores situacionales. Los investigadores e investigadoras también deben ser conscientes de que tener una respuesta emocional a un contenido descarnado o atroz es a menudo totalmente normal y no un signo de debilidad, sino que puede ser un signo de buena salud, e incluso de fortaleza.

125. En segundo lugar, deben adoptarse tácticas para minimizar la exposición a contenidos perjudiciales. Entre las estrategias más comunes a este respecto figuran desactivar el sonido cuando se ve un contenido potencialmente descarnado por primera vez, o cuando no sea necesario escucharlo para la tarea de análisis que se esté realizando en ese momento, ya que el sonido tiene una gran carga emotiva; reducir el tamaño de la pantalla en la medida de lo posible; tapar el material descarnado cuando se analiza el contexto que rodea un acto concreto y no el acto en sí; marcar cualquier contenido descarnado que esté incluido en un conjunto de datos para que los demás miembros del equipo no vean ese contenido sin saber previamente lo que van a ver; advertirse mutuamente cuando se compartan contenidos descarnados para mitigar el elemento sorpresa; trabajar en grupos de dos; evitar trabajar de forma aislada o a altas horas de la noche; y tomar descansos frecuentes, si es necesario.

126. En tercer lugar, los miembros del equipo y la organización para la que trabajan deben fomentar un sentimiento de pertenencia al grupo que puede tener un efecto protector, reproduciendo básicamente el sentimiento de camaradería que puede darse al realizar investigaciones sobre el terreno. Esto puede lograrse celebrando reuniones periódicas de información, que pueden reducir el aislamiento y ayudar a los investigadores e investigadoras a comprender mejor las repercusiones positivas de su trabajo; organizando salidas del equipo, por ejemplo para celebrar los hitos importantes de la investigación; y proporcionando formación al equipo sobre las estrategias de resiliencia. Los intentos de aumentar la resiliencia pueden ser especialmente fructíferos cuando se abordan a nivel individual, cultural y estructural, por ejemplo capacitando al individuo para que reflexione sobre sus necesidades psicosociales cuando trabaja en una investigación y fomentando un entorno en el que los aspectos psicosociales del trabajo se tomen en serio, se favorezcan las prácticas de apoyo tanto explícita como implícitamente y se promuevan la inclusividad y la diversidad.

E. Políticas y herramientas de datos

127. En el curso de una investigación deben elaborarse, aplicarse y cumplirse políticas relativas al manejo, la conservación y la destrucción de los datos. Las organizaciones deben establecer políticas para conservar (políticas de conservación) y eliminar la información (políticas de eliminación), cuando proceda, así como políticas sobre el acceso a la información (internamente) y al intercambio de información (externamente). Además, también puede ser conveniente contar con políticas específicas sobre la creación y el uso de identidades virtuales, así como sobre el acceso a los programas computacionales aprobados y las herramientas utilizadas.

1. Políticas de datos

a) Políticas de conservación de datos

128. Las políticas de conservación de datos son importantes para cumplir con muchas leyes de protección de datos y reglamentos de conservación de datos. En algunos casos, existen requisitos mínimos sobre el tiempo que deben conservarse los datos, mientras que en otras circunstancias hay un límite máximo. Las políticas deben establecer un enfoque del

almacenamiento de datos persistentes y de la gestión de registros con miras a cumplir los requisitos legales y las necesidades de archivo de datos en la entidad en cuestión. Las diferentes políticas de conservación de datos sopesan, por un lado, los requisitos legales y de privacidad y, por otro, los intereses económicos y de necesidad de conocimiento para determinar los tiempos de conservación, las normas de archivo, los formatos de los datos y los medios permitidos de almacenamiento, acceso y cifrado[136]. Para elaborar dichas políticas será necesario entender las normas aplicables.

b) Políticas de eliminación de datos

129. La eliminación de partes de un conjunto de datos sin políticas claras de eliminación y preservación y sin llevar un registro de lo que se ha eliminado, quién lo ha hecho y cuándo —y con qué fines— puede plantear problemas importantes, en particular cuando la información puede utilizarse en los tribunales. Los investigadores e investigadoras deben cumplir la normativa aplicable en materia de eliminación de datos digitales y ser conscientes de que la utilización de uno u otro método podría tener consecuencias legales.

c) Políticas de acceso a los datos

130. Las organizaciones que recopilan y procesan datos, especialmente datos confidenciales, deben tener una política clara sobre quién puede acceder a los distintos tipos de datos. Las bases de datos o los sistemas deben configurarse de manera que se refleje esta política.

d) Políticas de compartición de datos

131. Conviene que las organizaciones elaboren una política de compartición de datos con entidades externas. Si se trabaja con asociados, deben establecerse memorandos de entendimiento o contratos para garantizar que estos cumplan dichas políticas.

2. Gestión de la información

132. Antes de emprender investigaciones en fuentes abiertas, especialmente en la recogida y preservación de material digital, el personal investigador, los equipos y organizaciones deben establecer un sistema de gestión de la información. Existen distintas opciones para dicho sistema, y el Protocolo no aboga por una en concreto. En cambio, a continuación se indican las principales funcionalidades que pueden ser útiles para el proceso de investigación, y en algunos contextos pueden ser necesarias. Además, como se ha comentado en el capítulo IV, deben existir infraestructuras y protocolos de seguridad.

a) Sistema de gestión de la investigación

133. Un sistema de gestión de la investigación es un sistema con el que se documentan las actividades realizadas en el marco de una investigación. No todas las organizaciones que llevan a cabo investigaciones cuentan con este tipo de sistemas, pero son muy recomendables, especialmente para las organizaciones o equipos de investigación más grandes. Estos sistemas pueden utilizarse para asignar tareas e informar sobre las actividades, de modo que el proceso esté estructurado y sea lo más eficiente posible, reduciendo de ese modo la duplicación de tareas.

b) Sistemas de gestión de la información y las pruebas

134. Los sistemas de gestión de la información se utilizan para almacenar los datos recogidos en el marco de las investigaciones. El sistema de gestión de la información debe cumplir dos funciones distintas: a) controlar la recogida y el manejo del material, y b) separar el material que pueda ser utilizado como prueba.

3. Infraestructura: consideraciones logísticas y de seguridad

135. Tanto al diseñar la infraestructura para una organización que realiza investigaciones en fuentes abiertas como al decidir qué herramientas utilizar como investigador o investigadora independiente, hay varias consideraciones logísticas y de seguridad importantes. En general, existen tres enfoques de la adopción de sistemas: a) emplear herramientas y sistemas creados a medida; b) utilizar herramientas y *software* de código abierto o gratuitos disponibles en

[136] Yvonne Ng, "How to preserve open source information effectively", en *Digital Witness, Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig y Daragh Murray, eds. (Oxford, Oxford University Press, 2020), págs. 143 a 164.

Internet; o c) adquirir productos comerciales de terceros. Cada uno de estos enfoques presenta ventajas e inconvenientes, y su éxito depende de las circunstancias y el contexto específicos de la investigación. Una vez más, el Protocolo no aboga por un enfoque u otro, sino que presenta las ventajas e inconvenientes de cada uno, así como los factores específicos que deben tenerse en cuenta al tomar decisiones sobre qué productos utilizar.

a) Productos comerciales

136. La ventaja de los productos comerciales es que una empresa privada puede tener una mejor infraestructura de seguridad y ser capaz de proporcionar asistencia técnica continua y consistente. Sin embargo, los productos comerciales tienen el evidente inconveniente del costo. Además, el interactuar con terceros y depender de ellos puede ser un problema para las organizaciones que quieren mantener la confidencialidad de sus investigaciones. Muchos productos comerciales tienen un código cerrado para proteger su propiedad intelectual. Los productos comerciales también pueden plantear problemas relacionados con la propiedad, la portabilidad y la exportabilidad de los datos, y la interoperabilidad con otros sistemas. Además, cabe la posibilidad de que la empresa proveedora ceda a la presión del Gobierno y le permita acceder a información privada. Uno de los principales problemas es que, aunque las empresas cuenten con equipos de seguridad para proteger sus productos y usuarios, estos tienen que confiar en que la empresa ha diseñado y mantendrá sus sistemas adecuadamente, y en que no habrá más tarde costos ocultos.

b) Herramientas creadas a medida o personalizadas

137. La ventaja de crear desde cero una herramienta a medida o de personalizar una herramienta ya existente es que el equipo investigador o la organización mantienen el control de todo el sistema y de sus datos y, por tanto, no tienen que interactuar con terceros. Los sistemas creados a medida también pueden ser más fáciles de integrar con otros sistemas similares. El inconveniente es el tiempo, el costo y los conocimientos técnicos necesarios para crear y mantener estos sistemas, lo que puede suponer un reto para la mayoría de las organizaciones. Además, cuando se crea un sistema cerrado con un número limitado de probadores beta y usuarios es difícil detectar las vulnerabilidades u obtener retroalimentación suficiente para maximizar la funcionalidad.

c) Herramientas de código abierto y gratuitas

138. Las herramientas de código abierto son aquellas cuyos creadores han hecho público el código fuente para que cualquiera pueda utilizarlo o modificarlo libremente. Existen algunos productos comerciales de código abierto y algunas herramientas gratuitas con código fuente cerrado, pero son las excepciones. Lo más habitual es que las herramientas de código abierto sean gratuitas. Las herramientas gratuitas pueden ser una opción interesante para las organizaciones más pequeñas cuyo presupuesto sea limitado, así como para las organizaciones más grandes que tengan procedimientos onerosos de adquisición de productos de pago. Sin embargo, hay herramientas gratuitas para usuarios que obtienen beneficios de otras maneras, como vendiendo los datos de los usuarios y sus análisis de estos, lo que plantea problemas de seguridad y privacidad. Además, para utilizar estas herramientas se debe indagar previamente quién las ha creado, si han sido auditadas de forma independiente y si son sostenibles. Los tres aspectos podrían mermar la credibilidad de una investigación. En particular, las herramientas pueden ser problemáticas desde el punto de vista legal si el caso llega a juicio y la parte contraria cuestiona la herramienta. Además, estos sistemas y herramientas de *software* requieren un plan de emergencia y un sistema de migración de datos y copias de seguridad, en caso de que queden obsoletos o no se pueda acceder a los creadores. Aunque las herramientas de código abierto pueden resultar atractivas para las organizaciones, en parte por el hecho de que otros grupos afines las utilicen, los investigadores e investigadoras deben realizar evaluaciones completas e independientes de su funcionamiento y de las consecuencias que su empleo podría tener en un contexto concreto.

139. Al tomar la decisión de crear una herramienta a medida, utilizar un *software* de prueba gratuito o de código abierto, o comprar un producto, las personas que investigan deben seguir las recomendaciones sobre las medidas de precaución que figuran en el anexo V.

VI

PROCESO DE INVESTIGACIÓN

RESUMEN DEL CAPÍTULO

- El proceso de investigación consta de seis fases principales. Estas son: a) la indagación en línea; b) la evaluación preliminar; c) la recolección; d) la preservación; e) la verificación; y f) el análisis de la investigación. En conjunto, forman parte de un ciclo que puede repetirse numerosas veces a lo largo de una investigación, o cada vez que se descubre una información nueva que da lugar a nuevas líneas de investigación.
- Las personas investigadoras deben documentar sus actividades durante cada fase. Así lograrán que sus investigaciones se comprendan mejor, sean más transparentes —incluidas las cadenas de custodia— y más eficientes, eficaces y completas, además de mejorar la comunicación entre los miembros del equipo.

140. Las investigaciones en fuentes abiertas requieren observación cuidadosa e indagaciones sistemáticas para establecer los hechos en un entorno digital complejo y dinámico. Las personas que las realizan deben tener un ojo crítico para examinar los contenidos en línea y ser capaces de apreciar las formas en que el material digital puede ser distorsionado o manipulado. También deben aplicar un enfoque estructurado a sus búsquedas en Internet, teniendo en cuenta el sesgo algorítmico y la desigualdad en cuanto a la disponibilidad de información de fuentes abiertas relativa a determinados grupos, así como la naturaleza dinámica de la información en línea. Cada alegación debe ser examinada rigurosamente. Este capítulo ofrece un enfoque estructurado de las investigaciones en fuentes abiertas. La figura que se muestra a continuación representa el ciclo de investigación en fuentes abiertas. Es importante señalar que las investigaciones en fuentes abiertas rara vez son lineales y a menudo requieren la repetición de este proceso, dada la naturaleza cíclica de la creación de un argumento. También puede haber motivos válidos para desviarse de este orden.

Ciclo de investigación en fuentes abiertas

A. Indagaciones en línea

141. Las indagaciones en línea constan de dos procesos principales: a) la búsqueda, que consiste en descubrir información y fuentes utilizando metodologías de búsqueda generales o avanzadas; y b) el monitoreo, que consiste en descubrir nueva información mediante la revisión coherente y persistente de un conjunto de fuentes constantes.

1. Búsqueda

142. La búsqueda en línea es una actividad orientada a descubrir nueva información relevante para un objetivo definido o una pregunta de investigación. Las búsquedas deben ser estructuradas y sistemáticas, lo que incluye comenzar con una pregunta de investigación clara y parámetros de búsqueda, así como palabras clave y operadores[137]. Cada motor de búsqueda, herramienta de búsqueda, término de búsqueda y operador da resultados diferentes, por lo que las personas investigadoras deben actuar con cierta creatividad y tenacidad, además seguir diversas vías y canales para encontrar la información relevante. Además de los motores de búsqueda utilizados para encontrar información en los sitios web indexados, también pueden realizarse búsquedas estructuradas en plataformas de redes sociales y en bases de datos. Debido a la necesidad de adoptar un enfoque variado, diverso y específico para cada caso, se deben documentar cuidadosamente los procesos de investigación para poder explicarlos en la sección de metodología de los informes o en los procedimientos judiciales. Este proceso puede ser retroactivo y no desarrollarse necesariamente al mismo tiempo que la propia investigación. Sin embargo, la documentación debe realizarse siempre con la mínima demora posible. La documentación de las búsquedas estructuradas debe incluir la siguiente información:

a) Objetivo y preguntas de investigación: se debe formular la pregunta o preguntas a que pretende responder la búsqueda en línea, teniendo en cuenta el principio de objetividad antes expuesto;

b) Hechos, conjeturas e incógnitas: se debe partir de un punto en el que se conocen los hechos, si es que se han establecido. También puede trabajarse sobe la base de una información de una pista o de conjeturas lógicas, aunque no se hayan verificado todavía. Sin embargo, es esencial que cualquier conjetura se haga constar como tal. Por último, puede ser conveniente formular lo que se desconoce u otras "incógnitas" al principio de la investigación. La delimitación de estas categorías de información ayudará a evitar resultados sesgados o distorsionados al aclarar los términos de búsqueda y sus bases;

c) Términos de búsqueda y palabras clave: para realizar una búsqueda específica, se deben crear listas de palabras clave que cumplan el principio de objetividad sobre la base de la teoría o teorías del caso. De ser posible, se deben utilizar palabras clave en todas las lenguas y alfabetos pertinentes, teniendo cuidado de no obtener ni demasiados resultados de búsqueda, ni demasiado pocos. En este sentido, cada caso será diferente, pero hay ciertos temas generales que deben incorporarse en las listas de palabras clave, como lugares significativos, nombres, organizaciones, fechas y etiquetas *(hashtags)* relevantes. También puede ser conveniente determinar qué información podría ser incriminatoria o eximente en el contexto de la investigación de que se trate;

d) Búsquedas y motores de búsqueda: se deben documentar las búsquedas realizadas y las vías de acceso al material pertinente, incluidos los términos, operadores y motores de búsqueda que llevaron a ese contenido. No es necesario dejar constancia de los resultados de todas las búsquedas, que sería excesivamente oneroso y no tendría mucho valor probatorio.

2. Monitoreo

143. El monitoreo consiste en seguir una fuente de información establecida, por ejemplo un tema

[137] Los operadores booleanos son palabras sencillas, como "y", "o" y "no", que pueden utilizarse "para combinar o excluir palabras clave en una búsqueda, lo que permite obtener resultados más concretos y productivos". Véase Alliant International University Library, "What is a Boolean operator?". Disponible en https://library.alliant.edu/screens/boolean.pdf.

concreto, a lo largo del tiempo. El objetivo es observar los cambios en los contenidos generados por una fuente constante. El monitoreo en línea debe ser una actividad estructurada que utilice listas de fuentes en línea conocidas y previamente evaluadas, como sitios web o cuentas de redes sociales, así como búsquedas de objetivos definidos ejecutadas de forma continua. Véanse, por ejemplo, las siguientes fuentes:

a) Sitios web y cuentas de redes sociales: se deben mantener listas de trabajo de los sitios web y perfiles que se van a monitorear, justificando en cada caso por qué se monitorean; la persona al mando del monitoreo; quién realiza el monitoreo; y la frecuencia del monitoreo;

b) Etiquetas y palabras clave: se debe mantener y actualizar periódicamente una lista de trabajo de etiquetas y palabras clave que se están monitoreando;

c) Automatización: en la labor de monitoreo es posible que se utilicen herramientas automatizadas que, por ejemplo, realicen periódicamente una búsqueda en sitios específicos o usando determinados parámetros. Siempre hay que dejar constancia del empleo de dichas herramientas, de sus nombres, versiones, y de la información introducida en ellas.

3. Sesgos

144. Al realizar actividades de búsqueda estructurada y monitoreo, las personas investigadoras en fuentes abiertas deben permanecer siempre atentas a sus propios tanto sesgos cognitivos como a los inherentes a la información disponible en línea. Por ejemplo, si se busca información sobre el delito sexual de violación, es probable que la mayoría de los datos proporcionados, o la información encontrada en línea, sea sobre violaciones de mujeres en edad de procrear cometidas fuera de las relaciones conyugales. Los resultados de la búsqueda podrían ocultar en cierto modo otros tipos de violaciones menos visibles o denunciadas, como las cometidas contra hombres y niños varones, personas lesbianas, gais, bisexuales, transgénero e intersexuales, y mujeres mayores o violaciones conyugales.

145. Otro ejemplo de posibles sesgos son las investigaciones sobre actos de violencia incitados por discursos de odio en línea, ya que dichos discursos suelen incorporar y utilizar un lenguaje en clave y símbolos que no son fáciles de detectar por personas investigadoras o máquinas. Especialmente cuando quien investiga no pertenece a la comunidad en cuestión, existe el riesgo de que desconozca el uso, en la cultura y el contexto de que se trate, de los términos y símbolos utilizados para incitar al odio o la violencia. Además, con frecuencia el discurso de odio en línea se formula deliberadamente de forma que no sea detectado por quien lo monitorea (sea una persona o una máquina) para así evitar que sea eliminado de las plataformas en línea, cuando en realidad es un medio de incitar a la violencia o la discriminación contra un grupo determinado. Para tratar de superar la dificultad de detectar la incitación a la discriminación, la hostilidad o la violencia, se debe aplicar una ponderación basada en los derechos humanos, por ejemplo la prevista en el Plan de Acción de Rabat sobre la prohibición de la apología del odio nacional, racial o religioso que constituye incitación a la discriminación, la hostilidad o la violencia[138].

146. En última instancia, lo mejor que pueden hacer los investigadores e investigadoras para contrarrestar los "sesgos tecnológicos" junto con sus propios sesgos es ser conscientes del potencial de dichos sesgos, tener presentes los riesgos y tomar medidas activas cuando sea posible para contrarrestar los sesgos, investigando la terminología y los símbolos relevantes para un contexto o conjunto de delitos o incidentes en particular, y ampliando y diversificando la indagación en línea. En los casos de violencia sexual y violencia de género, así como de otros delitos en que se estigmatiza a las personas sobrevivientes y se utiliza un lenguaje en clave, deben consultar a especialistas que puedan identificar y descifrar el lenguaje en clave y las prácticas de comunicación que

[138] Véase ACNUDH, "Libertad de expresión vs incitación al odio: el ACNUDH y el Plan de Acción de Rabat". Disponible en www.ohchr.org/es/freedom-of-expression.

dichas personas sobrevivientes y sus agresores suelen utilizar cuando se comunican en línea[139].

B. Evaluación preliminar

147. Antes de recolectar contenidos de Internet, las personas que realizan investigaciones en fuentes abiertas deben llevar a cabo una evaluación preliminar de cualquier material que identifiquen para evitar una recogida excesiva y cumplir los principios de la minimización de datos y la investigación específica, así como para garantizar que la recogida del material no infrinja el derecho a la privacidad de las personas. En ese sentido, deben tener en cuenta los siguientes factores para determinar si deben recoger un contenido digital de Internet.

1. Pertinencia

148. Las personas que realizan investigaciones en fuentes abiertas deben determinar si un elemento digital es a primera vista pertinente para la investigación de que se trate. La pertinencia de cualquier elemento depende de su contenido y de su fuente, así como de los objetivos de la investigación y de lo que se sabe sobre una situación. En las primeras fases de una investigación puede ser difícil saber qué es pertinente, lo que puede llevar a una recolección excesiva. No obstante, los investigadores e investigadoras en fuentes abiertas deben ser capaces de expresar por qué creen que un elemento es potencialmente pertinente, y esta evaluación debe quedar registrada (por ejemplo, mediante un sistema de etiquetado o almacenamiento sencillo y fácil de usar que vincule la información recopilada con, por ejemplo, un lugar, una fecha, un incidente, una persona o un tipo de infracción que se esté investigando).

2. Fiabilidad

149. Los investigadores e investigadoras en fuentes abiertas deben determinar si la información o las afirmaciones que recoge un contenido digital son a primera vista fiables, revisando y evaluando el contenido, así como la información contextual incluida en el archivo. Podría ser necesario comprobar los metadatos integrados, la información vinculada y la fuente[140]. Para ello se debe tratar de identificar la fuente original del material, lo que podría requerir rastrear la procedencia en línea de los datos, o a la persona que subió el contenido a Internet o lo creó.

3. Eliminación

150. Las personas que investigan en fuentes abiertas deben evaluar si es probable que un elemento digital sea eliminado de Internet o deje de ser de acceso público. Si llegan a la conclusión de que así es, deben recoger la versión conocida más fiable del elemento, incluso mientras se realizan más verificaciones y se buscan versiones anteriores o mejores. La probabilidad de que se elimine un contenido puede evaluarse en función de una serie de factores, como la presunta identidad de la fuente, la ubicación del contenido y su compatibilidad con las condiciones de utilización del proveedor de servicios. Por ejemplo, los contenidos descarnados u ofensivos con un gran valor probatorio potencial para condenar a los autores de delitos o infracciones figuran entre los más probables de ser eliminados.

4. Seguridad

151. Las personas investigadoras de fuentes abiertas deben determinar si es seguro recoger un elemento digital o si se pueden y deben tomar más precauciones. Los mayores problemas en ese sentido surgen cuando el contenido que se quiere recoger está en un sitio web que pueda contener elementos corruptos que podrían dañar el sistema interno.

5. Tareas subsiguientes

152. Los investigadores e investigadoras de fuentes abiertas deben determinar qué tareas pueden tener que realizar si se encargan de la custodia de un elemento digital, como la tarea de preservarlo de forma segura para cumplir las leyes de protección de datos[141].

[139] Véase, por ejemplo, Koenig and Egan, "Hiding in plain site: using online open source information to investigate sexual violence and gender-based crimes".

[140] Véase el cap. VI.E, sobre la verificación.

[141] Véase el cap. VI.D, sobre la preservación.

C. Recolección

153. La recolección es el acto por el que se adquiere la posesión de una información en línea mediante una captura de pantalla, la conversión a PDF, la descarga forense u otra forma de captura. Una vez que el contenido digital se identifica y se considera relevante para una investigación y a primera vista pertinente y fiable, se debe determinar el método adecuado de recolección. Los métodos de recolección pueden variar en función de si el contenido en línea podría tener valor probatorio en un juicio, si se utilizará para la toma de decisiones o si contribuirá únicamente al producto de trabajo interno. En los casos en que solo se trate de un producto de trabajo, puede bastar con una captura de pantalla o la conversión a PDF, mientras que el contenido que pueda tener valor probatorio puede requerir un método de captura más preciso y completo (por ejemplo, mediante la asignación de un valor de direccionamiento (*hash*, véase más adelante)).

154. La recolección de contenidos en línea puede realizarse manualmente (siguiendo un procedimiento operativo estándar) o automatizarse (utilizando diversas herramientas o secuencias de comandos). Independientemente del proceso, lo ideal es que la información que se indica a continuación se capture en el momento de recolección. Esta información puede ser útil para establecer la autenticidad de un elemento digital, lo cual podría ser especialmente importante en el caso de procedimientos judiciales en que se presenta un elemento como prueba, sobre todo si la persona que lo creó no está identificada, localizada o disponible para testificar. Los investigadores e investigadoras en fuentes abiertas deben recolectar los contenidos en línea en su formato original o en un estado lo más parecido posible a su formato original. Toda alteración, transformación o conversión causada por el proceso de recolección debe documentarse.

155. A continuación se ofrece orientación sobre lo que hay que recolectar y cómo hacerlo. Existen varias herramientas que ayudan a capturar la información que se indica a continuación, pero también se puede hacer manualmente. Si bien la recolección de toda la información se considera una mejor práctica, los tres primeros elementos (localizador uniforme de recursos (URL), código fuente del Lenguaje de Marcación de Hipertexto (HTML) y captura de la página completa) se consideran el mínimo indispensable para aportar pruebas ante los tribunales. Por supuesto, esa norma variará en función del contexto, pero la captura de todos los elementos enumerados a continuación proporcionará una base sólida en cualquier contexto:

a) Dirección web de destino: debe dejarse constancia de la dirección web del contenido recogido, también conocida como localizador uniforme de recursos (URL) o identificador uniforme de recursos (URI);

b) Código fuente: se debe capturar el código fuente HTML de la página web, si procede. El código fuente HTML incluye mucha más información que la parte visible de la página web. El código fuente HTML contribuirá a autenticar el material recogido;

c) Captura de la página completa: se debe realizar primero una captura de pantalla de la página web de que se trate donde se indiquen la fecha y la hora. La finalidad es tener la mejor representación posible de lo que se vio en el momento de la recolección;

d) Archivos multimedia integrados: si se descarga una página web con videos o imágenes, por ejemplo, esos elementos específicos también deben extraerse y recogerse de la página web;

e) Metadatos integrados: se deben recopilar los metadatos adicionales del elemento digital, si están disponibles y procede. Los metadatos pueden variar en función de las fuentes, pero los más comunes son el identificador del usuario que subió el contenido; el identificador del mensaje, la imagen o el video; la fecha y hora en que se subió el contenido; la etiqueta geográfica *(geotag)*; la etiqueta *(hashtag)*;

f) Datos contextuales: también debe recolectarse el contenido contextual si procede para entender el elemento digital. Puede tratarse de comentarios sobre un video, imagen o mensaje; información sobre la subida a Internet; o información sobre la persona que lo subió o el usuario, como el nombre de usuario, el nombre real o la biografía. Es necesario determinar si la información circundante debe recogerse, en función de las características específicas del caso y del elemento digital;

g) Datos de recolección: los investigadores e investigadoras en fuentes abiertas deben dejar constancia de todos los datos pertinentes de la recolección, como el nombre de la persona que la hizo, la dirección IP de la máquina utilizada para recoger la información, la identidad virtual utilizada, si la hay, y un sello de fecha y hora. Deben asegurarse de que el reloj del sistema sea preciso, preferiblemente sincronizándolo con un servidor de Protocolo de Hora de Red. La finalidad es garantizar que los metadatos relacionados con la hora se representen con precisión en los archivos recolectados. Si se utiliza una identidad virtual para acceder a la información recogida, debe señalarse;

h) Valor de direccionamiento: los valores de direccionamiento *(hash)* son una forma única de identificación digital que confirma, mediante el uso de la criptografía, que el contenido recogido es único y no ha sido modificado desde entonces. En el momento de la recogida, las personas investigadoras en fuentes abiertas deben añadir manualmente —o la herramienta de recogida debe añadir automáticamente— un valor de direccionamiento. Hay muchos tipos de valores entre los que elegir, y las normas han evolucionado con el tiempo. Se debe evaluar qué valor utilizar basándose en la norma aceptada en el momento[142].

156. Cuando se recurre a la recolección automatizada, algunos de los procesos descritos pueden ser ejecutados por herramientas diseñadas para recoger el contenido y los metadatos pertinentes. Para cada elemento recolectado debe elaborarse un informe técnico que incluya la información mencionada con el fin de establecer posteriormente la autenticidad del elemento. La información contextual y todos los tipos de metadatos deben almacenarse y preservarse siempre con el elemento digital, como se explica en la sección siguiente.

D. Preservación

157. A menudo, la información en línea no está disponible permanentemente. En ocasiones, las redes sociales eliminan contenidos de sus plataformas de acuerdo con sus condiciones de uso, y en otras los usuarios optan por eliminar o editar los contenidos que han subido. Además, la información en línea puede descontextualizarse, perderse, borrarse o corromperse fácilmente[143]. Para que el material digital siga siendo accesible y utilizable en un procedimiento judicial, es necesario preservarlo tanto a corto como a largo plazo[144]. En general, el objeto de la preservación digital es mantener la accesibilidad[145]. Sin embargo, cuando se preservan contenidos digitales para utilizarlos en un mecanismo judicial, el objetivo es gestionarlos y mantenerlos de manera que se garantice su accesibilidad, autenticidad y uso potencial en dichos mecanismos, lo que incluye el hecho de que sean admisibles en un juicio. Así pues, la preservación digital en el contexto de la investigación entraña el mantenimiento de la información a lo largo del tiempo, de modo que el elemento recolectado siga siendo comprensible por sí solo para los usuarios a los que se destina, y su autenticidad pueda confirmarse suficientemente.

158. Para preservar un elemento a largo plazo, puede ser necesario actualizar el *hardware* y los formatos de almacenamiento, de modo que el material siga siendo accesible con los dispositivos que se utilicen en el futuro.

1. Propiedades de un elemento digital que deben protegerse y preservarse a largo plazo

159. La profesión archivista considera que las propiedades de un elemento digital que deben protegerse y preservarse a largo plazo son su autenticidad, disponibilidad, identidad, persistencia, representabilidad y comprensibilidad, que se describen brevemente a continuación.

[142] El Instituto Nacional de Normas y Tecnología de los Estados Unidos ofrece orientación sobre la norma actual. Véase www.nist.gov.

[143] Ng, "How to preserve open source information effectively".

[144] *Ibid.*, pág. 143. Véase Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, "Noción de preservación digital". Disponible en https://es.unesco.org/themes/information-preservation/digital-heritage/concept-digital-preservation.

[145] Ng, "How to preserve open source information effectively".

a) Autenticidad

160. La autenticidad es la capacidad de demostrar que un material digital sigue siendo el mismo que cuando se recogió. Para ello, el elemento digital debe permanecer sin alterarse mientras se encuentre archivado, o bien se debe documentar cualquier modificación del mismo[146].

b) Disponibilidad

161. La disponibilidad de un material digital, en su sentido más simple, es el hecho de seguir existiendo y ser recuperable, mientras que en su sentido jurídico se refiere a la capacidad de obtener los derechos de propiedad intelectual necesarios para acceder al elemento y utilizarlo[147].

c) Identidad

162. La identidad de un material digital se refiere a la posibilidad de referenciarlo. El material digital debe ser identificable y distinguible de otros materiales digitales, por ejemplo aplicándole un identificador, como un número de identificación único[148].

d) Persistencia

163. La persistencia de un material digital se refiere a su integridad y viabilidad en términos técnicos. Las secuencias de bits del elemento digital deben estar intactas y ser procesables y recuperables[149].

e) Representabilidad

164. La representabilidad de un material digital es su cualidad que permite a seres humanos o máquinas interactuar con él o utilizarlo con el *hardware* y el *software* adecuados[150].

f) Comprensibilidad

165. La comprensibilidad de un material digital es su cualidad para ser interpretado y comprendido por los usuarios previstos[151].

2. Problemas específicos de la investigación

166. Las personas investigadoras también deben tener en cuenta y prever los problemas específicos de la investigación que pueden surgir o surgirán durante el proceso de preservación.

a) Cadena de custodia

167. La expresión "cadena de custodia" se refiere a la documentación cronológica de la secuencia de custodios de un material de información o prueba, y a la documentación del control, la fecha y hora, la transferencia, el análisis y la enajenación de dicha prueba. Una vez recogido un elemento digital, la cadena de custodia debe mantenerse implantando un sistema de preservación digital adecuado.

b) Copia probatoria

168. Se entiende por copia probatoria el material digital recogido por la investigación en su forma original, que no debe alterarse ni modificarse. Los elementos digitales deben almacenarse en su forma original. Es decir, se debe preservar un original limpio del elemento digital recolectado en todos los formatos en que se recogió.

c) Copias de trabajo

169. Se deben crear una o varias copias del material digital al objeto de analizarlo, y almacenarlas por separado para que el equipo investigador pueda trabajar con la copia, en lugar de con el original. Así se reduce al mínimo la manipulación del original y el peligro de que resulte comprometido o alterado. Todos y cada uno de los cambios realizados en el elemento, incluida la realización de copias, deben documentarse. Si es posible, la copia probatoria y las copias de trabajo deben almacenarse en sistemas separados.

d) Almacenamiento

170. El almacenamiento ayuda a garantizar la persistencia de los elementos digitales y la

146 *Ibid.* Nótese que el uso del término "autenticidad" en este contexto es diferente a su uso en un contexto jurídico.
147 *Ibid.*
148 *Ibid.*
149 *Ibid.*
150 *Ibid.*
151 *Ibid.*

posibilidad de encontrarlos y recuperarlos. El almacenamiento no debe considerarse algo pasivo, sino un proceso activo con tareas y responsabilidades continuas y gestionadas. Incluye el almacenamiento permanente, en el que los medios de almacenamiento son importantes, pero también la gestión de la jerarquía de almacenamiento, la sustitución de los medios, la comprobación de errores, la comprobación de la continuidad (verificar que el elemento no ha sido alterado), la recuperación en casos de desastre y la localización y devolución de los objetos almacenados[152]. La información digital puede almacenarse *in situ* (en línea o en formato físico) o en otro lugar (en línea o en formato físico)[153]. Los contenidos digitales pueden almacenarse en un disco duro local o un soporte local extraíble; o en una unidad en red que forme parte de una red de área local o un servidor remoto o sistema de almacenamiento en la nube. Los factores que deben tenerse en cuenta al elegir una opción de almacenamiento son la capacidad de almacenamiento (espacio); el acceso y control; las copias de seguridad; la legislación pertinente; y la seguridad de la información y la protección de los datos. También se debe tener en cuenta la velocidad, la disponibilidad, el costo, la sostenibilidad, la gestión del almacenamiento y los sistemas de recuperación[154].

i) Copias de seguridad

171. Si se producen pérdidas de datos o errores, los servicios de archivo o técnicos pueden tratar de recuperar los datos. Lo ideal es que antes se haya realizado una copia de seguridad o los datos hayan sido duplicados en un lugar distinto. Las mejores prácticas de tecnología de la información recomiendan tener al menos tres copias de los datos, en al menos dos tipos diferentes de almacenamiento, con al menos una copia separada geográficamente de las demás.

ii) Degradación

172. Una de las dificultades del almacenamiento es que los soportes se degradan con el tiempo. Los servicios de archivo pueden mitigar el riesgo de fallo de almacenamiento utilizando tipos de soportes especialmente duraderos; sin embargo, cualquier dispositivo de almacenamiento acabará teniendo o desarrollando un defecto, desgastándose o fallando aleatoriamente. Aun si no ocurre un fallo total, pueden producirse errores de datos o los archivos pueden resultar corrompidos a medida que los soportes almacenados se deterioran. Por lo tanto, es importante mantener copias de seguridad y supervisar periódicamente la infraestructura de almacenamiento y la permanencia de los archivos almacenados, por ejemplo comprobando periódicamente los valores de direccionamiento de muestras aleatorias para verificar que no se ha producido ninguna degradación.

iii) Obsolescencia

173. Los archivos digitales se vuelven obsoletos cuando el *hardware* necesario para acceder a los datos ya no está razonablemente disponible o no se considera razonable mantenerlo. Independientemente de lo duradero que sea un soporte de almacenamiento, también puede quedarse obsoleto, dificultando o imposibilitando la recuperación de los datos almacenados. Por lo tanto, los equipos de investigación deben asegurarse de mantener y, cuando sea necesario, actualizar los soportes de almacenamiento para mantener la representabilidad y la disponibilidad de los datos.

iv) Recuperación

174. Los archivos digitales pueden ser eliminados accidental o deliberadamente. Cuando un usuario "elimina" un archivo en una computadora, el contenido del archivo eliminado permanece en el soporte de almacenamiento hasta que es sobrescrito por otro archivo[155]. Por lo tanto, cuanta más actividad haya en la computadora o soporte de almacenamiento, más rápido se sobrescribirá y será irrecuperable. La mayoría de las computadoras tienen utilidades de *software*

[152] *Ibid.*, pág. 154.

[153] Shira Scheindlin y Daniel J. Capra, *Electronic Discovery and Digital Evidence in a Nutshell* (Saint Paul, West Academic Publishing, 2009), págs. 21 y 22.

[154] Ng, "How to preserve open source information effectively", pág. 156.

[155] Scheindlin y Capra, *Electronic Discovery and Digital Evidence in a Nutshell*, pág. 24.

integradas en el sistema operativo para permitir la recuperación de los archivos eliminados. Además, existen en el mercado programas de recuperación de datos que a veces se utilizan para "deseliminar" los archivos. Los equipos de investigación en fuentes abiertas tal vez necesiten contar con la ayuda de especialistas en tecnología de la información para acceder a los datos eliminados.

v) Actualización

175. La actualización consiste en copiar el contenido de un soporte de almacenamiento a otro. Su único objeto es evitar la obsolescencia del soporte, por lo que no se trata de una estrategia de preservación integral. Sin embargo, la actualización debe considerarse parte integrante de la estrategia global de preservación[156].

E. Verificación

176. La verificación es el proceso por el cual se establece la exactitud o validez de la información que se ha recogido en línea. La verificación de la información de fuentes abiertas puede integrarse en un análisis de todas las fuentes —incluidas las fuentes cerradas y confidenciales— o basarse exclusivamente en las fuentes abiertas. En relación con la verificación deben tenerse en cuenta tres consideraciones distintas —la fuente, el elemento o archivo digital y el contenido— que deben examinarse conjuntamente y compararse para comprobar su coherencia.

1. Análisis de la fuente

177. El análisis de la fuente es el proceso por el que se evalúa la credibilidad y fiabilidad de una fuente. El entorno en línea presenta dificultades para el análisis de las fuentes, ya que muchas de ellas son anónimas o utilizan pseudónimos. Para analizar correctamente las fuentes de información, los investigadores e investigadoras de fuentes abiertas deben identificar primero la fuente o fuentes correctas, lo que significa atribuir la información a su fuente original. Por "análisis de atribución" se entiende la determinación de la fuente de la información digital —que puede ser un sitio web específico, un suscriptor o usuario de una cuenta o plataforma determinada— o la identidad de las personas autoras o creadoras de determinados contenidos, o quienes los subieron a Internet. No siempre es posible realizar un análisis de atribución, para el cual puede ser necesario investigar más en línea y en el mundo real o emplear técnicas avanzadas de búsqueda y análisis. Aunque conviene identificar la autoría, no suele ser imprescindible para establecer la autenticidad de un elemento digital, ya que hay otras formas de autenticar la información de fuentes abiertas.

a) Procedencia

178. Por procedencia se entiende el origen o la primera existencia conocida de algo. En lo tocante a los contenidos en línea, la procedencia puede referirse a la primera aparición en línea o al elemento original antes de que se subiera a Internet. En el caso de los contenidos en línea, es preferible referirse a la "primera copia encontrada en línea" en lugar de a "la primera copia en línea", ya que el original puede haber sido eliminado. Incluso cuando los equipos de investigación están seguros de haber encontrado la primera versión de, por ejemplo, un video u otra información de fuentes abiertas en línea, no pueden estar seguros de su procedencia debido a la existencia de canales cerrados, como correos electrónicos y grupos de mensajería privados, que pueden haberse utilizado para compartir el elemento antes de su aparición pública en línea[157].

b) Credibilidad

179. El historial de publicaciones de una fuente, su actividad en línea y su presencia en Internet pueden contener información relevante que pese en contra o en favor de su credibilidad. Los investigadores e investigadoras en fuentes abiertas deben examinar la presencia en línea y el historial de publicaciones de una fuente, que puede incluso ayudar a detectar un intento deliberado de engaño. Por ejemplo, si una

[156] Cornell University Library, "Digital imaging tutorial". Disponible en http://preservationtutorial.library.cornell.edu/tutorial/preservation/preservation-03.html.

[157] Por ejemplo, un usuario puede enviar una fotografía por correo electrónico a otro usuario, que luego la sube a las redes sociales. Por lo tanto, el origen de la fotografía es la persona que envió el correo electrónico, no la que la subió a Internet.

fuente publica mensajes sobre hechos en un país concreto, ¿sus demás mensajes sugieren que realmente se encuentra en ese país?

c) Independencia e imparcialidad

180. Las investigaciones deben examinar la imparcialidad de una fuente. Para ello se pueden evaluar los grupos, organizaciones o afiliaciones con que está asociada, así como la forma en que gana dinero y de quién recibe financiación. ¿Existen conexiones o relaciones con alguna de las partes implicadas en el caso o incidente investigado? Al evaluar la independencia de una fuente, hay que examinar si puede estar asociada a entidades relevantes (por ejemplo, las partes de un conflicto). La ideología de una fuente y cualquier afiliación que tenga a un grupo también pueden ser relevantes. Las personas investigadoras deben examinar y descubrir las motivaciones o intereses subyacentes de todas las fuentes, y el grado en que podrían influir en su veracidad.

d) Especificidad

181. Cuanto más precisas sean la información y las afirmaciones, más fácil será probarlas o refutarlas. Las afirmaciones poco concretas y vagas suelen ser más difíciles de evaluar desde un punto de vista crítico.

e) Atenuación

182. Los textos redactados al mismo tiempo que los hechos a que se refieren tienden a considerarse más fiables que los producidos mucho después de que hayan ocurrido los hechos[158]. Este factor puede complicar la labor de investigación en fuentes abiertas cuando no se sabe a ciencia cierta cuándo se creó un texto digital.

2. Análisis técnico

183. El análisis técnico es el análisis de un elemento digital en sí, ya sea un documento, una imagen o un video. Para comprobar la integridad de un archivo, es decir, si ha sido alterado, manipulado o modificado digitalmente, los investigadores e investigadoras en fuentes abiertas pueden considerar apropiado someterlo a un examen forense digital, a veces denominado análisis de investigación digital. Dicho análisis se compone de los siguientes componentes.

a) Metadatos

184. Los metadatos son datos que describen y dan información sobre otros datos. Pueden ser creados por el usuario que generó un elemento, por otros usuarios, por un proveedor de servicios de comunicación o por cualquier dispositivo en el que se crean, transfieren, reciben o ven datos. Los metadatos son importantes para describir un elemento y las circunstancias de su generación, difusión o alteración. Pueden incluir el nombre de la persona que creó un archivo, su fecha de creación, los datos de carga, las modificaciones, el tamaño del archivo y los geodatos. Los metadatos pueden estar integrados en un archivo, ser visibles en una página web o estar presentes en el código fuente. Algunos metadatos pueden ser eliminados antes o durante la carga, o al usar aplicaciones de redes sociales, pero si se dispone de ellos, deben ser revisados por si pueden ayudar a establecer la autenticidad. Los metadatos originales pueden perderse porque las plataformas a menudo transcodifican los contenidos multimedia subidos para optimizar su visualización, compartición o reproducción en línea. En estos casos, los metadatos se referirán al nuevo archivo, y no al original. Cuando los metadatos han sido eliminados, las investigaciones en fuentes abiertas deben buscar otras formas de verificar un elemento.

b) Datos de formato de archivo de imagen intercambiable

185. El formato de archivo de imagen intercambiable es un tipo de metadatos que especifica los formatos de las imágenes, el sonido y las etiquetas auxiliares que utilizan las cámaras digitales, los escáneres y otros sistemas que manejan archivos audiovisuales grabados por cámaras digitales.

c) Código fuente

186. El código fuente es el código de programación que hay detrás de cualquier página web o *software*. En el caso de los sitios web, este código puede ser visto por cualquier persona utilizando diversas herramientas, incluso un navegador web. El código fuente de un sitio

[158] Institute for International Criminal Investigations, *Investigators Manual*, 5ª ed. (La Haya, 2012), pág. 88.

web es fácil de ver utilizando una serie de herramientas disponibles gratuitamente. Puede contener metacontenidos o contenidos ocultos o manipulados, y muestra la estructura de enlaces y los enlaces rotos.

3. Análisis de contenido

187. El análisis de contenido es el proceso mediante el cual se evalúa la autenticidad y veracidad de la información contenida en un video, imagen, documento o declaración. El análisis de contenido es igualmente polifacético e implica el análisis de indicios visuales o, por ejemplo, la corroboración de la imagen con los metadatos. Las características del entorno en línea dan lugar a numerosos problemas que pueden incidir en la validez o veracidad real o supuesta de la información procedente de fuentes abiertas en línea. Entre ellos se encuentran la referencia circular, la descontextualización de la información y el error de interpretación. Los datos de contenido son los datos incluidos en el elemento digital, como un video, una imagen, una grabación sonora, un documento o un texto no estructurado.

a) Identificadores únicos

188. Cuando deban verificar un contenido visual, los equipos de investigación deben empezar por buscar rasgos únicos o identificativos. Puede tratarse de edificios, flora y fauna, personas, símbolos o insignias. Hay que tener especial cuidado al analizar rasgos humanos con objeto de identificar a una persona concreta[159]. Las prácticas de identificación suelen requerir habilidades específicas, como las adquiridas con el tiempo y mediante la formación especializada de la profesión forense. Los análisis realizados por profesionales sin formación pueden ser inexactos, perjudiciales o problemáticos.

b) Información objetivamente verificable

189. A menudo, puede ser útil empezar por identificar lo que podría calificarse como "información objetivamente verificable". Por ejemplo, el tiempo que hacía un día concreto, el nombre y el rango de un oficial al mando o la ubicación de un edificio podrían ser objetivamente verificables. Al evaluar un material de fuentes abiertas se debe contrastar su contenido con esa información objetivamente verificable.

c) Geolocalización

190. La geolocalización es la identificación o estimación de la ubicación de un objeto, una actividad o el lugar desde el que se generó un material digital. Por ejemplo, utilizando técnicas de geolocalización puede ser posible determinar la ubicación desde la que se tomó un video o una fotografía descargada de Internet. Dichas técnicas podrían incluir, por ejemplo, la corroboración de características geográficas únicas presentes en una fotografía, con su ubicación real en un mapa.

d) Cronolocalización

191. La cronolocalización es la corroboración de las fechas y horas de los hechos representados en una información, generalmente imágenes visuales. Por ejemplo, puede ser posible determinar la hora del día en que se tomó una fotografía examinando la longitud de las sombras creadas por la luz del sol, junto con otros indicadores.

e) Totalidad

192. Un documento o un video incompletos pueden ser, no obstante, probatorios, pero toda laguna puede influir en el peso que se atribuya a un elemento. Por lo tanto, al recoger información de fuentes abiertas es importante capturar el archivo de que se trate en su totalidad y, cuando sea importante, capturar el contexto circundante.

f) Coherencia interna

193. Puede realizarse una evaluación de la coherencia interna en relación con un único elemento de

[159] El análisis forense y la identificación de rasgos humanos con herramientas o los análisis humanos (por ejemplo, reconocimiento facial, análisis de la marcha, etc.) requieren una persona experta en la ciencia forense. Véase Nina M. van Mastrigt y otros, "Critical review of the use and scientific basis of forensic gait analysis", *Forensic Sciences Research*, vol. 3, núm. 3 (2018), págs. 183 a 193 (disponible en www.tandfonline.com/doi/full/10.1080/20961790.2018.1503579); Royal Society y Royal Society of Edinburgh, "Forensic gait analysis: a primer for courts" (Londres, 2017) (disponible en https://royalsociety.org/-/media/about-us/programmes/science-and-law/royal-society-forensic-gait-analysis-primer-for-courts.pdf). Véase también European Network of Forensic Science, *Best Practice Manual for Facial Image Comparison* (2018) (disponible en http://enfsi.eu/wp-content/uploads/2017/06/ENFSI-BPM-DI-01.pdf); National Center for Audio and Video Forensics, "Height analysis of surveillance video" (disponible en https://ncavf.com/what-we-do/forensic-height-analysis).

información procedente de una fuente abierta en línea o con un conjunto de información procedente de una fuente concreta (o de fuentes con la misma procedencia o autoría). Al evaluar la coherencia interna de un solo elemento de información en línea se pretende establecer si la información es coherente y congruente por sí sola. Un elemento o conjunto de información internamente coherente no debe contradecirse.

g) Corroboración externa

194. Se habla de corroboración externa cuando una información se encuentra fuera de un elemento digital pero coincide con la veracidad de su contenido y, por lo tanto, la respalda.

F. Análisis investigativo

195. El análisis investigativo es la práctica de revisar e interpretar la información de los hechos para llegar a conclusiones sustantivas relevantes para la toma de decisiones o la construcción de un argumento. El volumen y la calidad variable de la información de fuentes abiertas requiere un enfoque bien estructurado del análisis.

196. Antes de someter la información de fuentes abiertas a determinados tipos de análisis, puede ser necesario procesarla primero. Ello puede implicar traducir información que esté en otro idioma o agregar diferentes conjuntos de datos para ayudar a analizar el comportamiento de individuos, lugares y objetos, así como relaciones o redes, movimientos, actividades o transacciones. También puede ser necesario modificar la naturaleza o el formato de un elemento digital para hacerlo compatible con un *software* específico. Los tipos más comunes de procesamiento de datos son:

a) Traducción: si los datos están en un idioma que no habla el equipo de investigación o que no es procesado por el software necesario para revisar el material, puede ser necesario traducir los datos antes de dar otros pasos;

b) Agregación: pueden ser necesario agregar diferentes conjuntos de datos en uno más grande para poder analizarlo;

c) Reformateo: para que los datos sean más fáciles de buscar o recuperar, puede ser necesario cambiar el formato de un elemento digital.

197. Es aconsejable procesar únicamente las copias de trabajo de un elemento digital, y no el original o copia probatoria. Todo procesamiento de un elemento digital debe ser documentado. Si se emplean tecnologías digitales para procesar datos, por ejemplo analizándolos con algoritmos, como los utilizados en el procesamiento del lenguaje natural (natural language processing) y el aprendizaje profundo (deep learning), se debe tener presente el riesgo de sesgo inherente al procesamiento de dichos datos.

198. Una vez procesada, la información puede ser analizada. Los productos de los análisis de información de fuentes abiertas variarán en función de la finalidad, el tipo y el alcance de la información subyacente, el calendario de producción y su público. Se elaborarán en función de las necesidades de la investigación y podrán incluir gráficos, resúmenes, glosarios, diccionarios y ayudas visuales, como mapas y cartografías[160].

199. Los equipos de investigación deben aplicar normas rigurosas para garantizar la objetividad, la puntualidad, la pertinencia y la exactitud de los datos y las conclusiones contenidas en los productos de análisis, así como para proteger la privacidad y otras consideraciones de derechos humanos, especialmente cuando se trate de información que permita identificar a una persona. Dicha información solo debe incluirse en los productos para los que se haya obtenido el consentimiento de las personas implicadas y que sirvan al objeto directo de la investigación. También deben estudiarse las limitaciones legales y éticas de su uso[161].

200. A continuación se describen tipos comunes de análisis que pueden realizarse para alcanzar los objetivos de la investigación utilizando información de fuentes abiertas.

1. Análisis comparativo de imágenes y videos

201. El análisis comparativo o ciencia comparativa es el proceso de comparar características

[160] Véase el cap. VII, sobre la presentación de los resultados.

[161] Véase el cap. III, sobre el marco jurídico.

de objetos, personas o lugares con otros elementos desconocidos o conocidos cuando al menos uno de los elementos en cuestión es una imagen. Es un análisis del contenido de imágenes y videos, comparando diferentes elementos y características, así como su calidad de imagen y configuración visual (luz, perspectiva, etc.). Aunque muchas personas no expertas en la materia conocen hoy en día los fundamentos del análisis comparativo de imágenes, la asistencia de especialistas cualificados y certificados en análisis forense de videos o criminalística digital puede ayudar a proporcionar análisis científicos y un dictámenes periciales. Las investigaciones relacionadas con los derechos humanos y otros tipos de investigaciones también pueden recurrir a esas personas expertas para dar más peso a sus conclusiones.

2. Análisis interpretativo de imágenes o videos

202. Relacionado con la comparación de imágenes o videos, el análisis interpretativo de imágenes o videos consiste en analizar un elemento digital para comprender su contenido visual. Por ejemplo, el análisis de disparos, heridas, sangre, vehículos, armas y bienes militares o el análisis de la velocidad de un vehículo en movimiento, o de la edad de un individuo, forman parte del análisis interpretativo de imágenes o videos. Puede ser realizado por analistas con fines de investigación o por especialistas, ya sean forenses o en la materia, para establecer los hechos en un procedimiento judicial o llegar a conclusiones sobre violaciones de derechos humanos.

3. Análisis espacial

203. El análisis espacial o geoespacial puede incluir análisis de contenidos visuales y de metadatos en el caso de elementos que ofrecen coordenadas geográficas o nombres de lugares. El análisis espacial implica el examen de diferentes objetos y características del paisaje, a una resolución adecuada, y la corroboración con imágenes de satélite u otras imágenes, geodatos y mapas, el conocimiento adecuado del caso y del contexto, así como el uso de herramientas de sistemas de información geográfica[162].

4. Mapeo de actores

204. El mapeo de actores es una técnica utilizada para determinar quiénes son los actores clave e identificar las relaciones de poder y canales de influencia[163]. Por lo tanto, primero se identifica a los actores clave y luego se establecen las relaciones entre ellos.

5. Análisis de redes sociales

205. Parecido al mapeo de actores, el análisis de redes sociales consiste en determinar y medir las relaciones entre personas, grupos, organizaciones, computadoras, URL y otras entidades de información o conocimiento conectadas[164]. Las personas y grupos suelen denominarse nodos, mientras que los enlaces muestran las relaciones entre los nodos. El análisis de redes sociales utiliza las conexiones en las redes sociales y otras plataformas móviles o digitales para establecer y comprender las relaciones entre los individuos. El análisis de los datos de conexiones o enlaces puede ser realizado manualmente por un miembro de la investigación o con un *software* de análisis.

6. Mapeo de incidentes

206. El mapeo de incidentes es una técnica analítica utilizada para establecer las relaciones temporales y geográficas entre diferentes incidentes, que en el contexto de las violaciones del derecho penal internacional y el derecho internacional de los derechos humanos puede referirse a la ubicación de dichas violaciones o crímenes, y de los hechos anteriores y posteriores. También puede incluir el mapeo de otros hechos importantes, como dónde y cuándo hicieron declaraciones los presuntos autores.

7. Análisis de patrones delictivos o criminales

207. En el contexto de la actividad policial nacional, un patrón delictivo es un grupo de dos o más delitos denunciados o descubiertos por los

[162] Un sistema de información geográfica es una base de datos computacional para gestionar y analizar datos espaciales.

[163] ACNUDH, *Manual on Human Rights Monitoring*, cap. 8, sobre el análisis, pág. 24.

[164] Orgnet, "Social network analysis: an introduction". Disponible en www.orgnet.com/sna.html.

cuerpos de seguridad del Estado. Estos delitos que son únicos porque comparten al menos una característica común en cuanto al tipo de delito; el comportamiento de los delincuentes o las víctimas; las características del delincuente o delincuentes, las víctimas u objetivos; los bienes sustraídos; o el lugar en que fueron cometidos[165]. Del mismo modo, la información de fuentes abiertas puede ayudar a establecer patrones delictivos o criminales en cuanto violación del derecho penal internacional y el derecho internacional de los derechos humanos.

[165] International Association of Crime Analysts, "Crime pattern definitions for tactical analysis", Standards, Methods and Technology Committee White Paper 2011-01, pág. 1.

VII

PRESENTACIÓN DE RESULTADOS

RESUMEN DEL CAPÍTULO

- Los resultados de una investigación en fuentes abiertas, referentes tanto a los datos recogidos como las conclusiones extraídas de esos datos, pueden presentarse de forma oral, visual o escrita.
- Al decidir: a) los formatos que utilizarán y b) los datos que incluirán, los equipos de investigación deben estudiar qué formatos son los más apropiados para su mandato y su público previsto, teniendo en cuenta factores como el nivel de conocimientos tecnológicos del público y la accesibilidad, objetividad, transparencia y seguridad.

208. En este capítulo se describen las formas en que pueden presentarse o comunicarse las investigaciones en fuentes abiertas, incluidas las metodologías, datos brutos y los resultados analíticos. En muchos casos, la información de fuentes abiertas se presenta junto con otra información recolectada mediante otros métodos de investigación. La presentación puede adoptar muchas formas, como informes escritos, orales o visuales, o cualquier combinación de las mismas. Los informes pueden ser para uso interno o externo, y pueden considerarse periciales o no periciales en función de una serie de factores. Los informes deben garantizar los siguientes elementos:

a) Exactitud: deben representarse con exactitud los datos recogidos[166]. Debe incluirse la información exculpatoria, así como una explicación de toda censura o laguna;

b) Atribución: debe distinguirse claramente entre el contenido que es de dominio público o información general no reservada de la información reservada o restringida y del contenido que refleja el juicio o la opinión del equipo de investigación o de otros profesionales. Los equipos de investigación y otras personas que presentan resultados basados en información de fuentes abiertas también deben tomar precauciones y obtener los permisos adecuados para usar los contenidos que puedan pertenecer a otros, por ejemplo obteniendo los derechos de propiedad intelectual necesarios;

c) Totalidad: los resultados deben indicar que los datos en que se basan son completos, especialmente si se excluye algún dato deliberadamente;

d) Confidencialidad: aunque se haya encontrado en fuentes abiertas, se debe evaluar qué material omitir o censurar para proteger la confidencialidad o minimizar riesgos, en particular los riesgos potenciales para las fuentes, testigos, víctimas y miembros de las comunidades vinculadas con la información de fuentes abiertas;

e) Lenguaje: se debe utilizar un lenguaje neutro y evitar el lenguaje emotivo o emocional. Los hechos deben exponerse con claridad, sin abusar de adjetivos o énfasis. Los informes deben estar redactados en un lenguaje que tenga en cuenta las cuestiones de género. De ser posible, los informes públicos deben publicarse en la lengua o lenguas de las comunidades afectadas, además de la lengua o lenguas oficiales utilizadas por el equipo o entidad de investigación;

f) Transparencia: los informes deben exponer con claridad el modo en que se llevó a cabo la investigación, así como sus objetivos, procesos y métodos. Normalmente, esa información se expone en la sección del informe sobre la metodología, pero también debe tenerse esto en cuenta en las descripciones incluidas en todo el texto. Las descripciones deben ser lo más transparentes posible sin crear vulnerabilidades de seguridad, por ejemplo revelando información confidencial.

A. Presentación escrita

209. Los resultados de las investigaciones en fuentes abiertas pueden presentarse por escrito, por ejemplo con informes internos e informes a clientes, así como informes públicos. Uno de los métodos para comunicar esos resultados analíticos es mediante un informe escrito, como en el caso de los informes de ONG, comisiones de investigación, misiones de determinación de hechos y Naciones Unidas, así como los informes periciales para un tribunal o corte, entre otros[167]. La información digital de fuentes abiertas se integra a menudo con otras formas de datos y análisis de fuentes abiertas y cerradas. Los informes escritos deben analizar la información recogida para extraer conclusiones lógicas, estimaciones y predicciones. Los informes deben reflejar una buena metodología y explicar dicha metodología al público destinatario. La

[166] Véase el cap. II.B, sobre los principios metodológicos.

[167] Para un ejemplo de informe escrito de una investigación digital en fuentes abiertas, véase, por ejemplo, Human Rights Investigations Lab, "Chemical strikes on Al-Lataminah: March 25 & 30, 2017 – a student-led open source investigation" (Berkeley, Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley, 2018).

veracidad e integridad de la información en que se basa el informe son cruciales. Cuando los datos son erróneos, se extraen conclusiones erróneas[168].

210. Los informes escritos deben incluir las siguientes secciones, a menos que exista un motivo justificado y expreso para no hacerlo, como la necesidad de mantener la confidencialidad de algunas técnicas, métodos y fuentes de la investigación en línea:

a) Objetivos de la investigación: se deben incluir los objetivos de la investigación y los mandatos subyacentes o instrucciones del cliente, y expresar las preguntas de investigación bien definidas y articuladas;

b) Metodología: se deben incluir los métodos de investigación para permitir que sean replicables y para que el público pueda entender y evaluar la credibilidad de la información y los resultados de la investigación, incluido lo que esta abarca;

c) Actividades realizadas: se debe incluir un resumen de las actividades que se realizaron sean importantes para los resultados o la evaluación de la calidad del análisis, estas incluyen las actividades efectuadas para identificar los datos subyacentes, los datos que se recolectaron y los que se analizaron;

d) Datos y fuentes subyacentes: se debe incluir una descripción de los datos subyacentes, incluidas las fuentes y la calidad de los mismos;

e) Lagunas o incertidumbres: se debe señalar cualquier laguna o incertidumbre que pueda ser importante para los resultados en los datos subyacentes;

f) Resultados y recomendaciones: se deben incluir las interpretaciones del equipo de investigación sobre los datos, o sus conclusiones basadas en el análisis de los datos, señalando posibles advertencias y nuevas pistas.

B. Presentación oral

211. Si los resultados de una investigación en fuentes abiertas llegan a un tribunal, los miembros del equipo podrían tener que declarar como testigos, presentando su investigación mediante un testimonio oral. También pueden presentarse oralmente los resultados de la investigación ante comisiones de la verdad, foros de ONG, tribunales populares o medios de comunicación.

212. Toda persona que deba presentar oralmente los resultados de su investigación en fuentes abiertas debe ser capaz de explicar con claridad y exactitud el trabajo, describiendo la metodología aplicada y las herramientas utilizadas. Así se garantizará que el testimonio oral y los resultados descritos se traten con la debida importancia.

213. En el caso de los procedimientos judiciales, a menudo se llama a testificar a la persona responsable de la investigación, que debe ser capaz de hablar sobre el trabajo de su equipo. Para ello, obviamente, debe conocer lo que ha hecho su equipo y poder responder a preguntas sobre las funciones desempeñadas y el razonamiento subyacente a cualquier decisión relativa al alcance de la investigación, sus métodos, las herramientas utilizadas, etc. Las personas investigadoras pueden ser llamadas a declarar en calidad pericial o como testigos no expertos. Los testigos peritos —testigos considerados peritos por su experiencia, conocimientos, competencias, formación, educación o credenciales— pueden testificar sobre las conclusiones a que llegaron como de otros productos del trabajo analítico. Los testigos no expertos suelen limitarse a testificar sobre los hechos y, en concreto, sobre los que observaron personalmente.

[168] Teniendo en cuenta las circunstancias y los requisitos de confidencialidad, se recomienda la revisión por pares para garantizar la exactitud y calidad de los datos, así como del análisis y las conclusiones extraídas de los mismos.

C. Presentación visual

214. La visualización de datos es la representación gráfica de la información en forma de, por ejemplo, diagramas, gráficos, cuadros, mapas e infografías que proporcionan una forma accesible de ver y comprender las tendencias, los valores atípicos y patrones de datos[169]. Puede incluir diagramas y otras representaciones gráficas de datos en el espacio y el tiempo; gráficos (incluidos los que demuestran conexiones, tendencias o relaciones matemáticas); análisis de redes, que demuestran las relaciones entre distintas personas; y cuadros o diagramas estadísticos. Los mapas bidimensionales y tridimensionales para visualizar objetos en el espacio y tiempo, así como las reconstrucciones tridimensionales de diversos lugares, incluidas las escenas del delito, también forman parte del repertorio de visualización de datos[170]. Estas herramientas pueden ayudar a comprender grandes cantidades de datos, como las que se suelen utilizar en las investigaciones en fuentes abiertas, o a entender mejor hipótesis fácticas complejas.

215. Cabe destacar otros tipos de visualizaciones de datos, como las siguientes:

a) Mapas mentales: un mapa mental es un medio gráfico de representar ideas y conceptos y la manera en que se relacionan entre sí. Los mapas mentales estructuran la información para que sea más fácil analizarla, sintetizarla y comprenderla. Suelen incluir una explicación de cómo se descubrieron los datos subyacentes;

b) Flujogramas: un flujograma es una representación gráfica de una secuencia de hechos, como los pasos incluidos en un algoritmo, flujo de trabajo o procesos similares;

c) Infografía: una infografía es una representación ilustrada de una idea o concepto; puede utilizarse para representar información estadística.

216. La información de fuentes abiertas puede presentarse de diversas maneras, desde la muestra audiovisual de un solo video o sitio web hasta presentaciones multimedia interactivas, digitales y agregadas[171]. Las demostraciones e ilustraciones visuales, o plataformas digitales, pueden utilizarse para mostrar la información para que el público destinatario comprenda de forma más fácil los hechos subyacentes. Algunos ejemplos son las exposiciones secuenciales de los hechos, las fotografías compuestas (como una vista de 360º de la escena del delito) y los videos editados.

217. En el caso de la presentación de pruebas multimedia y visualizaciones de datos en un tribunal, o en otras presentaciones en público, los investigadores e investigadoras deben preveer las cuestiones técnicas que puedan surgir, incluyendo el tipo de plataformas que se necesiten para exponer de forma clara a quienes deban decidir sobre el caso. Al decidir sobre la mejor forma de representar los datos subyacentes, se deben tener en cuenta una serie de factores, como el público destinatario y su grado de comodidad con los posibles formatos y su capacidad para comprender la información

[169] Entre los ejemplos de presentación visual en diferentes contextos se encuentran las plataformas digitales utilizadas como pruebas demostrativas en la causa de la Corte Penal Internacional *Prosecutor v. Ahmad Al Faqi Al Mahdi* y en el asunto del Tribunal Especial para el Líbano *Prosecutor v. Salim Jamil Ayyash et al.*; el informe con las conclusiones detalladas de la comisión internacional independiente de investigación sobre las protestas en el Territorio Palestino Ocupado (disponible en www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session40/Documents/A_HRC_40_74_CRP2.pdf); BBC Africa Eye, "Cameroon atrocity: what happened after Africa Eye found who killed this woman", BBC News, 30 de mayo de 2019 (disponible en www.bbc.com/news/av/world-africa-48432122/cameroon-atrocity-what-happened-after-africa-eye-found-who-killed-this-woman). Véase también, en general, la labor de Forensic Architecture y SITU Research.

[170] Véase, por ejemplo, International Criminal Court Digital Platform: Timbuktu, Mali (desarrollado por SITU Research para la causa *Al Mahdi* de la Corte Penal Internacional). Disponible en http://icc-mali.situplatform.com. Véanse también diversas investigaciones en fuentes abiertas en línea y sus informes visuales en Forensic Architecture. Disponible en https://forensic-architecture.org/methodology/osint.

[171] Aunque no se ha presentado ante ningún tribunal, el Equipo de Investigaciones Visuales del New York Times ha producido una serie de explicaciones visuales diseñadas para agregar información de fuentes abiertas en línea, analizar incidentes complejos e informar sobre los resultados. Véase, por ejemplo, Nicholas Casey, Christoph Koettl y Deborah Acosta, "Footage contradicts U.S. claim that Nicolás Maduro burned aid convoy", *New York Times*, 10 de marzo de 2019 (disponible en www.nytimes.com/2019/03/10/world/americas/venezuela-aid-fire-video.html); Malachy Browne y otros, "10 minutes. 12 gunfire bursts. 30 videos. Mapping the Las Vegas massacre", *New York Times*, 21 de octubre de 2017 (disponible en www.nytimes.com/video/us/100000005473328/las-vegas-shooting-timeline-12-bursts.html).

que se comunica[172]. En definitiva, todas las presentaciones deben promover el objetivo de esclarecer los hechos relevantes para un caso de una manera que sea probatoria y no perjudicial, y deben cumplir los requisitos legales y éticos de la jurisdicción en que se presenta la información.

[172] Véase Alexa Koenig, "Open source evidence and human rights cases: a modern social history", en *Digital Witness: Using Open Source Information for Human Rights Investigation, Documentation and Accountability*, Sam Dubberley, Alexa Koenig y Daragh Murray, eds. (Oxford, Oxford University Press, 2020), págs. 38 a 40.

VIII

GLOSARIO

RESUMEN

- Términos y definiciones utilizadas en las investigaciones de fuentes abiertas o que pueden surgir en recursos relevantes o conexos.

218. Este capítulo contiene términos y definiciones que pueden ser útiles para las investigaciones en fuentes abiertas. No todos los términos se utilizan en el Protocolo, pero se incluyen porque pueden aparecer en recursos relevantes o conexos.

Air gap: cuando un dispositivo digital no está conectado directamente a Internet ni a ninguna red, lo que proporciona seguridad a la información que contiene.

Algoritmo: procedimiento o conjunto de instrucciones bien definidas que permiten a una computadora resolver un problema o responder a un supuesto predeterminado.

Anonimización: proceso que hace imposible identificar a un individuo concreto.

Aprendizaje automático: tipo de inteligencia artificial que utiliza técnicas estadísticas para dar a las computadoras la capacidad de "aprender" de dichos datos, sin ser programadas explícitamente.

Archivo digital: colección de documentos, páginas web o registros electrónicos. El término también puede referirse a una organización formal o informal que se responsabiliza de preservar la información y ponerla a disposición de los usuarios autorizados.

Archivo nativo: archivo en su formato original.

Autoridad de Números Asignados en Internet (IANA): organización que supervisa la asignación en todo el mundo de direcciones IP, números de sistemas autónomos y sistemas de nombres de dominio.

Baliza: mecanismo para controlar la actividad y el comportamiento de un usuario. Consiste en un elemento pequeño y discreto (a menudo invisible) situado en una página web (tan pequeño como un solo píxel transparente) que, al ser reproducido por el navegador, comunica a un tercero información sobre el navegador y la computadora que se están utilizando.

Búsqueda booleana: técnica de búsqueda en Internet que permite a los usuarios combinar palabras clave con operadores o modificadores (AND, OR, NOT) para acotar los resultados de la búsqueda y ofrecer así resultados más relevantes y específicos.

Blockchain: tecnología basada en la criptografía en la que se puede utilizar un registro abierto y distribuido, compuesto por "bloques", para dejar constancia de las transacciones entre dos partes o entidades de forma eficiente, verificable y permanente.

CAPTCHA: este acrónimo en inglés de "prueba de Turing pública y completamente automatizada para diferenciar a las computadoras de los seres humanos" es un tipo de prueba desafío-respuesta utilizada en computación para determinar si un usuario es humano.

Cifrado: el proceso de hacer que los datos sean inaccesibles sin una clave para descifrarlos.

Computación en la nube: modelo de operaciones que permite almacenar, procesar y analizar datos a través de una intranet o de Internet. Hay tres tipos de nubes: privadas, públicas e híbridas.

Cookie: pequeño conjunto de datos que envía un sitio web y que se almacena en la memoria de la computadora del usuario o se escribe en el disco de esta para que lo utilice el navegador. Las *cookies* suelen ser necesarias para que un sitio web funcione mejor, ya que permiten almacenar las preferencias y los datos de identidad del usuario, lo que evita que este tenga que introducir constantemente esos datos en sus visitas siguientes.

Corporación para la Asignación de Nombres y Números en Internet (ICANN): organización encargada de garantizar el funcionamiento estable y seguro de Internet coordinando el mantenimiento y los procedimientos de varias bases de datos relacionadas con los espacios de nombres y números de Internet.

Criptografía: la práctica de codificar o descodificar digitalmente la información.

Datos de tráfico: datos tratados con el fin de transmitir información sobre una red de comunicaciones electrónicas o para la facturación de dicha comunicación. Estos datos incluyen los relativos al encaminamiento, la hora o la duración de una comunicación.

Datos estructurados: datos o información que se ajustan a un formato rígido en un repositorio (normalmente una base de datos, pero también podría ser un conjunto de formularios ya hechos) de manera que sus elementos estén fácilmente disponibles para su tratamiento y análisis.

Datos integrados: datos almacenados en un archivo fuente o en una página web.

Datos no estructurados: datos e información que se presentan en formas muy diversas, que no están organizados en un formato rígido y que, por lo tanto, no son fáciles de tratar y analizar. Suelen ser texto, pero también pueden incluir archivos de imagen, sonido y video.

Dirección del Protocolo de Internet (IP): cualquier dispositivo digital que se conecte a Internet tiene una dirección IP. Hay dos tipos de direcciones IP: IPv4 (número de 32 bits) e IPv6 (número de 128 bits). Las direcciones IP sirven para identificar computadoras y otros dispositivos en Internet.

Dragnet: en el contexto digital, un amplio sistema de recogida o vigilancia automatizada.

Firma criptográfica: proceso matemático para verificar la autenticidad de un elemento digital. Mediante un algoritmo, se pueden generar dos claves vinculadas matemáticamente: una privada y otra pública. Para crear una firma digital, se utiliza un *software* que crea un *hash* de los datos electrónicos. La clave privada se utiliza entonces para cifrar el *hash*.

Formato de documento portátil (PDF): formato de archivo de diseño fijo que conserva el formato de un documento (incluidos los tipos de letra, el espaciado y las imágenes) independientemente del *software*, el *hardware* y los sistemas operativos utilizados para abrir y ver el documento. La conversión de un archivo de su formato original a un PDF elimina sus metadatos, proporcionando una imagen estática del documento.

Foro de Internet (también conocido como foro de debate): sitio web en el que los usuarios pueden publicar mensajes y mantener conversaciones. Los foros suelen contener mensajes más largos que los vistos en las salas de chat y son más propensos a archivar contenidos.

Hash* o valor *hash: cálculos que pueden ejecutarse en cualquier tipo de archivo digital para generar una cadena alfanumérica de longitud fija que puede utilizarse como prueba de que un archivo digital no ha sido modificado. Esta cadena seguirá siendo la misma cada vez que se ejecute el cálculo mientras el archivo no cambie.

Ingeniería social: la manipulación psicológica de una persona para acceder a una información sin autorización. Es similar a la piratería computacional, pero explota una vulnerabilidad humana en lugar de una vulnerabilidad técnica. Hay muchos tipos diferentes de ingeniería social, como el *phishing* y el *spear phishing*.

Inteligencia artificial (IA): rama de la computación dedicada a desarrollar programas para que las máquinas aprendan a reaccionar ante variables desconocidas y adaptarse a nuevos entornos.

Interfaz de programación de aplicaciones (API): código que permite que los programas de *software* se comuniquen entre sí.

Intranet: red computacional privada que utiliza los protocolos de Internet y la conectividad de red para establecer una versión interna de Internet.

Lenguaje de Marcación de Hipertexto (HTML): lenguaje de programación que se utiliza para diseñar páginas web a las que se accede mediante un navegador.

Localizador uniforme de recursos (URL): la ubicación de una página web en Internet. Es lo mismo que una dirección web.

Macrodatos: grandes conjuntos de datos que pueden analizarse para detectar correlaciones entre puntos de datos y revelar pautas que ayuden a prever comportamientos. Las principales características de los macrodatos son el volumen y la complejidad.

Malware: *software* malintencionado que está diseñado para causar daños a un dispositivo digital, red, servidor o usuario. Hay muchos tipos diferentes de *malware*, como virus, troyanos, programas secuestradores *(ransomware)*, *adware* y programas espía *(spyware)*.

Máquina virtual: *software* que emula un sistema computacional.

Metadatos: datos sobre datos. Contienen información sobre un archivo electrónico que está integrada o asociada al archivo. Los metadatos suelen incluir las características y el historial de un archivo, como su nombre, tamaño y fechas de creación y modificación. Los metadatos pueden describir cómo, cuándo y quién recogió, creó, accedió, modificó y formateó un archivo digital.

Minería de datos: práctica que consiste en examinar y extraer datos de bases de datos para generar conocimientos o nueva información.

Nombre de dominio: etiqueta que identifica un dominio de red. En Internet, los nombres de dominio se forman con arreglo a las reglas y procedimientos del Sistema de Nombres de Dominio (DNS). En general, un nombre de dominio representa un recurso del Protocolo Internet (IP), como una computadora personal utilizada para acceder a Internet, un servidor

que aloja un sitio web, el propio sitio web o cualquier otro servicio comunicado por Internet.

Preservación digital: las políticas y estrategias necesarias para gestionar y mantener la información digital con valor perdurable a lo largo del tiempo, de modo que la información digital sea accesible y utilizable por sus usuarios previstos en el futuro.

Protocolo de Transferencia de Hipertexto (HTTP): protocolo subyacente a Internet que define cómo se transfieren y reciben los datos.

Proveedor de servicios de Internet (PSI): entidad que proporciona a los usuarios de Internet servicios para acceder y utilizar la red.

Proveedor de servicios web: entidad que proporciona servicios y productos en Internet, como una empresa de redes sociales.

Pseudonimización: el tratamiento de datos personales de manera que la información ya no pueda atribuirse a un sujeto de datos específico sin utilizar información adicional.

Raspado: método de extracción masiva de datos de sitios web.

Rastreador: un tipo de *cookie* que aprovecha la capacidad de un navegador para mantener un registro de las páginas web que se han visitado, los criterios de búsqueda que se han introducido, etc. En general, los rastreadores son *cookies* persistentes que mantienen un registro continuo del comportamiento de un visitante en particular.

Red de área local (LAN): conjunto de dispositivos digitales conectados a la misma red en una ubicación física definida.

Red privada virtual (VPN): red segura o sistema de nodos seguros que utiliza el cifrado y otros procesos de seguridad para garantizar que solo los usuarios autorizados puedan acceder a la red. Las VPN ocultan la dirección IP y evitan que los datos sean interceptados.

Registrante del nombre de dominio: la persona, empresa u otra entidad que es propietaria o titular de un nombre de dominio.

Sala de chat: sitio web en Internet que permite a los usuarios mantener conversaciones en tiempo real en línea.

Sistema de nombres de dominio (DNS): sistema por el que se regula la asignación de nombres de dominio.

***Software* predictivo**: *software* que utiliza algoritmos predictivos y aprendizaje automático para analizar datos y hacer previsiones sobre el futuro o sobre acontecimientos o comportamientos desconocidos.

Stripping: proceso tecnológico para eliminar los metadatos de un archivo sin convertirlo a otros formatos.

***Web crawler* (también denominado araña web o *spiderbot*)**: programa que navega sistemáticamente por Internet según una secuencia automatizada de comandos para descargar e indexar los sitios web visitados.

Web oscura: la parte de Internet a la que solo se puede acceder mediante un *software* especial, lo que permite a los usuarios y a los operadores de los sitios web permanecer en el anonimato e impedir ser rastreados.

Web superficial: la parte de Internet a la que se puede acceder mediante cualquier navegador y en la que se pueden realizar búsquedas con los motores de búsqueda tradicionales.

WHOIS: registro que identifica quién posee un determinado nombre de dominio basándose en la entidad que lo registró. Las investigaciones en fuentes abiertas pueden utilizar una herramienta de búsqueda WHOIS durante el proceso de análisis y verificación de las fuentes.

World Wide Web (WWW): espacio de información en que los documentos y otros recursos web, identificados mediante URL, pueden estar interconectados por hipertexto y son accesibles a través de Internet. Los usuarios pueden acceder a los recursos de la World Wide Web mediante una aplicación computacional denominada navegador web.

ANEXOS

RESUMEN

- Modelo de plan de investigación en línea
- Modelo de evaluación de los riesgos y amenazas digitales
- Modelo de evaluación del panorama digital
- Formulario para recolectar datos en línea
- Consideraciones para la validación de nuevas herramientas

Anexo I

Modelo de plan de investigación en línea

Número de referencia de la investigación:	
Fecha de la evaluación:	
Resumen de la investigación: *asunto y ámbito territorial y temporal de la investigación*	

1. Objetivos y actividades previstas

Incluye los objetivos y la estrategia de la investigación en línea, así como las actividades específicas con su calendario de ejecución.

2. Resumen de la evaluación del panorama digital

Incluye una evaluación del panorama digital en el territorio geográfico investigado, como las redes sociales, las aplicaciones móviles y otras tecnologías populares, así como quién tiene acceso a esas tecnologías y las utiliza.

3. Estrategia de mitigación de riesgos y medidas de protección

Incluye las principales conclusiones de la evaluación de los riesgos y amenazas digitales, junto con una estrategia para identificar, gestionar y responder a dichas amenazas.

4. Mapeo de actores relevantes

Incluye una lista de las primeras personas que podrían haber recogido contenidos en línea potencialmente relevantes que ya han desaparecido, y los archivos digitales y proveedores de servicios de Internet y basados en la web que podrían tener versiones originales o metadatos adicionales de contenidos en línea que puedan obtenerse mediante una solicitud de asistencia. Aunque las investigaciones no judiciales pueden carecer de la autoridad legal para solicitar información de fuentes cerradas, podría ser de ayuda tener contactos dentro de los proveedores de servicios de Internet que puedan responder a las preguntas y ayudar a los usuarios a navegar por su plataforma.

5. Funciones y responsabilidades

Incluye la definición de las funciones y responsabilidades de los miembros del equipo y convendría identificar a un punto focal que coordine las actividades en línea. También puede incluir una evaluación de la persona que será potencialmente responsable de declarar ante un tribunal si se da el caso.

6. Recursos

Incluye una evaluación de las necesidades de personal (número de investigadoras e investigadores, diversidad e inclusividad del personal), así como cualquier formación especializada y material necesario para las actividades de investigación en línea.

7. Documentación

Incluye instrucciones específicas sobre cómo y dónde deben documentarse las actividades de investigación en línea de los miembros del equipo.

Anexo II

Modelo de evaluación de riesgos y amenazas digitales

Número de referencia de la investigación:	
Fecha de la evaluación	
Resumen de la investigación: *asunto y ámbito territorial y temporal de la investigación*	
Objetivos de la investigación:	

1. ¿Cuáles son sus bienes?

Personas (desglosadas por género):
Bienes tangibles:
Bienes intangibles (por ejemplo, datos):

2. ¿Cuáles son sus vulnerabilidades?

3. ¿Qué tipos de amenazas podrían explotar esas vulnerabilidades y dañar sus bienes?

4. ¿Quiénes son los posibles agentes generadores de amenazas?

A. ¿Cuáles son sus intereses?
B. ¿Cuáles son sus capacidades?
C. ¿Cuál es la probabilidad de que haya un ataque?

5. ¿Qué medidas de mitigación de riesgos son posibles o adecuadas? ¿Es necesario responder a los diferentes riesgos que enfrentan los distintos géneros?

Se deben tener en cuenta:

- Los daños físicos
- Los daños digitales
- Los daños psicosociales

Anexo III

Modelo de evaluación del panorama digital

Número de referencia de la investigación:	
Fecha de la evaluación:	
Resumen de la investigación: *asunto y ámbito territorial y temporal de la investigación*	
Objetivos de la investigación:	

El asterisco (*) indica que la investigación debe tener en cuenta diversos factores como la edad, el género, la ubicación y otros datos demográficos pertinentes.

1.	Partes relevantes (comunidades específicas, grupos armados, etc.). Indíquese si existe alguna diferencia en el uso de la tecnología o la representación en línea por género, edad o discapacidad en cada una de las partes.
2.	Idiomas relevantes (incluyendo dichos y otras lenguas de uso interno)*
3.	Motores de búsqueda de uso frecuente*
4.	Plataformas de redes sociales populares*
5.	Sitios web populares*
6.	Uso o acceso a Internet (desglosado por género, edad, etc.)
7.	Preferencias de teléfono celular o sistema operativo (desglosadas por sexo, edad, etc.)
8.	Aplicaciones móviles populares (desglosadas por sexo, edad, etc.)
9.	Proveedores de telecomunicaciones
10.	Conectividad: ubicación de las torres de telefonía celular y Wi-Fi
11.	Leyes pertinentes (libertad de expresión, acceso a la información, privacidad)
12.	Medios de comunicación y periodistas (presencia en línea)
13.	Bases de datos abiertas (por ejemplo, de datos gubernamentales, datos de ONG o investigaciones)
14.	Bases de datos de pago (por ejemplo, de datos gubernamentales, de empresas privadas o de investigaciones)
15.	Representatividad de los contenidos en línea (grupos incluidos y excluidos)

Anexo IV

Formulario para la recolección de datos en línea

1. Información sobre la persona que recoge la información

Investigación:

Persona que recoge la información:

Dirección IP de la persona que recoge la información:

Inicio de la recogida (sello de fecha y hora):

Fin de la recogida (sello de fecha y hora):

2. Información sobre el objetivo

Dirección web (URL):

Código fuente HTML:

Captura de pantalla:

Datos capturados:

Dirección(es) IP:

3. Información sobre el paquete de datos recogidos

Nombre del archivo del paquete de datos recogidos:

Lista de valores *hash* del paquete de datos recogidos:

Valor *hash* del archivo en que figura la lista de valores *hash* del paquete de datos recogidos:

4. Servicios utilizados

Producto(s) de *software*:

Servicio de hora:

Servicio IP:

Servicio WHOIS:

Anexo V

Consideraciones para la validación de nuevas herramientas

Características

Código abierto o código cerrado
De pago o gratis
Identidad, afiliaciones o intereses del propietario (persona o empresa)
Financiación (¿cómo y cuán bien se financia la herramienta? ¿Cuál es la vida útil probable del producto?)

Preguntas de seguridad

¿A quién pertenece la herramienta o el código subyacente?
¿El código subyacente es abierto o cerrado?
¿Se audita la herramienta de forma independiente?
¿Dónde se almacenarán los datos recogidos?
¿Quién tendrá acceso a los datos recogidos?
¿Cuál es la infraestructura de seguridad de la herramienta?
¿Qué obligaciones legales podrían afectar la seguridad del uso de la herramienta?
Si hay un incumplimiento de la ley, ¿hay derecho a reparación?

Preguntas prácticas

¿Cuál es la funcionalidad de la herramienta?
¿La herramienta es fácil de usar?
¿Cuál es la capacidad de asistencia al usuario del propietario, el proveedor o la herramienta?
¿Con qué frecuencia se actualiza la herramienta?
¿La herramienta es compatible con otros sistemas?

HUMAN RIGHTS CENTER
UC Berkeley School of Law

University of California
Human Rights Center (HRC)
2224 Piedmont Avenue
Berkeley, CA 94720 (Estados Unidos)
Correo electrónico: hrc@berkeley.edu
Sitio web: https://humanrights.berkeley.edu/

NACIONES UNIDAS
DERECHOS HUMANOS
OFICINA DEL ALTO COMISIONADO

Oficina del Alto Comisionado de las Naciones
Unidas para los Derechos Humanos
Palacio de las Naciones
CH 1211 Genève 10 (Suiza)
Correo electrónico: ohchr-infodesk@un.org
Sitio web: www.ohchr.org/es

Publicado conjuntamente por las Naciones Unidas, en nombre de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, y el Centro de Derechos Humanos de la Facultad de Derecho de la Universidad de California, Berkeley.

ISBN: 978-92-1-154246-2

Printed at United Nations, Geneva – 2012695 **(S)** – January 2024 – 1,396 – **HR/PUB/20/2**