Organización
de las Naciones Unidas
para la Educación,
la Ciencia y la Cultura

CÓMO DESARROLLAR LA SEGURIDAD DIGITAL PARA EL PERIODISMO

Una encuesta sobre temas escogidos

Jennifer R. Henrichsen • Michelle Betz • Joanne M. Lisosky

SERIE DE LA UNESCO SOBRE LIBERTAD EN INTERNET

CÓMO DESARROLLAR LA SEGURIDAD DIGITAL PARA EL PERIODISMO

Una encuesta sobre temas escogidos

Jennifer R. Henrichsen • Michelle Betz • Joanne M. Lisosky

Un informe elaborado por la División de Libertad de Expresión y Desarrollo de los Medios de Comunicación de la UNESCO. Las opiniones expresadas en este informe corresponden a las autoras y no reflejan necesariamente los puntos de vista de la UNESCO o su División de Libertad de Expresión y Desarrollo de los Medios de Comunicación.

Organización
de las Naciones Unidas
para la Educación,
la Ciencia y la Cultura

Oficina en México

Publicado en 2016 por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, 7, place de Fontenoy, 75352 París 07 SP, Francia, y la Oficina de la UNESCO en México, Presidente Masaryk 526, Polanco, 11560, México, Ciudad de México

ISBN: 978-92-3-300038-4

Título original: Building digital safety four journalism, publicado en 2015 por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura.

Esta publicación fue posible gracias a la contribución del Reino de Dinamarca y la traducción al español con financiamiento de la Oficina de la UNESCO en MÉXICO.

Coordinación y supervisión de la traducción, edición y publicación de la versión en español: Nuria Sanz, Carlos Tejada, José Pulido Mata, Chantal Connaughton, Rodrigo Morlesin, **Oficina de la UNESCO en MÉXICO**.

Traducción: Rafael Sánchez León

Impreso en México

CÓMO DESARROLLAR LA SEGURIDAD DIGITAL PARA EL PERIODISMO: UNA ENCUESTA SOBRE TEMAS ESCOGIDOS

Autoras:

Jennifer R. Henrichsen, Coordinadora de Programas e Investigación, Periodismo Después de Snowden, Centro Tow de Periodismo Digital de la Escuela de Periodismo de la Universidad de Columbia

Michelle Betz, Asesora, International Media Development

Dra. Joanne M. Lisosky, Profesora de Comunicación, Universidad Luterana del Pacífico

Con especial agradecimiento a los individuos de las siguientes organizaciones, quienes accedieron amablemente a ser entrevistados para esta publicación:

Access, Al Jazeera América, Artículo 19, Bytes for All, Citizen Lab, Universidad de Columbia, Comité para la Protección de Periodistas, Fundación para los Derechos Digitales, Fundación Fronteras Electrónicas, eQualit.ie, Federación de Periodistas Nepalíes, Freedom House, Free Press, Global Journalist Security, Global Voices Advocacy, Global Voices, Índice sobre Censura, Centro Internacional para Periodistas, Federación Internacional de Periodistas, Apoyo para Medios de Comunicación Internacionales, Instituto Internacional para la Seguridad Informativa, Fundación Internacional de Medios de Comunicación de Mujeres, Internews, Junta Internacional de Investigación e Intercambios, Asociación Iraquí para la Defensa de los Derechos de los Periodistas, Management Magazine, Iniciativa para la Defensa Legal de los Medios de Comunicación, Instituto Nacional Demócrata, Proyecto de Herramientas Abiertas para Internet, Fondo para Tecnología Abierta, Centro Americano PEN, Reporteros sin Fronteras, Robinson + Yu, Fondo Rory Peck, Centro SKeyes para Medios de Comunicación y Libertad Cultural, Alianza de la Prensa del Sureste Asiático, Colectivo para una Tecnología Táctica, The Guardian Project, The Mozilla Corporation, The Mozilla Foundation, The New America Foundation, Today's Zaman, Centro Tow para Periodismo Digital de la Escuela de Periodismo de la Universidad de Columbia, Trustwave, y diversos periodistas, blogueros y activistas de los derechos humanos autónomos.

Las encuestas incluidas en este informe fueron traducidas por:

Abeer Al Kazimi, Frederic Castellan, George Donald, Maren Anderson Johnson, Mahlon Meyer, Bassel Sommakia, Tamara R. Williams, Katie Youtz, y Ellen Wenjia Zhou.

Un agradecimiento para aquellos que leyeron borradores de este informe o proporcionaron orientación en diversas etapas del proceso de investigación:

Binod Bhattarai, Eva Galperin, Sabina Izzatli, Geoffrey King, Tom Lowenthal, Silvia Chocarro Marcesse, Karen Reilly, Seamus Tuohy y Eric Zimmermann.

Evento de lanzamiento

La investigación para este estudio fue lanzada en el Foro de Gobernanza de Internet de Estambul, el 3 de septiembre de 2014, en un taller auspiciado conjuntamente con Artículo 19, el Comité para la Protección de Periodistas y el Centro de Estudios sobre Libertad de Expresión (CELE) de la Universidad de Palermo, Argentina. Expresamos nuestro agradecimiento por los comentarios del público y los panelistas. Los oradores en el panel fueron:

Sr. Geoffrey King, Coordinador para la Defensa de Internet y Especialista en Seguridad Digital, Comité para la Protección de Periodistas, Estados Unidos de América

Sr. Eduardo Bertoni, Investigador, Centro de Estudios sobre la Libertad de Expresión y el Acceso a la Información (CELE) de la Universidad de Palermo, Argentina

Sra. Laura Tresca, Responsable de Libertad de Expresión en Brasil, Artículo 19

Sra. Silvia Grundmann, Encargada de la División de Medios de Comunicación, Consejo de Europa

Sr. Scott Busby, Vice-subsecretario de la Oficina de Democracia, Derechos Humanos y Asuntos Laborales del Departamento de Estado, Washington, DC.

Índice

Prólogo

Como agencia de las Naciones Unidas con el mandato de promover la libertad de expresión y su corolario, la libertad de prensa, la UNESCO tiene el compromiso duradero de fomentar la seguridad de los periodistas. La seguridad de los actores periodísticos interconectados digitalmente tiene importantes implicaciones para la libertad de expresión, la libertad de prensa y la protección de la privacidad, y es un tema de especial preocupación para la UNESCO.

Con el fin de mejorar el entendimiento a nivel global sobre las incipientes amenazas a la seguridad vinculadas a los desarrollos digitales, la UNESCO encargó esta investigación dentro de los esfuerzos actuales de la Organización por implementar el Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad, de carácter interinstitucional y encabezado por la UNESCO. Dicho Plan de las Naciones Unidas nació a partir del Programa Internacional para el Desarrollo de la Comunicación (PIDC) de la UNESCO, que concentra gran parte de su labor en promover la seguridad para los periodistas.

La seguridad de los periodistas, incluyendo la seguridad digital, es un tema de interés público de gran envergadura. Es vital para quienes se dedican al periodismo, para sus familias y para sus fuentes. Es esencial para el bienestar de las instituciones de medios de comunicación, la sociedad civil, el mundo académico y el sector privado en términos más amplios. Si valoramos el libre flujo de información para los ciudadanos, sus gobiernos y sus organizaciones internacionales, entonces la seguridad de los periodistas resulta fundamental.

En resumen, cuando es seguro dedicarse al periodismo, la sociedad se beneficia. Sin embargo, con el auge de las plataformas digitales, garantizar esta seguridad se ha vuelto más complicado. Existen nuevas vulnerabilidades abiertas a lo largo de toda la cadena de valor de la interconexión digital; y las nuevas dimensiones digitales no están desvinculadas de las amenazas existentes a periodistas en el mundo físico.

El presente estudio, basado en investigaciones realizadas por Jennifer R. Henrichsen, Michelle Betz y Joanne M. Lisosky, nos ayuda a comprender y abordar los nuevos desafíos como un problema creciente a la hora de garantizar la seguridad de los periodistas. La investigación fue posible gracias al gobierno de Dinamarca, a quien expresamos nuestro agradecimiento. Las ideas y opiniones emitidas en esta publicación corresponden a las autoras; no son necesariamente las de la UNESCO y no comprometen a la Organización.

Al examinar casos a nivel mundial, esta publicación sirve como recurso para una variedad de actores. En pocas palabras, examina las amenazas en constante desarrollo y evalúa las medidas preventivas y protectoras. Muestra que la seguridad digital para el periodismo abarca, pero también trasciende, la dimensión técnica. Se hacen recomendaciones para gobiernos, colaboradores y fuentes del periodismo, agencias de noticias, capacitadores, corporaciones y organismos internacionales.

Aunque no todas las personas que contribuyen al periodismo son periodistas de tiempo completo, la investigación adopta un enfoque inclusivo que resulta pertinente para cualquier actor en riesgo de convertirse en objetivo por hacer periodismo. Sin duda, muchos aspectos tratados son también de relevancia directa para defensores de los derechos humanos en general, para personas que representan fuentes periodísticas e incluso para actores que simplemente hacen uso personal de las comunicaciones digitales.

La investigación muestra también que la seguridad digital es una cuestión que no distingue entre sexos, y que esto debería tenerse en cuenta en la capacitación en seguridad digital. Propone que ésta debería incluir no sólo conocimientos prácticos y recursos digitales, sino cubrir también aspectos normativos, psicosociales y físicos.

Entre los consejos útiles proporcionados en este estudio está la sugerencia de que los profesionales desarrollen una evaluación de riesgos o "modelo de amenazas". Esto puede servir como base para un plan de seguridad personal que cubra la seguridad tanto digital como física. A su vez, ello puede contribuir para que los individuos tomen decisiones bien fundamentadas en torno a sus tiempos libres y sus recursos, siempre con plena conciencia de su seguridad.

Dado el rápido desarrollo tecnológico, esta publicación supone un documento puntual sobre importantes desafíos y recomendaciones actuales, y sus puntos de vista tendrán que ser revisados y actualizados con el paso del tiempo. No obstante, el principio se mantiene: el periodismo merece ser apreciado y protegido, independientemente de su interfaz tecnológica.

El enfoque de la UNESCO expuesto en el Plan de Acción de las Naciones Unidas para la Seguridad de los Periodistas y la Cuestión de la Impunidad es que la protección del periodismo necesita el apoyo de muchos otros actores. Por encima de todo está la audiencia. En particular, y como propone esta publicación, el periodismo necesita un público familiarizado con los medios de comunicación y la información, así como con las cambiantes dimensiones digitales. Son esta clase de competencias las que pueden garantizar que los ciudadanos se empoderen regularmente para valorar y ayudar a defender al periodismo frente a sus adversarios.

Getachew Engida
Director General Adjunto de la UNESCO

Resumen ejecutivo

En paralelo a la creciente digitalización del periodismo, que aporta beneficios sin precedentes tanto a los periodistas como a las audiencias, han surgido amenazas preocupantes.

Las comunicaciones electrónicas de los medios informativos, los blogueros críticos y otros individuos u organizaciones que difunden información se han convertido en objetivo. El peligro emana de diversas fuentes, desde actores estatales a terceros. Existe una vigilancia digital que trasciende los estándares internacionales sobre privacidad y libertad de expresión. Existe *hacking* de datos y ataques perturbadores a sitios web y sistemas informáticos. De forma más extrema, algunos agentes de los medios de comunicación están siendo asesinados por su periodismo en la red. Entre 2011 y 2013, 37 de los 276 asesinatos de periodistas condenados por la Directora General de la UNESCO fueron periodistas cuyas principales plataformas estaban basadas en Internet.[2] Muchos, si no la mayoría, de los demás periodistas asesinados utilizaban también herramientas digitales en su labor cotidiana, lo que puede haberlos expuesto de diversas formas.

Algunos riesgos de seguridad simplemente se han trasladado del ámbito offline al ámbito online. Las amenazas de muerte ahora se envían por correo electrónico y pueden responder a contenidos publicados en Internet más que en periódicos impresos o en radiodifusoras. Una oficina de medios de comunicación o una imprenta todavía pueden ser objeto de una bomba, pero actualmente es más común la negación de servicios para echar abajo el sitio web de un medio de comunicación. Sin embargo, otras amenazas adoptan una nueva dimensión en su forma digital. A medida que se generan, almacenan, transmiten y buscan más datos, pueden intensificarse viejas amenazas como el acoso sexual. También surgen cuestiones relacionadas con la privacidad y la libertad de expresión. Por ejemplo, exponer los movimientos de periodistas a través de datos de geolocalización vinculados a teléfonos celulares, hacer visible su vida privada en medios sociales y extraer metadatos de sus comunicaciones.

Los peligros identificados en esta publicación cubren al menos 12 amenazas digitales, incluyendo vigilancia digital ilegal o arbitraria, rastreo de localizaciones, y *exploits* de *software* y *hardware* sin conocimiento del individuo objetivo. Algunos ejemplos adicionales que se consideran son: *phishing*, ataques de dominios falsos, ataques de intermediario o *man-in-the-middle* (MitM) y ataques de denegación de servicio (DoS).

También se incluyen ejemplos que muestran cómo los periodistas necesitan protección frente amenazas como la alteración de sitios web, cuentas de usuario comprometidas, confiscación o robo de sus recursos digitales; intimidación, desinformación y campañas de difamación online. Al mismo tiempo, se reconoce que la seguridad digital experimenta cambios constantes, y que también es cada vez más barata para quienes desean organizar ataques digitales.

Estas claves resultan valiosas para legisladores, organizaciones de la sociedad civil, empresas de medios de comunicación y una variedad de actores periodísticos, ofreciéndoles un mejor entendimiento sobre los nuevos desafíos para la seguridad del pe-

riodismo. Esta publicación aporta también una visión general de los actores e iniciativas que trabajan para abordar la seguridad digital, al tiempo que identifica lagunas en el conocimiento que requieren de una concientización.

Los riesgos de seguridad digital son analizados en su dimensión tecnológica, institucional, económica, política, legal y psicológica. Por ende, se proponen recomendaciones en cada una de estas categorías para las partes interesadas, las cuales cubren aspectos como el comportamiento digital de los profesionales, el desarrollo de capacidades para la seguridad digital, los servicios de experiencia digital y las medidas que son necesarias por parte de las empresas de medios de comunicación. Las recomendaciones apuntan también a la continua necesidad de datos e investigación. También se subraya la necesidad de promover mecanismos a nivel nacional para proteger a los periodistas de todas las amenazas, y concientizar sobre las normas en constante desarrollo del sistema de las Naciones Unidas, así como su relevancia para la práctica segura del periodismo.

Hay argumentos válidos para un enfoque de múltiples grupos de interés para proteger a los periodistas de forma más amplia, incluyendo las dimensiones digitales. Con la cooperación de actores relevantes, pueden garantizarse los derechos a la libre expresión y la libertad de prensa; incluso en sus interconexiones con Internet. De esta forma, el flujo sin restricciones de información periodística puede seguir contribuyendo a la sociedad y garantizar más ampliamente que las ventajas de Internet no se vean eclipsadas por sus riesgos.

1. INTRODUCCIÓN

Este capítulo presenta al periodismo y su evolución, y procura identificar la variedad de los actores de los medios de comunicación online que hacen periodismo. A medida que el periodismo se introduzca en el espacio digital, seguirá beneficiándose del mayor acceso a la información, mayores públicos y de las herramientas de publicación que ofrecen las nuevas tecnologías. Al mismo tiempo, existen nuevas amenazas.

El periodismo informa y educa a su público. Sirve a un interés social pues persigue la transparencia. Quienes se dedican a él, con frecuencia actúan como observadores, escudriñando la formulación de políticas públicas y haciendo énfasis en los diversos obstáculos que se oponen al desarrollo: la corrupción, los abusos a los derechos humanos o una ineficiente gobernanza. Esto tiene un papel fundamental para hacer realidad los derechos democráticos y el desarrollo de las sociedades. Muchos investigadores coinciden en que el periodismo proporciona a los ciudadanos la información que necesitan para ser libres y autónomos.[3] Estudios realizados por Pippa Norris han mostrado una correlación estadística entre medios de comunicación libres y la materialización de la democracia y el desarrollo.[4] En un estudio publicado por el Instituto del Banco Mundial, Joseph Stiglitz y otros autores demuestran más extensamente que la información precisa y oportuna da como resultado una mejor y más eficiente asignación de recursos, llegando a la conclusión de que unos medios de comunicación libres y críticos desempeñan un papel crucial para el desarrollo.[5] Estos aspectos se han vuelto cada vez de mayor actualidad a medida que las Naciones Unidas implementan la nueva Agenda de Desarrollo Sostenible.[6]

El periodismo se desenvuelve a través de la interacción humana, aunque a menudo es generado, procesado y difundido a través de medios electrónicos; sobre todo digitales. En el entorno multimedia global de hoy en día, el periodismo puede desempeñarse en una multimillonaria sala de prensa o desde un dormitorio. Dondequiera que tenga lugar, el periodismo a menudo implica un enorme riesgo para quienes lo producen y para sus fuentes, sobre todo allí donde la información desafía al poder o revela información que otros actores procuran ocultar.

Quienes se dedican al periodismo pueden ser blanco de ataques debido al importante papel que desempeñan; es a causa de este papel que también merecen protección. Necesitan estar seguros, ser libres y tener la oportunidad de expresar opiniones e información, monitorear y arrojar luz sobre operaciones gubernamentales y corporativas, y fomentar la rendición de cuentas.[7] No deberían tener que trabajar con temor a dar voz a quienes no la tienen, o de inquietar a quienes se sienten cómodos.

Las innovaciones tecnológicas han hecho más fácil que nunca dedicarse a la recopilación de noticias y la difusión de contenidos. Tan sólo a fines de 2013, casi 40% del mundo estaba online (aunque esta conectividad era considerablemente superior en el mundo desarrollado) y había 96 suscripciones a telefonía celular móvil por cada 100 personas.8 Hoy en día, cualquiera que produzca periodismo puede enfrentar riesgos. Las preocupaciones sobre seguridad digital y seguridad operativa aumentarán en importancia a medida que se diluyan cada vez más las distinciones entre actividad online y offline.

1.1 Definiciones, ámbito y objetivo de la investigación: identificar la amplia variedad de actores y la evolución del periodismo

Todos los actores de los medios de comunicación, idependientemente de las plataformas que utilicen, tienen derecho a disfrutar de la libertad de expresión, así como el derecho a ejercer esta libertad de forma segura. La sociedad tiene un interés particular en proteger a quienes producen periodismo. La interconexión que propician el Internet y las tecnologías móviles ha permitido a ciudadanos comunes participar en el periodismo: ya sea documentando eventos locales, investigando y analizando sucesos distantes y difundiendo noticias y opiniones emandas de diversas partes del mundo. En ciertas situaciones donde los periodistas de agencias de medios de comunicación tienen acceso limitado a la información o a las fuentes (debido a desastres naturales, crisis humanitarias o políticas), el reporte ciudadano resulta especialmente valioso pues proporciona información crucial para los diversos miembros de las comunidades locales e internacionales. En lugar de la era de una prensa exclusiva, hoy en día la recopilación y difusión de noticias a menudo se distribuye a través de diversos actores y plataformas, incluyendo las redes sociales.

Aquellos actores profesionales que actualmente publican online se ven cada vez más complementados por nuevos colaboradores que contribuyen de forma significativa a la transmisión de la información y la formación de la opinión pública. Además, gran parte del periodismo online se ha vuelto interactivo, lo que implica discusiones entre las propias audiencias, así como entre el público y los agentes periodísticos, diluyéndose las distinciones entre ambos en muchos casos. El reporte de fuentes abiertas –o colaboración entre reporteros, fuentes y lectores– supone un fenómeno en desarrollo.[9]

Esta proliferación de voces sobre temas relevantes ha incrementado las oportunidades de los medios de comunicación para fomentar una sociedad civil global, y ha permitido una cobertura más amplia de temas de interés para el público general, así como para ciertas minorías que a menudo no tienen acceso a los medios de comunicación.[10] También ha fortalecido el reporte de eventos en tiempo real. Además, cuando los ciudadanos dan testimonio o comentan a través de medios digitales como blogs, tuits o comentarios a través de SMS que se transmiten en los cintillos de las pantallas de televisión, surgen preguntas sobre la identidad y la condición periodística.

¿Quién es periodista?

El debate sobre quién es y quién no es periodista tiene mucha vigencia. La cuestión principal se centra en si individuos que recopilan información y difunden dicho contenido son periodistas. Muchos definen al periodismo no a partir de la plataforma o la condición formal del periodista, sino mediante lo que implica su práctica: la generación y circulación de informaciones y opiniones relevantes para el interés del público. Según Oktavía Jónsdóttir, Directora de Programas de la Iniciativa “Garantizar el Acceso a la Libertad de Expresión” (SAFE, por sus siglas en inglés) de la Junta Internacional de Investigación e Intercambios (IREX): “No se trata de dónde realizas tu labor, sino del hecho de que te dedicas a la recopilación de noticias”.[11] Este enfoque es similar al del Consejo de Europa en su Recomendación No. R (2000)7: “El término ‘periodista’ significa cualquier persona natural o jurídica que se dedique regular o profesionalmente a la recopilación y difusión de información para el público mediante cualquier medio de comunicación masiva”. Esta postura se asemeja a la del Comité de Derechos Humanos de las Naciones Unidas, que en 2011 definió a los periodistas en su comentario general No. 34 como “una amplia variedad de personas, como analistas y reporteros profesionales y de dedicación exclusiva, autores de blogs y otros que publican por su propia cuenta en medios de prensa, en Internet o por otros medios” (párrafo 44).

Hoy en día, esta definición abarca a muchos individuos que se consideran periodistas y sin embargo no son empleados de los medios informativos tradicionales. Muchos son

blogueros y fotógrafos que generan y publican artículos online. Algunos se dedican al periodismo en su tiempo libre además de a otros empleos y no necesariamente son remunerados monetariamente por esta actividad. Además, existen otros colaboradores que no se ven a sí mismos como periodistas, pero que, al hacer uso de la tecnología digital, contribuyen también como testigos, verificadores de información, comentaristas e incluso reporteros.

Esta perspectiva tecnológicamente neutral está implícita en el punto de vista del ex Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue:

> Los periodistas son individuos que observan y describen eventos, documentan y analizan eventos, declaraciones, políticas y cualquier proposición que pueda afectar a la sociedad, con el propósito de sistematizar dicha información y recopilar [...] hechos y análisis para informar a sectores de la sociedad o a la sociedad en su conjunto.[12]

Para fines de este reporte, se reconoce que, independientemente de la tecnología, no todos los actores de medios de comunicación que producen o contribuyen de forma "sistematizada" al periodismo lo hacen en la misma medida que aquellos individuos que se dedican a actividades de recopilación de noticias como empleo profesional. No todos los que hacen periodismo o contribuyen a él son periodistas. Sin embargo, la seguridad digital es sin duda relevante para todos.

Esta concepción inclusiva se corresponde con el Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad, que establece que "la protección de los periodistas no debiera limitarse a los que están reconocidos formalmente como tales, sino que debería comprender a otros, incluidos los trabajadores de los medios de comunicación comunitarios, los periodistas ciudadanos y otras personas que puedan estar empleando los nuevos medios de comunicación como instrumento para llegar a su público".[13]

Dicha perspectiva está en consonancia con los documentos aceptados por la UNESCO que se refieren a "periodistas, trabajadores de medios de comunicación y productores de medios sociales que generan una importante cantidad de periodismo de interés público".[14] Es esta perspectiva la que define por tanto la presente investigación. Y debido a que casi todas las personas involucradas en el periodismo hoy en día utilizan Internet y las telecomunicaciones en una u otra medida, aunque su producción se publique o transmita offline, la seguridad digital es un tema de relevancia general.

1.2 Examinar los desafíos y riesgos digitales que enfrentan los periodistas y otros agentes que contribuyen al periodismo

Internet es una vía para compartir información y un espacio de reunión virtual donde los individuos pueden proporcionar datos y opiniones diversas, debatir cuestiones clave y asociarse entre sí. Ofrece la oportunidad para que las personas hagan realidad el derecho a la libertad de expresión y asociación como en ninguna otra época de la historia. La recopilación de noticias y la difusión de información pueden a menudo solaparse con las redes sociales, así como con los blogs y las comunicaciones de telefonía celular. Dichas actividades pueden realizarse tanto por periodistas profesionales como por ciudadanos inexpertos que, sin embargo, producen contenidos periodísticos. Estos últimos se erigen como fuentes de información cada vez más vitales, a medida que nuevas plataformas y herramientas les permiten producir contenido de una forma sin precedentes, además de la posibilidad de implicarse en la producción de un periodismo más tradicional en una variedad de plataformas.

A medida que más actores participan en el periodismo y contribuyen a informar a la opinión pública, se convierten también en sujetos de interés para actores que quieren controlar el flujo de información. Según un informe sobre la seguridad de los periodistas realizado por el Alto Comisionado de las Naciones Unidas para los Derechos Humanos en julio de 2013: "Conforme ha aumentado el número de periodistas online, también lo han hecho los ataques en su contra, como el *hacking* ilegal de sus cuentas, monitoreo de sus actividades online, arresto y detención arbitrarias, y el bloqueo de sitios web que contienen información crítica sobre las autoridades".[15]

Según el representante para África Oriental del Comité para la Protección de los Periodistas, Tom Rhodes:

> El nivel de amenazas contra la prensa aumenta cada año […] a medida que las autoridades gubernamentales –entre otros actores– dirigen su mirada más estrechamente al impacto de los medios de comunicación online. Aparte de recibir amenazas online, muchos son localizados mediante redes de telefonía celular y amenazados adicionalmente a través de sus líneas telefónicas. También tenemos casos de periodistas/comentaristas online que son asesinados. Se está volviendo igual de peligroso, si no es que más (dado el impacto de los medios online), el trabajo de los periodistas que trabajan para medios de comunicación en la red que para los que lo hacen para otros medios como la prensa y la radio.[16]

La seguridad de los periodistas, conceptualizada de manera inclusiva, ha cobrado protagonismo en la escena global en los últimos años, encabezada por organizaciones internacionales para la libertad de prensa y organismos de las Naciones Unidas como la UNESCO, el Consejo de Derechos Humanos, el Alto Comisionado para los Derechos Humanos, la Asamblea General de las Naciones Unidas y el Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión. En 2012, el Plan de Acción de las Naciones Unidas para la Seguridad de los Periodistas y la Cuestión de la Impunidad fue suscrito por la Junta de Jefes Ejecutivos del Sistema de las Naciones Unidas con el objetivo de "obrar en favor del establecimiento de un entorno libre y seguro para los periodistas y los trabajadores de los medios de comunicación, tanto en situaciones de conflicto como en otras, a fin de fortalecer la paz, la democracia y el desarrollo en todo el mundo".[17] El Plan establece un marco para llevar a cabo acciones a nivel nacional e internacional para múltiples grupos de interés con el fin de garantizar la seguridad del periodismo. En 2013, la propia Asamblea General de las Naciones Unidas acogió dicho Plan. Para este estudio, se utiliza la conceptualización sobre seguridad de dicho Plan, la cual designa:

> Una amplia categoría que engloba desde medidas preventivas y protectoras hasta combatir la impunidad y promover una cultura social que

> aprecie la libertad de expresión y la libertad de prensa. […] La seguridad abarca el ámbito tanto online como offline, y […] las soluciones requieren de acciones informadas a nivel global, nacional y local, al tiempo que se responde a especificidades contextuales en cada caso.[18]

Los periodistas y otros actores que hacen periodismo con tecnologías digitales enfrentan una variedad de desafíos y riesgos digitales, que a veces contribuyen al entorno hostil al que se enfrentan en el mundo físico. Según el Comité para la Protección de los Periodistas (CPJ), 44% de los 70 periodistas registrados como asesinados en 2013 trabajaban para plataformas de medios online.[19] Asimismo, del total de periodistas que el CPJ registró como encarcelados en 2013, la mitad de ellos, 106, eran periodistas online.[20] Sin embargo, no sólo quienes publican online enfrentan riesgos. Éstos se aplican a todos los actores cuyas actividades periodísticas interactúan con tecnología electrónica, ya sea mediante el uso de computadoras para procesar información, de la utilización de telecomunicaciones o Internet para la recopilación y la investigación de noticias, o simplemente por el uso del correo electrónico para establecer comunicación. Por ende, este estudio se interesa en las amenazas que enfrentan todos los individuos cuyo uso de comunicaciones digitales para el periodismo puede exponerlos a riesgos definidos. Éstos son elaborados en el Capítulo 2.

Por varias razones, resulta difícil investigar los ataques y las amenazas que enfrentan quienes hacen periodismo digital.

En primer lugar, los ataques digitales a menudo son difíciles de identificar sin un alto nivel de experiencia. Aunque algunas organizaciones de noticias pueden contar con recursos a su disposición –incluyendo administradores de sistemas muy versados en amenazas digitales–, muchos blogueros independientes, trabajadores autónomos o periodistas ciudadanos a menudo no tienen esta experiencia o incluso acceso a semejante asistencia por parte de expertos.

En segundo lugar, las agencias de noticias y periodistas a menudo no saben o no comparten que han sido víctimas de ataques digitales. Existen diversas razones para ello. Algunos podrían estar preocupados de que revelar esta información pueda producir un mayor acoso. También porque, al reverlar que han sido objeto de amenazas, sus fuentes pueden ser reticentes a establecer contacto, quizá porque consideran que no son capaces de mantener la confidencialidad sobre información sensible.

En tercer lugar, resulta difícil señalar directamente qué entidad o entidades están vigilando o interviniendo comunicaciones electrónicas. Un especialista en seguridad digital podría ser capaz de descubrir el nombre de la empresa que creó el *software* de vigilancia, pero es más difícil determinar quién ordenó o desplegó el ataque. Lo mismo se aplica a ataques que perturban visiblemente las comunicaciones, como la alteración de sitios web o la implantación de *malware*. Diversos observadores creen que muchos de los ejemplos que conforman este estudio son causados por actores específicos, pero no es posible probar esto de forma contundente. Por ello, este estudio se concentra más en el tipo de ataques reportados y no suscribe ninguna suposición sobre la identidad de los perpetradores. La tarea importante es identificar las clases de amenazas y la protección adecuada para aquellos que se encuentran en peligro.

Por último, las organizaciones de derechos humanos –que buscan proteger y ampliar los derechos digitales de los usuarios en riesgo en todo el mundo– pueden no contar con datos sobre periodistas y otros actores online cuyo derecho a la libre expresión y a la privacidad ha sido violado en un entorno digital. Incluso cuando los tienen, no siempre cuentan con recursos suficientes para analizar y hacer anónimos los datos, de modo que puedan compartirse de manera segura. [21]

Con el fin de entender mejor y evaluar las amenazas al periodismo con respecto a su interacción con la tecnología digital, es necesario desmenuzar estos desafíos.

1.3 Mapeando las actividades referentes a la seguridad digital

Diversas partes interesadas, incluyendo comisiones, agencias de noticias, organizaciones gubernamentales y no gubernamentales, tecnólogos y periodistas, se han vuelto más conscientes de las dimensiones digitales de la seguridad periodística y están dando pasos para mitigarlas. A través de diversos compromisos, iniciativas, cursos de capacitación, reuniones y materiales, pueden mapearse áreas de ejercicio de acuerdo con las siguientes categorías:

- Labor normativa y concientización,
- Guías de capacitación y cursos de capacitación en seguridad digital,
- Líneas directas y asistencia en seguridad, y
- Reportes e investigación.

La siguiente sección ofrecerá un resumen de estos temas y de sus desafíos. En el Capítulo 2 de este informe se presenta un análisis a profundidad de algunos de los actores y sus acciones concretas dirigidas a enfrentar dichos desafíos. El tercer capítulo ofrece recomendaciones para abordar los problemas en las cuatro áreas de ejercicio identificadas.

Labor normativa y concientización

La concientización es una forma de sensibilizar a todos los actores sobre la seguridad integral para el periodismo, así como para promover la norma social de que esta clase especial de comunicación pública debería disfrutar de seguridad y protección, en particular con respecto a su interacción con tecnologías digitales.

Fomentar una amplia concientización es una actividad común entre los principales grupos de interés implicados en promover la protección y seguridad del periodismo. En este sentido, las organizaciones de libertad de prensa envían cartas a funcionarios de alto nivel, apelando para que investiguen delitos –incluyendo delitos digitales– contra periodistas. Los organismos intergubernamentales también trabajan con sus socios para garantizar que la seguridad de los periodistas sea una prioridad en la agenda internacional.

Las reuniones de coordinación de esfuerzos para mejorar la seguridad de los periodistas son a menudo encabezadas por la UNESCO en contextos tanto globales como locales. Estas reuniones normalmente incluyen a agencias de las Naciones Unidas, representantes de gobiernos, organizaciones no gubernamentales (ONG), agencias de medios de comunicación, asociaciones de periodistas, periodistas y académicos, e incorporan líneas de acción específicas sobre seguridad digital y derechos online. El tema de la protección de periodistas también se ha abordado en foros internacionales sobre derechos humanos como el Consejo de las Naciones Unidas para los Derechos Humanos. Hoy en día, hay cada vez más especialistas en tecnología que se unen con las organizaciones de derechos humanos y de protección a la prensa para ayudar a los periodistas y a otros a conocer las mejores prácticas de seguridad digital, eludir la censura, limitar su vulnerabilidad a la vigilancia y proteger mejor sus fuentes.

Sin embargo, hay una conciencia muy limitada de estas acciones entre muchos profesionales. Además, el uso y la práctica a nivel popular de dichos estándares normativos para impulsar apoyos y cambios de políticas –incluso en el ámbito digital– es insuficiente o limitada. Por otra parte, la dimensión de género no siempre es suficientemente valorada.

Guías de seguridad digital

El medio está inundado de guías de seguridad digital, en formatos que van desde aplicaciones para celular, hasta videos, animaciones y textos. Aunque resulta útil tener nuevas guías en este ámbito, la proliferación y los consejos (a veces contradictorios) pueden generar confusión. En conjunto, las guías son también limitadas en términos del número de idiomas abarcados y pueden rápidamente volverse obsoletas.

Capacitación en seguridad digital

Los programas de capacitación en seguridad digital para defensores de los derechos humanos y periodistas están en aumento. Sin embargo, aproximadamente 54% de los 167 participantes en la encuesta realizada para este informe respondieron que no habían recibido capacitación en seguridad digital.

Otras organizaciones también han registrado esta falta de capacitación en sus estudios. Un informe patrocinado por el Centro Internews de Innovación y Aprendizaje y realizado por la ONG pakistaní Bytes for All reporta que, de 37 periodistas y 15 blogueros entrevistados de aquel país, tres cuartas partes tenían poca noción de los riesgos de seguridad que podrían enfrentar, incluyendo la interceptación de correos electrónicos o el robo de datos. Muchos entrevistados tampoco conocían estrategias y herramientas para protegerse en la red.[22]

Según Andrew Ford Lyons, productor digital del Fondo Rory Peck, una ONG con sede en Londres que proporciona recursos y apoyo a periodistas autónomos, los periodistas autónomos tienen un nivel particularmente bajo de concientización sobre cómo utilizar de manera segura teléfonos celulares y vía satélite, archivar reportajes e implementar con éxito una encriptación.

Allí donde se da, la capacitación en seguridad digital se enfrenta a varios desafíos, incluyendo una falta de:

- Entendimiento entre organismos donantes y clientes sobre lo que puede lograr un capacitador en seguridad digital en el tiempo asignado;
- Lineamientos de cuidado personal para capacitadores en seguridad digital, ya que pueden ser susceptibles de agotamiento y fatiga emocional; y
- Permanencia, ya que las prácticas y tecnologías que pueden recomendarse como seguras en un momento determinado se vuelven superfluas u obsoletas con el tiempo.

Otro problema que algunos capacitadores en seguridad digital y responsables de programas han observado es que, aunque el periodista o defensor de derechos humanos confiaba en ellos individualmente, esa relación de confianza no comprendía a la organización del capacitador.[23] Esta falta de confianza en ocasiones conduce a que el periodista no solicite la ayuda técnica en seguridad digital.

Líneas directas y ayuda técnica en seguridad

Desde hace varios años, muchas ONG proporcionan ayuda técnica en seguridad a periodistas. Gran parte de esta ayuda se ha centrado en medidas de protección física, como equipos de seguridad para periodistas que cubren áreas en conflicto; seguros, asistencia financiera para traslados y otras disposiciones. En años más recientes, algunas organizaciones han trabajado con periodistas y agencias de noticias, así como con blogueros y otros, dentro de contextos nacionales y con el fin de proporcionar experiencia y capacitación en seguridad digital. Otros han actuado como intermediarios entre periodistas y especialistas en tecnología, conectándolos cuando hay una necesidad de seguridad digital. Los desafíos son los recursos y los conocimientos limitados de dichas habilidades por parte de periodistas bajo presión.

Reportes e investigación

Los reportes y la investigación por parte de las organizaciones de protección a la prensa, las instituciones académicas y las organizaciones internacionales de derechos humanos ayudan a arrojar luz sobre los tipos de ataques que enfrentan los periodistas y los activistas. En los últimos tiempos, este tipo de investigación ha incluido amenazas y ataques digitales como la vigilancia y el *malware* dirigido. Organizaciones dedicadas a la investigación interdisciplinaria como Citizen Lab, con sede en Toronto, Canadá, investigan ataques online contra la sociedad civil y los periodistas. El desafío es mantener y ampliar esta clase de investigación sobre las amenazas y los ataques digitales, los cuales probablemente se incrementan en la medida en que se elevan también los niveles de conectividad a Internet, la capacidad de almacenamiento de datos y la asequibilidad del costo de las tecnologías de vigilancia.

1.4 Desafíos específicos para diversas partes interesadas

Los actores que hacen periodismo en un contexto digital enfrentan numerosos y complejos desafíos, incluyendo los tecnológicos, institucionales, económicos, políticos, legales y psicosociales.

Desafíos tecnológicos, institucionales y económicos que afectan a periodistas y agencias de noticias

- La vigilancia, la capacidad de almacenamiento de datos y la tecnología para implementar ataques digitales se están volviendo menos caras y más generalizadas.
- Las herramientas de seguridad digital no siempre son fáciles de usar, lo cual conduce a que muy pocos periodistas implementen las herramientas correctamente o lo hagan en absoluto.
- Las herramientas de seguridad digital disponibles comercialmente pueden ser demasiado caras para ser adquiridas por trabajadores autónomos o blogueros, y muchas herramientas (gratuitas o no) no son fáciles de usar para los no especialistas.
- Las herramientas de seguridad digital de fuente abierta a menudo carecen de un modelo de negocio sostenible, lo que significa que pueden volverse obsoletas tras un corto periodo o pueden no actualizarse para resolver sus vulnerabilidades.
- Los ataques de denegación de servicio pueden dar como resultado una pérdida financiera para las agencias de noticias o los periodistas.
- Muchos periodistas y sus fuentes ignoran que diversos especialistas en tecnología están dispuestos a ayudarles si sufren una amenaza o ataque digital o que haya sido transmitido digitalmente.
- Muchos periodistas y sus fuentes no conocen el proceso de anonimización de datos o ni el uso de tecnologías seguras como la encriptación.
- Hay una falta de datos disponibles públicamente que documenten los tipos de ataques y amenazas digitales que enfrentan quienes hacen periodismo.
- Agentes estatales y no estatales pueden utilizar tecnología de rastreo de localizaciones para identificar a trabajadores de medios de comunicación –y a sus fuentes–, quienes a menudo necesitan confidencialidad para la producción de periodismo.

- La seguridad digital, tanto de quienes hacen periodismo como de sus asociados (fuentes, familias, colegas), a menudo puede comprometerse fácilmente mediante campañas de *phishing*. Las cuentas de usuario y dispositivos comprometidos pueden utilizarse para identificar a las fuentes y redes de quienes hacen periodismo, llevando a una mayor inseguridad.

- La capacitación sobre seguridad digital a menudo se imparte según su urgencia, si es que se llega a impartir, en lugar de ser sistemática e integral.

Desafíos políticos y/o legales que afectan a gobiernos nacionales, agencias de las Naciones Unidas y organizaciones intergubernamentales, ONG y corporaciones

- Los controles sobre el periodismo a veces se ocultan en las leyes sobre protección de datos, mientras que otras leyes son interpretadas de forma que pueden llevar al arresto o detención de periodistas por recibir, obtener o difundir información por medios digitales.

- La falta de voluntad política para abordar los delitos contra el periodismo, incluyendo delitos digitales, lo que da como resultado un clima de impunidad para los perpetradores.

- Las sanciones pueden dar lugar a una limitada disponibilidad de tecnología o actualizaciones de *software*, necesarias para que, quienes hacen periodismo digital, se mantengan seguros. Por su parte, la falta de sanciones puede dar como resultado una exposición a amenazas más potentes como consecuencia del comercio no regulado de *exploits* de *software* y tecnologías avanzadas para vigilancia y ciberataques.

Desafíos psicosociales que afectan a periodistas, agencias de noticias, escuelas de periodismo y otras instituciones educativas y de capacitación, y asociaciones de periodistas

- Un bajo nivel de valoración y entendimiento de los principios y herramientas de seguridad digital.

- La falta de decisión entre periodistas y otros actores de medios de comunicación puede dar lugar a una deficiente aplicación de las herramientas de seguridad digital o a su completa evitación.

- La capacitación en seguridad digital a menudo no está sistematizada o no es integral (por ejemplo, puede que excluya la seguridad operativa y la atención psicosocial).

- Las experiencias traumáticas previas pueden dar como resultado que los periodistas tomen decisiones equivocadas que lleven a una mayor inseguridad.

- La familia y los amigos pueden comprometer sin querer la seguridad digital de quienes hacen periodismo a través de revelaciones involuntarias en medios sociales.

- La naturaleza transversal y diversa de los desafíos que enfrenta el periodismo en un contexto digital tiene relevancia específica para una amplia variedad de partes interesadas. En el Capítulo 3 se ofrecen recomendaciones específicas para ellos.

2. RESUMEN GLOBAL: DESAFÍOS, PARTES INTERESADAS Y PRÁCTICAS

2.1 Introducción

En todo el mundo, el panorama de las amenazas digitales se ha ampliado y vuelto más complejo. Las amenazas a la seguridad online, como el *phishing*, el *malware* y el ciberespionaje, han aumentado y evolucionado en los últimos años, se han descubierto graves vulnerabilidades de *software* como Heartbleed y Shellshock, y las amenazas tradicionales han encontrado nuevas formas de provocar daños, incluso a través de redes sociales y dispositivos móviles.[24] Entretanto, la capacidad para recopilar, analizar y almacenar comunicaciones digitales se ha vuelto más sofisticada y asequible, mientras que el mercado de productos para tener la capacidad de intrusión ofensiva en redes de computación crece a un ritmo acelerado.[25]

Durante años, grupos de la sociedad civil a nivel global han considerado Internet y otros nuevos medios de comunicación como una poderosa herramienta para sus causas, pero recientemente han descubierto de qué forma los nuevos medios de comunicación pueden controlarse para limitar el acceso a la información y la libertad de expresión.[26] Según Ronald Deibert, de Citizen Lab, el ciberespacio se ha vuelto un entorno inseguro y utilizado peligrosamente como arma de guerra, donde los medios independientes pueden verse atrapados, acosados y explotados en la misma medida en que pueden verse empoderados.[27]

Organizaciones como Access, Citizen Lab, el Comité para la Protección de Periodistas, IFEX y Artículo 19 están documentando cada vez más ataques contra periodistas sufridos en el ámbito online, a menudo por parte de actores que buscan impulsar objetivos sociopolíticos. Estos ataques son llevados a cabo por adversarios de envergadura y con suficientes recursos.[28] Según los ingenieros de seguridad de Google, Shane Huntley y Morgan Marquis-Boire, 21 de las 25 agencias de noticias más importantes del mundo han sido objetivo de ataques de *hacking*, probablemente auspiciados por Estados.[29] "Si eres periodista o una agencia periodística, veremos cómo te conviertes en objetivo por parte del Estado. Esto sucede independientemente de la región; lo vemos en todas partes del mundo, tanto desde donde se encuentran los objetivos como desde donde proceden los objetivos", le aseguró Huntley a la agencia Reuters.[30] Según Marquis-Boire, el número de ataques no denunciados sobre agencias de medios de comunicación y periodistas fue significativamente superior al de los que se hicieron públicos.[31]

Estos ataques, así como otros, se producen a un alto costo para los periodistas y sus redes, así como para la libertad de expresión y asociación en términos más generales.[32] Este capítulo ilustra algunas de las diversas (y a menudo coexistentes) amenazas que enfrentan los actores de medios de comunicación en el entorno tecnológico actual:

- Vigilancia y vigilancia masiva;
- Exploits de *software* y *hardware* sin el conocimiento del individuo objetivo;
- Ataques de *phishing*;
- Ataques de dominios falsos;

- Ataques de intermediario o *man-in-the-middle* (MitM);
- Ataques de denegación de servicio (DoS) y DDoS, ataques distribuidos de denegación de servicio;
- Alteración de sitios web;
- Cuentas de usuario comprometidas;
- Intimidación, acoso y exposición forzada de redes online;
- Campañas de desinformación y difamación;
- Confiscación de productos de la labor periodística; y
- Almacenamiento y extracción de datos.

Limitaciones de la investigación

Este capítulo se centra en la seguridad de los periodistas y otros que contribuyen al periodismo, y no en cuestiones digitales que afectan a la libertad de expresión en sentido más amplio (apagones de comunicaciones, cuestiones de *copyright* online, denegación de capacidades de pago electrónico, filtrado o bloqueo de contenidos, notificaciones de eliminación de contenidos, etcétera). Aunque los investigadores intentan ofrecer un cuadro integral de las amenazas y los ataques digitales que enfrentan los actores periodísticos, no todos los tipos o casos están documentados. Es probable que salgan a la luz revelaciones de nuevas amenazas a la seguridad digital y de vigilancia después de que se publique este informe. No obstante, este capítulo proporciona un punto de partida para la discusión entre las principales partes interesadas que buscan salvaguardar a los periodistas y otros que generan una importante cantidad de periodismo de interés público.

2.2 Mapeo de desafíos y riesgos digitales que enfrentan los periodistas y otros que contribuyen al periodismo

Agentes estatales o no estatales pueden tratar de influir en el flujo o contenido de la información negando, dificultando, manipulando o monitoreando el acceso a una variedad de datos electrónicos. Los métodos cambian, debido a que los *exploits* y ataques se ven influidos por diversos factores, incluyendo el contexto económico, social y político donde se aplican los controles a la información.[33] El control de la información se ve también influido por los tipos de infraestructura de comunicaciones con que cuentan los países, como el número de Proveedores de Servicios de Internet (ISP), empresas de telecomunicaciones, el grado de competencia del mercado y el nivel general de penetración y crecimiento de Internet.[34]

Vigilancia y vigilancia masiva

La vigilancia, como el monitoreo, interceptación, recopilación, preservación y retención de información que ha sido generada, almacenada y transmitida a través de redes de comunicaciones, es una de las formas que buscan los actores para monitorear.[35] Las tecnologías de vigilancia son diversas: rastreo de localizaciones, inspección de paquetes en profundidad, reconocimiento facial y monitoreo masivo.[36] También existen métodos de interceptación masiva para mensajes de voz, SMS, MMS, e-mail, fax y comunicaciones telefónicas vía satélite.[37] La vigilancia puede producirse de forma masiva o estar dirigida a individuos. Aunque la vigilancia cuenta con muchos usos legítimos, cuando se recopila masivamente, sin una supervisión fiable por parte de un organismo independiente de monitoreo, puede menoscabar derechos humanos –incluyendo la libertad de expresión, la libertad de asociación y el derecho a la privacidad– y amenazar a la democracia. Esto está reconocido en una resolución del Consejo de Derechos Humanos adoptada en marzo de 2014, donde se registró una profunda preocupación "por el impacto negativo que la vigilancia y/o interceptación de comunicaciones, incluyendo la vigilancia y/o interceptación extraterritorial de comunicaciones, así como la recopilación de datos personales, en particular cuando se lleva a cabo a escala masiva, puede tener sobre el ejercicio y disfrute de los derechos humanos".[38]

Según el Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos publicado en junio de 2014,

> "Allí donde existe un propósito legítimo y se aplican las salvaguardas adecuadas, se podría permitir a un Estado dedicarse a una vigilancia bastante intrusiva; sin embargo, el Gobierno tiene la responsabilidad de demostrar que la interferencia es tanto necesaria como proporcional al riesgo específico que se está abordando. Los programas de vigilancia masiva pueden por consiguiente considerarse como arbitrarios, aunque sirvan a un propósito legítimo y hayan sido adoptados sobre la base de un régimen jurídico comprensible".[39]

La vigilancia masiva reduce la capacidad de funcionamiento de una prensa libre debido a que facilita la recopilación indiscriminada de información sobre las comunicaciones de todas las fuentes posibles.

Además, la vigilancia masiva a menudo se rige por leyes secretas y ambiguas, lo que puede sembrar confusión entre los periodistas y sus fuentes sobre qué tan estrechamente podrían ser monitoreados.[40] Esta falta de información hace más difícil que los periodistas y sus fuentes intenten protegerse a sí mismos y a sus fuentes de la vigilancia masiva. El periodismo depende de la disposición de las fuentes a hablar públicamente y confidencialmente; si la comunicación entre los periodistas y sus fuentes no puede mantenerse confidencial, entonces es posible que las fuentes dejen de hablar.[41]

La vigilancia masiva puede también dar lugar a un efecto disuasorio en la disposición de los escritores para investigar y publicar reportajes. Por ejemplo, en 2013, el Centro Americano PEN y el Grupo de Investigación Farkas Duffett realizaron un estudio para determinar qué impacto, si lo hubiere, había tenido la vigilancia gubernamental sobre los miembros del PEN.[42] El estudio reveló que:

- Los escritores del PEN actualmente suponen que sus comunicaciones son monitoreadas.
- La suposición de que están bajo vigilancia perjudica la libertad de expresión al obligar a los escritores a autocensurar su obra de múltiples formas, incluyendo la reticencia a:
    - Escribir o hablar sobre determinados temas;
    - Investigar sobre determinados temas; y
    - Comunicarse con fuentes, o con amistades en el extranjero, por miedo a poner en peligro a sus contrapartes al hacerlo.

En el contexto de la vigilancia masiva, no siempre existen disposiciones especiales que protejan las comunicaciones periodísticas de ser recopiladas o evaluadas. Además, si las comunicaciones periodísticas son recopiladas, rara vez existen protecciones frente a que sean utilizadas para fines jurídicos, a menos que sea absolutamente necesario y tras el debido procedimiento.[43]

Y, a medida que son recopilados y almacenados más contenidos y metadatos (o información generada cuando se utiliza tecnología), la imagen de un periodista y sus fuentes se vuelve más nítida. Según una reciente declaración por parte de varias ONG internacionales a la Oficina del Alto Comisionado para los Derechos Humanos:

> La histórica distinción entre los datos sobre las comunicaciones de un individuo y el contenido de sus comunicaciones se ha vuelto insignificante. A medida que los datos se vuelven cada vez más reveladores, sea de forma aislada o cuando se emparejan con otros datos, ya no resulta adecuado someter la información sobre sus comunicaciones a umbrales inferiores, o considerar su recopilación y procesamiento como una práctica menos invasiva que la interceptación de contenido. Los datos sobre las comunicaciones pueden actualmente revelar información igual de sensible que el contenido de las mismas, y deben disfrutar de igual protección conforme a la legislación sobre derechos humanos.[44]

En pocas palabras, sin considerar siquiera el contenido de las interacciones telefónicas o mediante correo electrónico entre un periodista y una fuente, analizando simplemente los metadatos sobre tiempo, lugar y frecuencia de las comunicaciones, es posible identificar a los actores implicados en una revelación periodística concreta.

Exploits de *software* y *hardware* sin conocimiento del individuo objetivo

La tecnología de vigilancia puede también utilizarse para infectar computadoras en todo el mundo con "implantes" de *malware* que permiten a entidades externas introducirse en redes informáticas específicas.[45] Las herramientas que permiten el acceso para monitoreo y vigilancia incluyen el *software* de intrusión y los troyanos, que operan como vectores de ataque. "Los vectores de ataque son como las ganzúas o duplicados de llaves para entrar en un edificio", afirma Seamus Tuohy, especialista del Instituto de Tecnología Abierta de la New America Foundation.[46]

En muchos países se han encontrado tecnologías de vigilancia desarrolladas por entidades comerciales y supuestamente se han utilizado como objetivo para determinados periodistas y activistas.[47] Citizen Lab ha registrado también tecnologías de vigilancia disponibles comercialmente que han sido vendidas a varios países.[48] El mercado de las tecnologías de vigilancia masiva y las capacidades de intrusión en redes está en auge. Las tecnologías de vigilancia que detectan un uso de Internet encriptado y encubierto son artículos muy demandados, como lo son las tecnologías que permiten a los usuarios analizar interceptaciones de web y telefonía celular en tiempo real.[49]

Algunas entidades pueden también convertir en objetivo de vigilancia a periodistas instalando un *bug* físico (o modificación de *hardware* en un enrutador de Internet) o un micrófono oculto en los dispositivos de comunicación o en el mismo cuerpo de un periodista. Esta vigilancia puede suceder tanto dentro de la casa de un periodista como a larga distancia a través de micrófonos de alta potencia. Un periodista podría ser objeto de un pinchazo telefónico para que el contenido de sus llamadas y comunicaciones de Internet pueda ser monitoreado en secreto por quienes desean ejercer un control. Para capturar los metadatos de las comunicaciones de periodistas también pueden utilizarse dispositivos de registro de llamadas (*pen registers*), que recolectan los números de teléfono marcados como llamadas salientes, y dispositivos de control y rastreo, que registran los números de las llamadas entrantes.[50]

Los periodistas pueden también ser objetivo de un "ataque de día cero": cuando un adversario explota la vulnerabilidad de un *software* o *hardware* en un momento en el que no hay conocimiento previo de dicha falla en la comunidad y, por tanto, no hay disponible ninguna solución o parche.[51] Esto se hace para acceder al dispositivo de un individuo con el fin de introducir *malware*. Una vez que un adversario tiene acceso a la computadora de alguien, él o ella pueden instalar *software* para monitorear las comunicaciones en ese dispositivo, tales como un registro de pulsaciones del teclado, acceso de manera remota a webcams/micrófonos, monitoreo de e-mails, extracción de archivos, etcétera. También permite al atacante evitar la encriptación. Esto es especialmente importante dado el aumento en el tráfico encriptado durante los últimos años.

En otras ocasiones, los periodistas pueden convertirse en objetivo mediante sus datos de localización. Según Oktavía Jónsdóttir, directora de programas de la Iniciativa SAFE de IREX, el geoetiquetado tiene un margen de error de 2 a 5 m si un teléfono está prendido (incluso en casos donde esté activada la configuración de privacidad y desactivada la configuración de localización) y de 50 m si un teléfono está apagado.[52] Un estudio de 2013 realizado por investigadores del Instituto de Tecnología de Massachusetts (MIT) de Estados Unidos y la Universidad Católica de Lovaina, Bélgica, muestra que los datos de localización revelan una importante cantidad de información sobre una persona, lo que da como resultado un bajo grado de anonimato.[53]

Para ayudar a proteger el contenido de las comunicaciones, los periodistas y sus fuentes tienen que considerar utilizar tecnologías de encriptación. Sin embargo, incluso la encriptación de contenido no es infalible para proteger a las fuentes. Se puede deducir mucha información a partir de los metadatos de intercambios. El uso de encriptación y otras tecnologías también puede de hecho señalar al periodista o la fuente como alguien de interés que tiene algo que ocultar. Sin duda, se ha reportado que el simple interés en proyectos de privacidad, anonimato y encriptación online desencadena un mayor rastreo y monitoreo en muchos casos.[54] En algunos países, los canales encriptados como las Redes Privadas Virtuales (VPN) son considerados ilegales, aunque no siempre se les aplica la ley de forma estricta. Dichas comunicaciones pueden ser almacenadas y posiblemente desencriptadas cuando hay interés en acceder a la información que contiene el mensaje encriptado. Aun así, la comunicación encriptada puede ayudar a "ganar tiempo", según afirma Eva Galperin de la Fundación Fronteras Electrónicas (EFF).[55]

No saber si tus comunicaciones, aunque encriptadas, son monitoreadas puede tener un efecto disuasorio sobre la labor periodística. Algunos periodistas suponen que están bajo vigilancia aunque no lo puedan probar. Sin embargo, esta creencia no necesariamente se correlaciona con el entendimiento de que sus prácticas de comunicación digital podrían haber facilitado dicha vigilancia.[56] En otros casos, los periodistas advierten que sus cuentas han sido comprometidas, pero no están seguros de cómo sucedió. Los periodistas y defensores de los derechos humanos a veces sólo tienen pruebas de que han sido monitoreados después de ser arrestados y de que sus registros de chats o e-mails son puestos a su alcance por autoridades gubernamentales.

Campañas de *phishing*

Los periodistas y las agencias de noticias pueden convertirse en objetivo de vigilancia mediante campañas de *phishing* o *spear phishing*. Estas campañas dirigidas a menudo utilizan links o archivos adjuntos cargados con *malware* que son enviados a través de e-mail o redes sociales.[57] Aunque el *malware* difiere en sus capacidades, una de las maneras más malévolas que se ha sabido que afecta la labor de los periodistas son los Troyanos de Acceso Remoto (RAT). Entre más sofisticado es un RAT, más probable es que evite la detección por parte de un antivirus. Si se hace clic sobre ellos o son descargados, estos RAT permiten al atacante recopilar cualquier cosa que quieran en la computadora comprometida.

"Si la computadora puede hacerlo por ti, ellos también pueden hacer que lo haga para ellos; o incluso que trabaje para sus necesidades, como desviar el tráfico para un ata-

que de intermediario", afirma Seamus Tuohy.[58] Otras veces, estos ataques adoptan la apariencia de un dominio (sitio web) falso. El sitio recopila sigilosamente información de cuentas que el periodista introduce, pensando que es legítimo. Un frecuente ataque de *phishing* es cuando un periodista recibe un e-mail que parece ser de alguien que conoce. Podría ser de una dirección de e-mail familiar o escrita como si procediera de un conocido. Esta correspondencia fraudulenta obliga entonces al destinatario a hacer clic en un link o un archivo adjunto que descarga *malware* en su computadora. Según Bill Marczak, investigador de Citizen Lab y estudiante de Doctorado en Informática de la Universidad de California, Berkeley, incluso los periodistas asistidos por los investigadores de Citizen Lab siguieron siendo objetivo reiteradamente mediante archivos adjuntos, a pesar de las advertencias de los investigadores de que abrieran los archivos adjuntos únicamente en la nube (tal como se ofrece a través de varios proveedores de servicios de correo web). Marczak cree que los daños podrían reducirse en 85% si los periodistas dejaran de abrir directamente archivos adjuntos.[59]

Las campañas de *phishing* y la consiguiente instalación de tecnología de vigilancia en el dispositivo de un periodista pueden:

- comprometer información personal, datos y fuentes de un periodista a menudo sin que el periodista mismo lo descubra;
- dar lugar a un chantaje por el mal uso de información personal; y
- llevar a una autocensura.

Ataques de dominios falsos

Según Access, una ONG internacional que defiende y amplía los derechos digitales de los usuarios en riesgo en todo el mundo, los ataques de dominios falsos generalmente encajan en dos categorías: 1) introducen *malware*, o, 2) proporcionan contenido falso que afecta la credibilidad de la agencia de noticias o el periodista.

En un ataque de *malware* de dominios falsos, el dominio falso copia el contenido existente del sitio web objetivo y suministra *malware* a los visitantes del sitio web falso. Los atacantes pueden ampliar su alcance de víctimas al crear cuentas en redes sociales que enlacen al sitio falso con el fin de incrementar el PageRank en Google del sitio falso y convertirse así en la primera opción tras la búsqueda del dominio.[60]

Con este tipo de ataques, se busca menoscabar la credibilidad del medio de comunicación en cuestión. Así, el ataque tiene como objetivo influir en la opinión pública, cambiar el escenario de protestas o evitar que se publique información novedosa.[61]

Los visitantes a menudo no saben que han sido víctimas de un *malware* "de paso" o que están leyendo contenido falso. Puede que accedan a un sitio a través de una URL abreviada, una URL extraída de redes sociales o a través del redireccionamiento de la empresa de telecomunicaciones privada o estatal que proporciona el acceso a Internet.[62]

Según Access, 4% de 60 casos reportados durante 10 meses fueron ataques de dominios falsos.[63] Para ayudar a la sociedad civil y a los periodistas a defenderse contra estos ataques, Access lanzó un *plug-in* para navegadores llamado Fake Domain Detectives (detectives de dominios falsos).[64]

Asimismo, se han reportado supuestos casos de proveedores de servicios de Internet que utilizan el redireccionamiento de DNS o el secuestro de DNS para dirigir a los usuarios a un dominio falso.[65] El redireccionamiento de DNS es cuando una dirección web es desplazada deliberadamente a una página falsa. En estos casos, los visitantes de los sitios de medios de comunicación independientes son redireccionados a versiones falsas de esos sitios.

Ataques de intermediario o *man-in-the-middle* (MitM)

Un MitM se produce cuando los atacantes se insertan ellos mismos, o su tecnología, entre un usuario y un sitio web. Durante un ataque MitM, el intermediario puede obtener sigilosamente información de ambas partes e incluso cambiar el contenido sin que el usuario o el administrador del sitio web lo sepan.

Una variante común de un ataque MitM consiste en un atacante utilizando un enrutador de WiFi para interceptar la comunicación con los usuarios. Un ejemplo es cuando un atacante configura un dispositivo inalámbrico de conexión WiFi y le da un nombre común, en un lugar público, para hacer creer a los individuos que se trata de una conexión legítima. Cuando los individuos se conectan a él y acceden a sitios como banca online o e-mail, sus credenciales son capturadas y almacenadas para su uso posterior.[66] En este sentido, los periodistas deberían interesarse por el propietario y la independencia de su ISP, ya que pueden ser objetivo de un ataque MitM incluso cuando no utilicen WiFi.

Una variante ligeramente novedosa de un ataque MitM implica atacar al navegador. Esto se produce cuando un atacante infiltra código *malware* en la máquina de una víctima que se ejecuta cuando se abre el navegador específico, registrando así los datos intercambiados entre el navegador y los sitios web objetivo que el atacante ha prefijado en el *malware*.[67]

Es importante saber que algunos individuos se dedican a realizar ataques MitM por diversas razones. Puede que quieran recopilar suficiente información para realizar futuras acciones fraudulentas, como falsificar información o transferir dinero a la cuenta del atacante. Otras veces, el atacante podría suministrar información falsa a una de las partes, o a ambas, para entorpecer las comunicaciones y deteriorar la confianza (o simplemente para espiar).[68]

Ataques de denegación de servicio (DoS)

Los ataques de denegación de servicio (DoS) es otra de las tácticas que se pueden utilizar para intimidar a los periodistas online y limitar su libertad de expresión. Un ataque DoS se produce cuando una computadora y una conexión a Internet se utilizan para saturar a un servidor con la intención de colapsar el sitio y hacerlo inaccesible para otros. Por otra parte, además de el ataque DoS, el periodismo puede ser presa de un ataque distribuido de denegación de servicio (DDoS), el cual utiliza varias computadoras y conexiones, a menudo distribuidas por todo el mundo, para atacar a una computadora. Similar a un ataque DoS, un ataque DDoS sobrecarga los sitios web y los deja inaccesibles.[69] Según Arbor Networks, una empresa de seguridad de Estados Unidos, y Akamai Technologies, una red de distribución de contenido para Internet de Estados Unidos, los ataques DDoS están en auge en todo el mundo.[70] El espectacular aumento –más de un 200%– fue observado en ataques DDoS de gran volumen,[71] ya que es más difícil para un servidor resistir un ataque DDoS que un ataque DoS.[72] Los expertos apuntan que el uso de ataques DDoS viene generalmente acompañado de intervenciones en la comunicación, alteraciones de sitios web y tácticas de amenaza offline.[73] Aunque el uso de este tipo de ataque puede estar generalizado, algunos expertos apuntan que los DDoS están siendo sustituidos por el *hacking* dirigido o la alteración de sitios web.[74]

Según Gustaf Björksten, Director de Tecnología de Access, 8% de los casos reportados en la Línea de Asistencia de Seguridad Digital 24/7/365 de Access Tech (60 casos en 10 meses) fueron casos de DDoS. Normalmente, los ataques DDoS están relacionados con una coyuntura específica; por ejemplo, se producen en sitios web de la oposición política y los medios independientes durante elecciones, o en sitios web de activistas y medios independientes durante protestas; ocasionalmente también se pueden producir como represalia por demostrar apoyo a alguna campaña que vaya en contra de los intereses del atacante.[75] Como Access, Google también ayuda a mitigar

los ataques DDoS. Su Project Shield proporciona apoyo para agencias de medios de comunicación a través de un programa llamado Deflect.

Los ataques DDoS resultan eficaces para aumentar la censura y es difícil atribuirlos a algún agente en particular. Por ello, los ataques DoS y DDoS suponen un importante problema para los medios online que hacen periodismo debido a que:

- evitan que determinada información sea difundida y visualizada, lo que da como resultado una censura directa;
- pueden dar lugar a pérdidas financieras para el medio en cuestión ya que los restringe a un ámbito offline y su audiencia es incapaz de acceder al sitio;
- pueden ocasionar gastos extras pues se debe buscar asistencia técnica; y
- pueden dar como resultado que el público piense que la publicación ya no sigue existiendo.

Alteración de sitios web

Existen muchas formas para que un sitio web pueda ser alterado. Una táctica común implica utilizar ataques MitM para comprometer las cuentas de usuarios legítimos. Alternativamente, un atacante podría explotar las vulnerabilidades del *software* del servidor del sitio web.

La alteración de una página web es un ataque utilizado frecuentemente contra agencias de medios de comunicación.[76]

Cuentas de usuario comprometidas

Es importante tomar en cuenta que uno de los objetivos prioritarios de la mayoría de los atacantes consiste en robar el acceso a información que aún no se genera.[77] Por ende, las cuentas de usuario, como las de e-mail, redes sociales o Skype, pueden comprometerse de diversas formas. Mediante un ataque de *phishing* se puede instalar *malware* en el dispositivo de un periodista y, así, registrar las pulsaciones del teclado de su dispositivo y capturar contraseñas y otra información sensible. Un atacante también puede utilizar un sitio web falso y, después de que el usuario introduce su información de acceso, el atacante puede entonces utilizarla para acceder al sitio web real sin alertar al usuario.[78] La autenticación de dos factores ayuda a evitar que una cuenta sea comprometida pues requiere tanto la clave de acceso a la cuenta como el dispositivo para acceder (un teléfono celular, por ejemplo), el cual recibe un código de uso único para iniciar la sesión. Desafortunadamente, incluso la autenticación de dos factores puede verse comprometida por un atacante habilidoso.[79]

En el pasado se han dado también casos en las que las cuentas de usuario son amenazadas mediante sofisticadas tácticas de ingeniería social,[80] tal y como cuando la cuenta de Twitter de la Associated Press fue secuestrada en abril de 2013 para informar falsamente que el presidente de Estados Unidos, Barack Obama, había resultado herido tras dos explosiones en la Casa Blanca, provocando que el índice Dow Jones cayera de golpe en 140 puntos.[81]

Intimidación, acoso y exposición forzada de redes online

La intimidación, el acoso y el arresto de periodistas no son fenómenos nuevos. Sin embargo, los periodistas y quienes contribuyen al periodismo actualmente sufren amenazas en múltiples plataformas. Organizaciones de protección a la libertad de prensa de todo el mundo han reconocido el incremento de este fenómeno.[82]

Las amenazas físicas y digitales suponen una grave preocupación pues pueden ser la antesala para ataques contra periodistas.[83] Según investigaciones del CPJ, 38% de los periodistas asesinados en los últimos 21 años fueron amenazados antes de ser victimados.

A veces, los periodistas son intimidados para que entreguen información de sus cuentas digitales. Por ejemplo, las autoridades pueden detener o amenazar a un periodista para obligarlo a que entregue las contraseñas de sus cuentas de redes sociales o correo electrónico.

Para tratar de protegerse, los periodistas a veces comparten sus contraseñas con colegas. Si son arrestados, sus colegas pueden acceder y eliminar información que podría ser suficiente para detener a alguien de acuerdo con leyes muy estrictas de libertad de expresión. En ocasiones, las ONG trabajan con empresas para cerrar la cuenta de un periodista tan pronto como se reporta que ha sido secuestrado o arrestado. Además, los periodistas y los distribuidores de contenido noticioso pueden también tener cuentas múltiples, de modo que si son forzados a revelar detalles de una cuenta puedan seguir manteniendo en secreto información especialmente sensible. El arresto y detención de los periodistas es importante para la seguridad digital porque puede exponer sus redes y a sus fuentes, aumentando el riesgo de perjuicio para ambas.

Desinformación y campañas de difamación

La divulgación de información falsa de los periodistas no es novedosa, pero las campañas de difamación online resultan particularmente problemáticas debido a que pueden tener una larga vida online y difundirse por todas partes muy rápidamente.

Las campañas de difamación implican muchas tácticas de intimidación que a menudo son tanto online como offline. Éstas pueden incluir la creación de sitios web falsos o la intimidación con fotos o videos comprometedores que se pueden difundir online. Otras veces, los atacantes eligen clonar un sitio web para confundir a los lectores y atentar contra la credibilidad y legitimidad de una agencia de noticias. En otros casos, agentes de medios de comunicación han reportado casos de cibersuplantación, campañas de propaganda online, campañas de difamación y ataques en foros virtuales.

También se pueden establecer campañas de desinformación contra sitios de noticias online. En septiembre de 2013, el sitio de periodismo de investigación Ukrainska Pravda (Verdad Ucraniana) advirtió la aparición de una copia de su sitio web denominada Ukrainska Kryvda (Mentiras Ucranianas), que imitaba en todo al diseño de su página original.[84]

Las campañas de difamación son importantes para la seguridad de los periodistas de medios online –especialmente cuando se aplican en la red– debido a que:

- dañan la credibilidad, integridad y confianza de los periodistas: elementos que son esenciales para realizar con éxito su labor; y
- intimidan a fuentes y periodistas, lo que da como resultado una autocensura.

Confiscación de herramientas periodísticas

La confiscación de heramientas periodísticas no es una táctica novedosa para intimidar o acosar a los periodistas. Sin embargo, en un entorno cada vez más digital donde los periodistas almacenan enormes cantidades de información en dispositivos portátiles (como laptops y teléfonos celulares), las fuentes y la información confidencial están en mayor riesgo. Estos dispositivos contienen demasiada información y datos con los que se pueden revelar los nombres y la ubicación de las fuentes, poniéndolas en peligro.[85]

Almacenamiento y extracción de datos

El almacenamiento de datos se ha vuelto cada vez más barato y más eficiente, permitiendo que se recopilen y almacenen –incluyendo el contenido de e-mails, textos y otras comunicaciones– durante periodos más largos. Esto facilita el proceso de extracción de datos, entendido éste como la búsqueda a través de grandes cantidades de información computarizada para encontrar patrones o tendencias útiles.[86] Por ejemplo, puede utilizarse para señalar a probables fuentes periodísticas. En este sentido, existe un importante mercado para analizar datos masivos y muchas de las empresas que suministran datos de consumidores a sitios como Facebook son las mismas que suministran información a agencias de inteligencia y de seguridad, sin ningún tipo de control o contrapeso.[87]

Existen casos donde supuestamente se ha tenido acceso a información almacenada de fuentes periodísticas (incluyendo datos sobre localización y tráfico de teléfonos celulares) debido a la existencia de leyes de retención de datos en ciertos países.[88]

La extracción de datos tiene consecuencias mucho después del acto inmediato de intercepción o incautación, incluyendo:

- un efecto disuasorio sobre las fuentes y periodistas, que quedan intimidados;
- la invasión del derecho a la privacidad de periodistas y fuentes; y
- detención, arresto, enjuiciamiento y encarcelamiento.

2.3 Mapeo de las principales partes interesadas e iniciativas

Este apartado presentará a varias de las principales partes interesadas y sus iniciativas. Las prácticas se mostrarán temáticamente y cada sección contará con ejemplos que reflejen las regiones geográficas de los Estados Miembros de la UNESCO. Al igual que en la sección 1.3, las principales áreas de ejercicio han sido categorizadas de la siguiente forma:

- Labor normativa y concientización
- Cursos y guías de capacitación en seguridad digital;
- Líneas directas y asistencia en seguridad;
- Reportes e investigación.

Ésta no es una lista exhaustiva, pero pretende proporcionar un resumen de los tipos de prácticas que existen en todo el mundo. Las descripciones de las organizaciones mencionadas pueden encontrarse en el glosario incluido al final del informe.

Labor normativa y concientización

La concientización es una forma de sensibilizar a todos los actores sobre la seguridad digital para el periodismo, y promover la norma social de que dicha comunicación debería disfrutar especialmente de seguridad y protección. Elaborar estas normas implica a nivel global decisiones y posiciones por parte de organismos intergubernamentales que tienen una base legítima para ello. Promover dicha concientización es entonces necesario si estas posiciones han de convertirse en normas existentes frente a las que puede medirse un comportamiento. Existe una creciente implicación normativa en la seguridad del periodismo y sus dimensiones digitales.

Global

El Consejo de Derechos Humanos (CDH) es un organismo intergubernamental de las Naciones Unidas compuesto por 47 Estados Miembros elegidos por la Asamblea General y que durante varios años se ha centrado en la seguridad de los periodistas. De manera significativa, afirmó en 2012 que "los mismos derechos que las personas tienen offline deben también ser protegidos online, en particular la libertad de expresión, la cual es aplicable independientemente de las fronteras y a través de cualquier medio de comunicación de propia elección, de acuerdo con el artículo 19 de la Declaración Universal de los Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos".[89]

También en 2012, el CDH aprobó una emblemática resolución sobre la seguridad de los periodistas que se centra específicamente en los elevados riesgos que enfrentan los periodistas y en la necesidad de garantizar una mejor protección para los trabajadores de los medios de comunicación. La resolución reconoce la importancia de todas las formas de medios de comunicación, incluyendo Internet, en la promoción y protección del derecho a la libertad de opinión y expresión, y condena todos los ataques y actos de violencia contra periodistas.[90] En 2014, el CDH continuó con otra resolución (A/HRC/27/L.7) que elaboraba considerablemente a partir de la resolución anterior, y en el mismo año el Secretario General de las Naciones Unidas publicó un exhaustivo informe sobre la seguridad de los periodistas y la cuestión de la impunidad (A/69/268).

El 18 de diciembre de 2013, la Asamblea General de las Naciones Unidas adoptó la Resolución sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad en su 68ª sesión. La resolución "condena de manera inequívoca todos los ataques y actos de violencia contra periodistas y trabajadores de medios de comunicación, como la tortura, los asesinatos extrajudiciales, las desapariciones forzadas y la detención arbitraria, así como la intimidación y acoso en situaciones tanto de conflicto como de no conflicto". En la misma sesión, proclamó también el 2 de noviembre como Día Internacional para Poner Fin a la Impunidad de los Crímenes contra Periodistas.[91]

En mayo de 2013, los participantes de la conferencia de la UNESCO "Hablar sin miedo: por el ejercicio seguro de la libertad de expresión en todos los medios", adoptaron la Declaración de San José, en el marco del 20 Aniversario del Día Mundial de la Libertad de Prensa. Esta declaración insta a los medios de comunicación y asociaciones profesionales a desarrollar y mantener prácticas de seguridad, incluyendo la capacitación en seguridad digital para empleados autónomos y trabajadores regulares.[92] También llama a los Estados Miembros de la UNESCO a emprender acciones que garanticen la libertad de expresión de todos aquellos que utilizan medios digitales, incluyendo blogueros y productores de medios sociales, y que los protejan contra la intimidación física, ciberataques y atentados contra sus vidas. Principios similares fueron promovidos en la Declaración de París, adoptada en la conferencia del Día Mundial de la Libertad de Prensa 2014 que se celebró en la sede de la UNESCO: "El derecho de acceso a la información, a medios de comunicación independientes y a la seguridad para ejercer la libertad de expresión son esenciales para el desarrollo". En el contexto de una resolución sobre cuestiones relacionadas con Internet, en noviembre de 2013 los Estados Miembros de la UNESCO afirmaron que "la privacidad es esencial para proteger a las fuentes periodísticas, las cuales permiten que una sociedad se beneficie del periodismo de investigación, fortalezca la buena gobernanza y el estado de derecho, y que dicha privacidad no debería estar sujeta a interferencias arbitrarias o ilícitas".[93]

La seguridad digital no está específicamente señalada en el informe sobre mejores prácticas de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos de 2013 sobre la seguridad de los periodistas.[94] Sin embargo, la resolución del CDH, A/HRC/27/L7, sobre la seguridad de los periodistas adoptada en septiembre de 2014, hace hincapié en dos dimensiones: el importante papel de las agencias de medios de comunicación a la hora de proporcionar seguridad digital y el reconocimiento de la "particular vulnerabilidad de los periodistas de convertirse en objetivo de vigilancia ilícita o arbitraria y/o de interceptación de comunicaciones en violación de sus derechos a la privacidad y la libertad de expresión".

En noviembre de 2013 la Asamblea General de las Naciones Unidas llamó a todos los Estados a revisar sus políticas de vigilancia y establecer una supervisión independiente. La Oficina del Alto Comisionado recibió el mandato de hacer un estudio adicional sobre la privacidad, incluyendo la privacidad digital, que apareció como A/HRC/27/37 en junio 2014.[95] Aunque no se ocupaba específicamente de los periodistas, llegó a la conclusión de que "la legislación internacional sobre derechos humanos proporciona un marco claro y universal para la promoción y protección del derecho a la privacidad, incluso en el contexto de la vigilancia doméstica y extraterritorial, la interceptación de comunicaciones digitales y la recopilación de datos personales. Sin embargo, las prácticas en muchos Estados han puesto de manifiesto una falta de legislación y/o aplicación de la ley adecuada a nivel nacional, malas salvaguardias procesales y una supervisión ineficaz, todo lo cual ha contribuido a una falta de rendición de cuentas para la interferencia arbitraria o ilícita en el derecho a la privacidad". Y recomendaba: "Deberían adoptarse medidas para garantizar que son aplicados regímenes y prácticas de supervisión eficaces e independientes, con atención al derecho de las víctimas a un remedio efectivo".

No entra en el ámbito de este estudio profundizar en las políticas y medidas de los Estados para dar seguimiento a estas resoluciones en formas que mejoren la protección digital de las personas que hacen periodismo. Sin embargo, está claro que, según sus propios estándares fijados, los propios Estados tienen que respetar, proteger y promover los derechos a la libre expresión y la privacidad. Esto los obliga a tener un propósito legítimo, así como controles y contrapesos adecuados, con respecto a su implicación en cuestiones digitales que tengan un impacto en la libertad de prensa. Ello debido a la necesidad de garantizar que sus propias actividades se ajustan a los estándares internacionales, como la necesidad y proporcionalidad respecto a cualquier limitación o intrusión en la libertad de expresión y la labor periodística. Los Estados tienen también que contar con regímenes adecuados de protección de datos que protejan la privacidad y eviten el abuso por parte de actores tanto públicos como privados.

Además de las Naciones Unidas, otros actores internacionales que se dedican a estas cuestiones incluyen la Coalición para la Libertad Online. Esta asociación de 23 gobiernos ha adoptado recomendaciones para la libertad online, incluyendo un compromiso para apoyar los conocimientos digitales para empoderar a los usuarios de Internet y proteger sus derechos humanos y libertades fundamentales. La Coalición llama también a los gobiernos a que pongan fin, entre otras cosas, a la censura y el *hacking*.[96]

En la sociedad civil, la red de Intercambio Internacional por la Libertad de Expresión (IFEX) es una red global que defiende y promueve la libre expresión, monitorea regularmente las violaciones a la libertad de expresión y la seguridad de los periodistas en todo el mundo, emite noticias, difunde boletines informativos y alberga un archivo consultable en línea de alertas.

Como parte de sus esfuerzos de concientización a nivel internacional, el CPJ envía regularmente cartas a funcionarios de alto nivel instigándolos a investigar ataques contra periodistas y mejorar el clima de impunidad. El CPJ documenta también amenazas y ataques en el ciberespacio y concientiza sobre ellos con alertas informativas y entradas de blogs.

RightsCon es una conferencia anual sobre derechos humanos que reúne a especialistas en tecnología, defensores de los derechos humanos, legisladores y otros para discutir importantes cuestiones y políticas que se relacionan con los derechos humanos y la tecnología.[97]

Otro esfuerzo internacional para fortalecer las normas y crear conciencia es la Reunión de Blogueros Árabes, auspiciada por la Fundación Heinrich Boell y Global Voices, que ha desempeñado un papel importante a la hora de ayudar a activistas digitales a desarrollar una red de solidaridad común.[98] Aunque la Reunión de Blogueros no es anual, para 2013 ha habido cuatro instancias.

Norteamérica y Europa

En mayo de 2014, el Consejo de Europa (CdE) adoptó las Directrices de la Unión Europea (UE) sobre Libertad de Expresión online y offline.[99] En su declaración, el CdE afirmó que se basaría en el contenido de resoluciones relevantes de las Naciones Unidas, incluyendo aquellas que se centran en la seguridad de los periodistas y el derecho a la privacidad en la era digital. El Comisionado para los Derechos Humanos del CdE, Nils Muižnieks, afirmó vía Twitter el 19 de mayo de 2014: "Necesitamos abordar la situación particular de los blogueros y periodistas online. #SafetyOfJournalists".[100]

La Organización para la Seguridad y la Cooperación en Europa (OSCE) actualizó su guía "La seguridad de los periodistas" en mayo de 2014, incluyendo sus lineamientos sobre seguridad digital.[101] Además, el representante de la OSCE sobre libertad de los medios de comunicación, Dunja Mijatović, ha incluido cada vez más la cuestión de la seguridad digital en sus declaraciones y discursos.

Un organismo que se centra en la cuestión de la seguridad de los periodistas es la Comisión Nacional del Reino Unido para la UNESCO. La Comisión trabaja con diversas organizaciones, incluyendo grupos de periodistas y defensores de la libertad de prensa, para garantizar que la seguridad de los periodistas sigue siendo una prioridad entre los gobiernos, la UNESCO y la comunidad internacional. Actualmente, la Comisión trabaja para elevar el perfil de las resoluciones de las Naciones Unidas sobre la seguridad de los periodistas y para ayudar a proteger a los profesionales de los medios de comunicación de todo el mundo.[102]

En enero de 2014, Privacy International lanzó una iniciativa de tres años conocida como el proyecto de Monitoreo y Defensa contra la Vigilancia Global (GSMA). Dicha iniciativa se centra en detectar e investigar tecnologías avanzadas de vigilancia dirigidas a periodistas, activistas y defensores de los derechos humanos. El GSMA pretende apoyar cambios utilizando los hallazgos de su investigación para analizar cómo y dónde se están desplegando estas tecnologías.[103]

El Instituto Humanista para la Cooperación al Desarrollo (HIVOS), con sede en Holanda, lanzó un proyecto para defensores digitales en 2012, a iniciativa de la Coalición para la Libertad Online, que intenta proteger la libertad de expresión proporcionando apoyo de emergencia para blogueros, periodistas y otros que son atacados mientras promueven y protegen los derechos humanos y la democracia.

Latinoamérica y el Caribe

En Colombia, la Fundación para la Libertad de Prensa (FLIP) monitorea la libertad de prensa y la seguridad de los periodistas a través de su red de alerta y protección. Cuenta con una red de 30 corresponsales desplegados a lo largo del país que reportan sobre violaciones a la libertad de prensa.

El Centro Internacional para Periodistas (ICFJ) lanzó la Iniciativa para el Periodismo de Investigación en las Américas en 2013. Este programa de cuatro años, cofinanciado por la Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) y la Oficina de Democracia, Derechos Humanos y Asuntos Laborales (DRL) del Departamento de Estado estadounidense, se centra en promover y fortalecer la transparencia, la seguridad y la libertad de expresión de los medios de comunicación, ofreciendo talleres específicos para cada país sobre seguridad digital y móvil, además de otros diversos cursos y actividades de capacitación.

África

La Relatora Especial sobre Libertad de Expresión y Acceso a la Información en África, Faith Pansy Tlakula, ha integrado la seguridad digital en su promoción de la seguridad

de los periodistas. En 2014, ofreció comentarios sobre los desafíos que enfrenta el periodismo online, como parte del simposio de un día sobre medios digitales de la Plataforma de Innovación Informativa del Instituto de Prensa Internacional, incluyendo la sostenibilidad, la seguridad y la autorregulación.[104]

En 2013, fue establecida una iniciativa conocida como Testigo No Deseado (UW) por parte de Geoffrey Wokulira Ssebaggala, quien ganó recientemente el Premio para Defensores de los Derechos Humanos de la Unión Europea. Entre sus muchos proyectos, UW monitorea la vigilancia por parte de gobiernos, ofrece apoyo legal a blogueros y defiende los derechos digitales.[105]

A principios de 2014, fue lanzado el Intercambio Africano para la Libertad de Expresión (AFEX). Dicha red se compone de organizaciones africanas para la libertad de expresión, las cuales son miembros del Intercambio Internacional para la Libertad de Expresión (IFEX). Esta red pretende embarcarse en campañas conjuntas para garantizar el acceso a la información de ciudadanos africanos, promover la seguridad de los periodistas, pedir justicia para los ataques contra periodistas y desafiar las leyes que restringen la libertad de expresión. La red incluye a las siguientes organizaciones:

- Instituto de Medios de Comunicación para África del Sur (MISA),
- Centro Africano para la Libertad de Información (AFIC),
- Centro para Estudios sobre Medios de Comunicación y Consolidación de la Paz (CEMESP),
- Red de Derechos Humanos para Periodistas – Uganda (HRNJ-Uganda),
- Periodista en Peligro (JED),
- Fundación de Medios de Comunicación para África Oriental (MFWA),
- Agenda sobre Derechos de los Medios de Comunicación (MRA), y
- Sindicato Nacional de Periodistas Somalíes (NUSOJ).

Otra organización que se dedica a cuestiones de periodismo digital es la Iniciativa de Medios Africanos (AMI). AMI es una organización panafricana compuesta por más de 800 empresas de medios de comunicación de África que trabaja para fortalecer el sector de medios privados e independientes del continente y promover la gobernanza democrática, el desarrollo social y el crecimiento económico.[106] El asesor de medios de comunicación y becario del ICFJ, Justin Arenstein, dirige el programa de innovación digital de la AMI, donde contribuye desarrollando estrategias y recursos para ayudar a los medios de comunicación africanos a superar cualquier incidencia, además de apoyar un programa de habilidades digitales, entre otras actividades.[107]

Estados árabes

El Centro de Medios Independientes de Kurdistán (IMCK) es una organización sin fines de lucro fundada hace varios años en la región del Kurdistán de Irak, con apoyo de Free Press Unlimited. Proporciona programas de capacitación a periodistas y profesionistas que quieren trabajar en periodismo. También lleva a cabo aproximadamente 80 cursos cada año, algunos enfocados en la seguridad en Internet.[108]

En diciembre de 2013, el Instituto para el Reporte de la Guerra y la Paz (IWPR) lanzó la Academia Ciber-Árabes como una plataforma online para cursos gratuitos sobre seguridad digital en árabe.

Asia-Pacífico

En 2012, y frente a la inseguridad sistémica de los periodistas y blogueros paquistaníes, el Centro de Innovación y Aprendizaje de Internews elaboró un amplio informe sobre "Seguridad digital y periodistas: Un panorama de concientización y prácticas en Pakistán".[109] El informe "pretende subrayar áreas donde los periodistas y blogueros de Pakistán son especialmente vulnerables en su uso de medios digitales, y hace algunas recomendaciones", concretamente, el uso de servicios de e-mail seguros, encriptación de datos o servicios de bloqueo de IP.

Cursos de capacitación en seguridad digital

Diversos individuos y organizaciones han respondido a la necesidad de un mayor conocimiento en seguridad digital desarrollando cursos de capacitación específicos, incluyendo algunos de los mencionados bajo la sección sobre normas y concientización de más arriba.

Global

El Programa Intergubernamental para el Desarrollo de la Comunicación de la UNESCO proporciona subvenciones anuales a iniciativas de seguridad en el periodismo, incluyendo cursos online y desarrollo de capacidades para seguridad digital, así como indicadores de apoyo en seguridad que incluyen una dimensión digital.[110] En marzo de 2014, la UNESCO, en cooperación con el Instituto para el reporte de la guerra y la paz, organizó una serie de cursos de capacitación sobre seguridad digital para periodistas tunecinos. Los cursos consistían en dos talleres de capacitación de cuatro días, con 29 participantes en total, de las cuales 16 fueron mujeres.[111]

En la RightsCon 2014, el equipo técnico de Access organizó un mostrador de ayuda sobre seguridad digital, donde su equipo dedicó dos días a diagnosticar las computadoras de los participantes, ofrecer consejos sobre seguridad digital y ayudar a implementar herramientas de seguridad digital. El mostrador estuvo concurrido durante la conferencia, lo que indica que hay una necesidad previamente no satisfecha para este tipo de asesoría. Para satisfacer dichas necesidades, la iniciativa piloto de un año del IREX conocida como SAFE abrió tres centros regionales de recursos para seguridad en El Salvador, Georgia y Kenia en el verano de 2013. SAFE adapta su asistencia utilizando a aprendices locales para proporcionar capacitación en seguridad digital, seguridad física y atención psicosocial para periodistas.[112]

Artículo 19 proporciona varios cursos de capacitación en seguridad digital y física a lo largo del año en diversas ubicaciones internacionales. El personal de Artículo 19 proporciona también experiencia en marcos jurídicos nacionales y su relación con la libertad de expresión y la ética en los medios de comunicación.[113]

Aunque gran parte de la capacitación es patrocinada y proporcionada de forma gratuita a los participantes, algunas organizaciones sustentan sus servicios cobrando una tarifa por la capacitación. Un ejemplo es Global Journalist Security, una organización fundada y dirigida por Frank Smyth, asesor durante mucho tiempo del CPJ.[114]

El Instituto Internacional de Prensa (IPI) también llevó a cabo una capacitación en seguridad digital en Sudáfrica en 2014 como parte de su Plataforma Innovadora de Noticias.[115] El evento, llamado "ChalengeSSS of the New Age" se enfocaba en la sostenibilidad, la seguridad y la autorregulación.

Norteamérica y Europa

También se está produciendo cada vez más capacitación en seguridad digital en el ámbito online. Deutsche Welle Akademie organizó un seminario de capacitación online de una semana sobre seguridad digital para periodistas de todo el mundo en diciembre de 2013. El seminario incluía a tecnólogos del Colectivo de Tecnología Táctica y Citizen

Lab, así como a expertos en libertad en Internet de organizaciones como Reporteros sin Fronteras.

La Fundación Nacional de Prensa de Washington, D. C., y el Fondo Rory Peck de Londres ofrecieron cursos de capacitación online en 2013 que cubrieron cuestiones de seguridad digital para periodistas a nivel global. Estos cursos incluían a especialistas en tecnología y defensores de la libertad de prensa de organizaciones como el Colectivo de Tecnología Táctica, la Fundación Fronteras Electrónicas y la Fundación para la Libertad de Prensa. El Fondo Rory Peck pretende impulsar su labor en seguridad digital desarrollando y difundiendo una guía para la seguridad online. Además, el Fondo seguirá trabajando con socios como el Registro de Autónomos de Primera Línea y el Proyecto Guardian para proporcionar recursos en seguridad digital a periodistas autónomos.[116]

Latinoamérica y el Caribe

El Centro de Periodismo Digital de la Universidad de Guadalajara realiza anualmente un programa de cuatro semanas, "Cobertura segura", para periodistas de México. En 2013, 14 periodistas tomaron parte en la capacitación. El taller ayuda a periodistas a analizar y reconocer amenazas y aprender buenas prácticas de seguridad digital. Impartido por una serie diversa de expertos que incluye reporteros locales que han trabajado sobre el crimen organizado, la capacitación normalmente se centra en estrategias de prevención más que de reacción.[117]

Derechos Digitales lanzó una campaña llamada "No tengas miedo de Internet: La privacidad depende de nosotros", que hace uso de videos y gráficos para proporcionar consejos sobre cómo los individuos pueden cuidar de sus datos personales en el entorno digital.[118] En México, organizaciones como Periodistas de a Pie, Social TIC y Artículo 19 han organizado cursos de capacitación en seguridad digital.

En 2014, el FOPEA (Foro de Periodismo Argentino), en colaboración con el CELE (Centro de Estudios en Libertad de Expresión y Acceso a la Información) y la Asociación por los Derechos Civiles, organizaron un taller sobre ciberseguridad para periodistas argentinos. El taller fue dirigido por Robert Guerra, experto en ciberseguridad y derechos humanos.[119]

El Centro Internacional para Periodistas (ICFJ), junto con organizaciones locales mexicanas (el Centro de Investigación y Docencia Económicas, CIDE, y el Centro Nacional de Comunicación Social, CENCOS), así como la ONG Freedom House, están desarrollando cursos de seguridad digital para periodistas.[120] Estos cursos informarán a los periodistas de los riesgos para la seguridad relacionados con los teléfonos inteligentes, la geolocalización y los virus. Enseñarán a los periodistas cómo navegar de manera segura por Internet al tiempo que protegen sus comunicaciones y bases de datos.

La Sociedad Interamericana de Prensa (SIP) ofrece un seminario en video online dirigido a reporteros y editores que quieran entender los riesgos relacionados con el uso de las redes sociales (Facebook, Twitter…), así como obtener las herramientas que necesitan para evitar el *hacking* de estas redes.[121]

Asia y el Pacífico

En Pakistán, organizaciones como la Fundación para los Derechos Digitales, Bytes para Todos y Bolo Bhi han proporcionado cursos de capacitación en seguridad digital para periodistas, blogueros y defensores de los derechos humanos. Los cursos de capacitación de Bolo Bhi forman parte de una iniciativa piloto llamada "Garantizando tu cotidianidad online y offline", que imparte cursos básicos gratuitos de capacitación en seguridad digital, realiza análisis de riesgos y da consejos sobre seguridad física y seguridad digital. Bolo Bhi pretende ofrecer los cursos una vez al mes. En enero de 2014, la Fundación para los Derechos Digitales organizó una capacitación en seguridad digital en Pakistán específicamente para mujeres.

Guías de capacitación y plan de estudios de capacitación en seguridad digital

Guías de capacitación en seguridad digital

Norteamérica y Europa

Numerosas organizaciones, aparte de algunas de las ya mencionadas, han creado guías de seguridad digital para periodistas. Tactical Tech y Defensores de Primera Línea han desarrollado un proyecto online conocido como "Seguridad envasada" (Security-in-a-Box), que ejemplifica con situaciones hipotéticas para ayudar a los periodistas a entender mejor las amenazas a la seguridad digital. Incluye recomendaciones para *software* gratuito, proporciona tutoriales de video y está disponible en varios idiomas. También es actualizado a menudo con nuevas herramientas y tácticas, incluyendo más recientemente un kit de herramientas en concreto para la comunidad LGBT de los países de habla árabe.

Internews cuenta con un "Kit de herramientas para hablar de forma segura" que proporciona a los periodistas información sobre cómo estar más seguro online y cuándo utilizar sus teléfonos celulares. La guía está disponible en español, inglés y árabe. El Fondo Rory Peck cuenta con un recurso online en seguridad digital para periodistas autónomos, dispuesto cómodamente por temas y capturas de pantalla de video, mientras que Small World News tiene guías en inglés y árabe sobre cómo utilizar con seguridad teléfonos vía satélite.

Reporteros sin Fronteras tiene un kit de seguridad online en su sitio web WeFightCensorship (LuchamosContraLaCensura). Explica la necesidad de purgar los archivos de sus metadatos de identificación, plantea cómo utilizar Tor y VPN para anonimizar y encriptar comunicaciones, y ofrece consejos sobre cómo asegurar las comunicaciones y datos en teléfonos celulares y laptops.[122]

Otras guías de capacitación incluyen la "Guía de Seguridad de la Información" del CPJ, la guía de encriptación de la Fundación para la Libertad de Prensa y el "Proyecto para Autodefensa de la Vigilancia" de la EFF, que está disponible en inglés y ruso. La EFF también redacta un blog dedicado a diversas cuestiones, incluyendo asuntos de seguridad digital, conocido como el blog Deeplinks.[123]

La Asociación para Comunicaciones Progresistas, con apoyo de la Agencia Sueca de Cooperación para el Desarrollo Internacional, ha publicado un recurso titulado "Kit de primeros auxilios sobre seguridad digital para defensores de los derechos humanos", que proporciona pasos concretos, recursos adicionales y referencias para apoyar a grupos a quienes los activistas y periodistas pueden acudir en busca de orientación.[124]

Estados árabes

Algunas guías de capacitación han sustituido el tipo de enfoque cargado de texto en favor de la animación en video. Un ejemplo es la "Guía de supervivencia para periodistas", elaborada y publicada por el Centro SKeyes para Medios de Comunicación y Libertad Cultural, con sede en Beirut. La guía está disponible tanto en árabe como en inglés y está dirigida a periodistas profesionales y ciudadanos.[125]

Latinoamérica y el Caribe

El exbecario de periodismo internacional del Knight Center, Jorge Luis Sierra, escribió un manual en 2013, titulado "Manual de seguridad digital y móvil", para periodistas y blogueros de habla hispana. El manual ofrece consejos sobre cómo crear planes y protocolos de reducción de riesgos para seguridad digital y móvil, y fue publicado por el ICFJ y Freedom House.

Cursos de capacitación en seguridad digital

Las actividades de capacitación en seguridad digital para periodistas y otros que hacen periodismo son organizadas por diversas organizaciones, incluyendo instituciones académicas, ONG que trabajan a nivel internacional y organizaciones locales. Esta sección examina lo que se está haciendo para potenciar cursos y capacitadores, y para diseminar la seguridad digital en cursos más amplios, como en las escuelas de periodismo universitarias.

Un ejemplo es el de Internews, que en marzo de 2014 lanzó un plan de estudios y manual de capacitación en seguridad digital llamado "PeriodistaMásSeguro" (SaferJourno), que cuenta con lineamientos sobre mejores prácticas de las que pueden hacer uso los capacitadores en seguridad digital cuando enseñan a periodistas.[126] Internews también ha lanzado un plan de estudios de capacitación paso a paso, gratuito y de fuentes abiertas para capacitadores en seguridad digital. Contiene seis módulos, incluyendo "Cómo evaluar riesgos digitales", "Cómo evitar el *malware*", "Cómo mantener seguros los datos", "Cómo investigar de manera segura", "Cómo mantener seguro el correo electrónico" y "Seguridad para teléfonos celulares". El kit de herramientas fue probado sobre en la práctica con capacitadores de los ámbitos de radiodifusión, prensa y online, y evaluado por algunos de los principales expertos de la comunidad de seguridad digital.[127]

En 2013, la UNESCO publicó un programa modelo sobre seguridad para periodistas que cubría todo el panorama de la seguridad aunque sin profundizar acerca de las amenazas digitales.[128] Sin embargo, parece ser que en varias escuelas de periodismo la capacitación en seguridad digital todavía no está integrada sistemáticamente en el plan de estudios, aunque muchos profesores de periodismo parecen reconocer que esto es fundamental para los estudiantes.[129] Esto podría deberse a diversos factores, incluyendo una falta de concientización o conocimientos, inflexibilidad o limitaciones de tiempo en un plan de estudios de periodismo ya repleto, desacuerdos sobre cómo debería enseñarse la capacitación en seguridad digital y si todos los estudiantes de periodismo necesitan capacitación.

Una de las instituciones académicas que encabeza la capacitación en seguridad digital es el Centro Tow para Periodismo Digital de la Escuela de Periodismo de la Universidad de Columbia, en la ciudad de Nueva York.[130] En noviembre de 2013, el Centro organizó un taller de tres días para periodistas, reuniendo a expertos en seguridad, periodistas y abogados. El taller proporcionó a los participantes una visión general de cómo las prácticas de seguridad digital y física apoyan y mejoran el periodismo.[131] Durante el 2014, el Centro planeó identificar mejores prácticas cuando se enseña seguridad digital para periodistas, con la intención de desarrollar eventualmente una metodología que pueda utilizarse para enseñar a los estudiantes de periodismo. El Centro lanzó también Periodismo Después de Snowden, una iniciativa que investiga el periodismo en una época de vigilancia por parte del Estado.

La Escuela de Periodismo de Columbia y el Departamento de Informática de la Universidad de Columbia han creado un nuevo programa de certificación de posgrado que procurará mejorar la alfabetización digital para periodistas. Llamado Programa Lede, ofrecerá capacitación práctica en datos y tecnologías de datos impartida en el contexto del periodismo.[132]

Algunos profesores se han encargado de garantizar que sus estudiantes entiendan los fundamentos del análisis de riesgos y la seguridad digital incorporando discusiones teóricas de capacitación en seguridad digital en su plan de estudios existente. En la Universidad de Minnesota, Jane E. Kirtley, profesora de Ética y Legislación sobre Medios de Comunicación del Centro Silha, imparte una clase de nivel superior sobre los problemas actuales de libertad de expresión y prensa, y discute la seguridad digital de los periodistas en relación a la privacidad online y la seguridad de datos.[133] En la Escuela Superior de Periodismo de la Universidad de la Ciudad de Nueva York (CUNY), el profesor Sandeep Junnarkar ha añadido la capacitación en seguridad digital a su plan de estudios, creando un taller de cuatro horas que se centra principalmente en tácticas

y herramientas.[134] El periodista de investigación y profesor de la Escuela de Periodismo y Comunicación de Masas Walter Cronkite de la Universidad Estatal de Arizona, Steve Doig, ha ofrecido una conferencia sobre vigilancia y dispositivos de espionaje cada semestre durante varios años, pero sólo recientemente ha visto un repunte importante en cuanto al interés.[135] Según un artículo publicado en la Columbia Journalism Review, la conferencia de Doig a menudo es la primera vez que los estudiantes escuchan hablar de las vulnerabilidades en seguridad y de las medidas que los periodistas tienen que adoptar si se encuentran con fuentes de alto nivel.[136] El Centro Knight para el Periodismo en las Américas, con sede en Austin, Texas, también ha organizado seminarios web sobre cuestiones de seguridad online.

En Turquía, un profesor que ha integrado la capacitación en seguridad digital en su plan de estudios es Ismail Hakki Polat, profesor de Nuevos Medios de Comunicación de la Universidad de Kadir Has. Enseña seguridad de la información a estudiantes en dos cursos diferentes y lo lleva haciendo desde 2010.[137] El trabajo de curso incluye una introducción a los conceptos básicos de seguridad de la información, criptografía, seguridad de la comunicación en tiempo real, y leyes y regulaciones sobre información y seguridad, entre otros temas.[138]

En México, el exbecario del Knight Center del ICFJ, Jorge Luis Sierra, creó un plan de estudios de capacitación online y presencial sobre seguridad digital y móvil para el Centro para la Educación sobre Periodismo Digital de la Universidad de Guadalajara.[139]

Otras instituciones de enseñanza del periodismo están empezando a considerar la integración de la seguridad digital en su plan de estudios de periodismo. En la Escuela Danesa de Medios de Comunicación y Periodismo, los profesores debaten la cuestión de la seguridad digital con los estudiantes, aunque esto no estaba formalmente integrado en su programa en estos momentos.[140] Aunque no adscrita a una universidad, la Escuela de Periodismo de la Academia de la BBC es una institución de periodismo que forma periodistas para dicha cadena. La Escuela está planeando ofrecer capacitación en seguridad digital para periodistas, pero esto no ha sido implementado completamente en el momento de redactar el presente informe.[141] La Escuela de Periodismo Medill de la Universidad del Noroeste de EUA publicó recientemente una guía de seguridad digital escrita por el Director Ejecutivo de Global Journalist Security, Frank Smyth, aunque ellos tampoco habían integrado todavía la capacitación en seguridad digital en su plan de estudios en el momento de redactar el presente informe.[142]

Líneas directas y asistencia en seguridad

Muchas organizaciones proporcionan asistencia en seguridad, aunque prefieren no dar a conocer estos recursos fuera de sus redes de confianza, por temor a comprometer la seguridad de su personal y sus operaciones. Por consiguiente, no se han incluido en este informe. Otras opciones más públicas se han resumido más abajo.

Global

Programas de asistencia en seguridad para la protección física de periodistas han existido durante varios años por parte de organizaciones que incluyen el CPJ, Reporteros sin Fronteras y el Instituto Internacional de Seguridad en las Noticias. Estos programas de asistencia en seguridad resultan útiles y a menudo proporcionan asistencia jurídica, médica y en reubicaciones a periodistas y sus familias. Muchas de estas organizaciones, incluyendo el Comité Internacional de la Cruz Roja, proporcionan líneas directas para que los periodistas llamen cuando tienen problemas y necesitan recursos.[143]

Las entrevistas con expertos indican que es bastante común que las organizaciones de seguridad y defensa de la prensa conecten a periodistas con especialistas en tecnología. Sin embargo, con el aparente aumento de los ataques digitales contra periodistas, hay una necesidad de que más organizaciones proporcionen asistencia de respuesta inmediata a periodistas que sufren ataques digitales.

Una organización que aborda esta necesidad es la organización internacional no gubernamental Access, que en 2013 lanzó un sistema de respuesta inmediata para mitigar las amenazas digitales que enfrentan activistas y periodistas. Como parte del sistema de respuesta inmediata, Access opera una línea directa a la que los periodistas pueden llamar en busca de ayuda inmediata en seguridad digital si sospechan o son víctimas de un ataque digital.

El programa SAFE del IREX proporciona también una línea directa para periodistas que buscan ayuda en seguridad digital, incluyendo resolución de problemas con herramientas y técnicas, así como derivaciones a otras organizaciones que puede que sean capaces de ayudar en caso de peligro.[144]

Cada vez son más los especialistas en tecnología que unen sus esfuerzos con organizaciones de derechos humanos y protección a la prensa para ayudar a los periodistas a mejorar su seguridad digital, eludir la censura y evitar la vigilancia. A veces, estas reuniones se conocen como "hackatones", una colaboración intensiva de programadores y expertos durante un breve periodo de tiempo, a menudo en la misma ubicación física.[145]

Numerosas organizaciones desarrollan hackatones. Una de esas organizaciones es el Proyecto de Herramientas de Internet Abierto (Open ITP). Open ITP es una organización con sede en EUA que apoya a creadores de *software* y comunidades que desarrollan herramientas antivigilancia y anticensura de fuentes abiertas.[146]

Open ITP y CommunityRED organizaron recientemente un "Hackatón sobre libertad en Internet" en Washington D. C., donde los participantes aprendieron sobre herramientas para eludir la censura y recibieron comentarios generados por usuarios sobre éstas. Están previstos más hackatones próximamente.

Open ITP creó también los Tecno-Activismo Tercer Lunes (TA3M), que son encuentros informales diseñados para conectar a creadores de *software* y activistas que están interesados en censura, vigilancia y tecnología abierta. Actualmente, los TA3M se celebran en 16 ciudades de todo el mundo, y se esperan más próximamente.[147]

Otra organización que promueve hackatones en todo el mundo es la organización internacional de periodismo de base, en rápida expansión, conocida como Hacks/Hackers. El autoproclamado objetivo de la organización es crear una red de periodistas ("hacks") y tecnólogos ("hackers") que replanteen el futuro de las noticias y la información.[148] Existen numerosas secciones locales en países de todo el mundo y sus miembros organizan pláticas, días de demostraciones y hackatones.[149]

Dos periodistas crearon una aplicación llamada Hancel para mejorar la seguridad de los periodistas en Latinoamérica. Hancel es una aplicación de telefonía celular para Android que permite a los periodistas programar alertas automáticas en caso de un incidente y también reportar problemas a medida que ocurren. Los periodistas trabajan estrechamente con la Fundación para la Libertad de Prensa (FLIP) de Colombia y actualmente están desarrollando un proyecto piloto para Colombia y México. El proyecto recibió fondos de la Fundación Knight.[150]

Reportes e investigación

Internacional

Los informes de Freedom House y Reporteros sin Fronteras proporcionan valiosos datos y contexto sobre los tipos de ataques y amenazas que enfrentan los periodistas y otros actores que producen periodismo con tecnologías digitales, incluyendo a defensores de los derechos humanos de todo el mundo.

Freedom House publicó un informe que resume los hallazgos de su conferencia de noviembre de 2013 sobre la seguridad de los periodistas y otros actores que produ-

cen periodismo con tecnologías digitales.[151] El informe planteaba una serie de recomendaciones para su implementación por parte de organizaciones y donantes, que proporcionaría mejor protección online para periodistas y defensores de los derechos humanos.

El mapa "Voces amenazadas" de Voces Globales, realizado mediante *crowdsourcing*, registra a blogueros amenazados de todo el mundo, mientras que el ICFJ elabora también mapas para documentar ataques.

PEN América llevó a cabo recientemente una encuesta de sus miembros internacionales para documentar los ataques digitales que enfrentan los escritores, generando un informe gráfico para un fácil entendimiento de los resultados.[152]

El informe anual del CPJ sobre "Lista de riesgos" y "Ataques contra la prensa" ha empezado a incluir cuestiones de ciberseguridad, atrayendo la atención sobre los problemas que enfrentan los periodistas en este ámbito.[153]

Norteamérica y Europa

El Centro Tow organizó un taller de tres días sobre seguridad digital para periodistas en noviembre de 2013 en Nueva York, el cual reunió a un diverso grupo de especialistas en tecnología y periodistas digitales. Los capacitadores del taller instruyeron a los participantes sobre redes e Internet, y proporcionaron capacitación práctica sobre formas de eludir la censura y evitar la vigilancia. Las conferencias y debates fueron extraoficiales, pero el Centro Tow filmó y tomó notas para fines de investigación y se propuso redactar y difundir un informe sobre mejores prácticas en 2014.

Latinoamérica y el Caribe

Artículo 19 y la Fundación Fronteras Electrónicas han desarrollado memorándums que resumen los derechos de los blogueros, mientras que otras organizaciones están publicando información sobre los derechos que tienen los periodistas y otros actores que producen periodismo con tecnología digital, incluyendo el derecho a la privacidad y cuestiones de protección y acceso a datos.

2.4 Perspectiva de género en cuestiones de seguridad

Introducción

Según Irina Bokova, Directora General de la UNESCO, las mujeres periodistas a veces son víctimas de un "doble ataque", porque se convierten en objetivo tanto por ser mujer como por ser periodista.[154] De hecho, casi dos tercios de las periodistas encuestadas en un reciente estudio dijeron que habían sufrido actos de "intimidación, amenazas y abusos" en relación con su trabajo,[155] y casi la mitad de las encuestadas dijeron que habían sufrido acoso sexual[156] en sus empleos.[157] Las periodistas sufren de asaltos sexuales y violaciones que pueden producirse en represalia por su labor, durante eventos públicos por parte de multitudes o cuando están bajo arresto o cautiverio.[158]

El ámbito online a menudo refleja, y puede amplificar, las realidades y jerarquías que existen offline.[159] El abuso online en contra de mujeres es un fenómeno internacional en aumento, en formas que van desde acoso sexual a amenazas de violación y discurso de odio por motivos de género.[160] Entre 2000 y 2012, 72.5% de los incidentes de acoso recopilados por la organización estadounidense Trabajando para Detener el Abuso Online estuvieron dirigidos hacia mujeres.[161]

Investigadores del Departamento de Ingeniería Eléctrica y Computación de la Universidad de Maryland realizaron un experimento que encontró que las cuentas online que

tienen nombres femeninos reciben un promedio de 100 mensajes privados sexualmente explícitos o amenazantes al día, frente a un promedio de 25 para nombres ambiguos y de 3.7 con nombres masculinos.[162] Este estudio no estaba dirigido a periodistas, pero muestra cómo las mujeres en general pueden ser acosadas incluso sin ninguna interacción de su parte.[163]

Existen pruebas de varias mujeres periodistas y otras que contribuyen al periodismo que sufren acoso sexual en el mismo ámbito, amenazas violentas, discurso de odio por motivos de género y ciberacoso. Según un estudio del Instituto Internacional de Seguridad en las Noticias y la Fundación Internacional de Medios de Comunicación de Mujeres, más del 25% de las encuestadas afirmaron que habían recibido intimidación online verbal, escrita o física, incluyendo amenazas a familiares o amigos.[164]

La siguiente sección ofrece una discusión más detallada de este tema, incluyendo algunas campañas e iniciativas que buscan mitigar estos actos.

Amenazas y abusos digitales

Acoso sexual online, comentarios sexistas y amenazas con violencia

El acoso sexual online no ha sido bien definido, lo que hace difícil reconocer y responder a los casos. "La negativa a reconocer los perjuicios que afectan exclusivamente a las mujeres tiene un importante significado social: transmite el mensaje de que las conductas abusivas hacia las mujeres son aceptables y deberían tolerarse", afirma Danielle Keats Citron, profesora de la Facultad de Derecho de la Universidad de Maryland. A los perpetradores a menudo se les considera como "bromistas inmaduros" y las víctimas son vistas como "quejicas excesivamente sensibles".[165] Para responder a la falta de una definición clara y fomentar las oportunidades para rectificar, Citron clarifica las principales características de lo que ella llama "ciberacoso de género": 1) sus víctimas son mujeres, 2) el acoso está dirigido a mujeres concretas, y 3) el abuso implica la utilización del género de la mujer objetivo de forma sexualmente amenazante y degradante.[166] Citron cree que es fundamental reconocer el ciberacoso como discriminación de género y concientizar al público para garantizar que los relatos de las víctimas sean escuchados, persuadir a los perpetradores de que dejen sus invectivas online y modificar satisfactoriamente la subculturas online de la misoginia para promover la igualdad.[167]

Según Anja Kovacs, que dirige el Proyecto Democracia en Internet, las mujeres que escriben sobre política, religión, feminismo o sexualidad sufren más abusos online que aquellas que escriben sobre temas menos controvertidos.[168] Kavita Krishnan, comentarista y activista de la India, lo sabe de primera mano. Dice que el abuso se vuelve más mezquino cuando ella expresa sus opiniones políticas. Las amenazas han ido desde asaltos sexuales a la mutilación de genitales.[169]

Krishnan declaró a *The Observer*: "Las mujeres están sometidas a un tremendo discurso de odio. Por supuesto que siempre hay invectivas en política, pero esto está diseñado para intimidar a las mujeres".[170]

Según la columnista Laurie Penny, que escribe para el periódico londinense *The Independent*:

> Como escritora, llegas a suponer que te va a pasar, sobre todo si escribes sobre política. Llegas a esperar las invectivas, los insultos, las amenazas de muerte. Al cabo de un tiempo, los e-mails, los tuits y los comentarios de determinadas personas que se comunican a través de seudónimos y que te amenazan con fantasías demasiado gráficas sobre cómo y dónde y con qué utensilios de cocina les gustaría violarte, dejan de impactarte, y se vuelven simplemente una molestia diaria o semanal, algo sobre lo cual telefonear a tus amigas, buscando seguridad en la risa hueca.

> […] Muchas mañanas, cuando voy a revisar mis cuentas de e-mail, Twitter y Facebook, tengo que escudriñar a través de amenazas de violencia, especulaciones públicas sobre mis preferencias sexuales […] e intentos de desacreditación: puesto que yo y mis amigas somos tan poco atractivas, cualquier cosa que tengamos que decir debe ser irrelevante.[171]

Las mujeres periodistas que salen a la palestra online para escribir o discutir sobre política u otras cuestiones contenciosas a menudo alteran la imagen que algunos hombres tienen de las mujeres en términos más generales, lo que da lugar a que sean atacadas. Estos perpetradores probablemente esperan que las mujeres sean sumisas, y se creen en su derecho de utilizar medidas coercitivas para disciplinar a las mujeres que no actúan de forma servil.[172]

Comentarios sexistas hacia mujeres periodistas

Las mujeres periodistas a menudo reciben comentarios que se centran en la apariencia física más que en los logros profesionales.[173] Esto supone "una especie de clave visual que no puede realmente utilizarse de la misma forma para desestimar o menospreciar a un reportero varón", afirmó una periodista que se convirtió en objetivo.[174] Otra periodista observó que su marido, un conocido reportero al igual que ella, recibe virulentos ataques en Twitter por sus opiniones, pero que los comentarios no son de carácter sexualmente violento, como sí lo son contra ella.[175] Según Suzanne Franks, profesora de periodismo de la Universidad de la Ciudad de Londres y reciente autora de *Mujeres y periodismo*: "Cuando alguien no está de acuerdo con el artículo de un hombre, critican las ideas de su artículo; con las mujeres, critican su apariencia, su estilo, y los comentarios adoptan un tono muy personal".[176]

Un artículo del *New York Times* de enero del 2014 informaba que muchos de los argumentos que se estaban expresando en las audiencias públicas de Hawái en contra de los alimentos modificados genéticamente no tenían una base científica. Un grupo se disgustó por el artículo y respondió creando una imagen en la que pusieron digitalmente la cara de la autora sobre el cuerpo de una mujer en traje de baño de piel de leopardo. La imagen, subida en la página de Facebook de Democracia Alimentaria Ahora Food Democracy Now (FDN), mostraba a la periodista sonriendo en la playa, agarrándose de la mano con el director ejecutivo de una empresa de biotecnología y semillas.[177] La leyenda de la imagen decía: "Escritora del New York Times […] viaja a Hawái […] y se enamora de los GMOs [Organismos Genéticamente Modificados]". Poco después, varias personas publicaron comentarios burlándose de la autora con insultos sexistas. Después de que algunos miembros del grupo se quejaron de que la imagen de la autora creada por el grupo era incompatible con sus valores, otros miembros defendieron la imagen definiéndola como "una sátira, no sexismo".[178]

Amenazas de violación y otro tipo de violencia hacia las periodistas y sus familias

Las amenazas en contra de familiares de periodistas, sobre todo de violación o asesinato a las niñas, parecen ser más predominantes hacia mujeres profesionales de los medios de comunicación, y supuestamente son sumamente efectivas a la hora de silenciarlas.[179]

Una destacada presentadora de noticias de televisión de Latinoamérica que ha trabajado durante casi 20 años investigando el tráfico de personas, el tráfico de armas y las ejecuciones extrajudiciales, se ha enfrentado a reiteradas amenazas y acoso durante varios años. Sin embargo, no fue hasta que recibió llamadas telefónicas intimidatorias que amenazaban a su hijo pequeño, que se vio obligada a pedir un permiso para ausentarse de su programa matutino de periodismo de investigación.[180]

Otra periodista recibió una amenaza de bomba en Twitter al día siguiente de haber escrito un artículo que ponía de relieve la misoginia y el abuso online.[181] Otras periodistas

recibieron el mismo tipo de amenaza (incluso de periódicos como *The Independent*, *The Daily Telegraph* y *Time*). Se cree que estos ataques han estado vinculados a una campaña de amenazas violentas realizadas contra otra notoria periodista y miembro del parlamento que presionó con éxito para que la imagen de la novelista inglesa Jane Austen apareciera en los billetes de Reino Unido.

Una de las periodistas que se convirtió en objetivo dijo:

> Aquello materializó para mí algo que ya había sospechado, que era que el motivo de haber recibido la amenaza de bomba era por ser mujer. En cierta forma, aquello dio sentido a una situación sin sentido. […] Creo que la única cosa provocativa que hice fue ser mujer y estar en Twitter, y tener un perfil público, y tener opiniones.[182]

En otro caso, una cuenta de Twitter manejada con el nombre Tehreek e Taliban amenazó a renombradas periodistas pakistaníes, así como a otras, con una serie de tuits y en respuesta a sus opiniones. Por ejemplo: "Estos tuits deben dejar de vomitar contra los talibanes o las mataremos"; o, "No importa lo seguras que se sientan dentro de sus casas, recuerden que siempre tenemos acceso –Dejen la propaganda o prepárense para morir", etcétera.

En respuesta, algunas de las periodistas contactaron con un especialista en tecnología y capacitador en seguridad digital para que las ayudara a asegurar mejor sus comunicaciones digitales.[183]

Ciberacoso

El ciberacoso es cuando alguien utiliza comunicaciones electrónicas para rastrear y acosar reiteradamente a un individuo o grupo, sea online o a través de medios digitales.[184,185] Hay todavía cierto debate sobre si el ciberacoso es otra herramienta para individuos que se dedican al acoso tradicional o si debería existir como un concepto aparte con fines distintos.[186] Independientemente de cómo se defina, el ciberacoso, como otras formas de abuso, afecta principalmente a las mujeres.[187] Por ejemplo, una encuesta en la India encontró que las víctimas con edades comprendidas entre 18 y 32 años eran predominantemente mujeres.[188] En EUA, se cree que más de un millón de mujeres y 370 mil hombres son acosados anualmente. Una de cada 12 mujeres será acosada alguna vez en su vida, en comparación con uno de cada 45 hombres.[189] Según la Encuesta Nacional sobre Victimización Delictiva estadounidense, las mujeres constituyen el 58% de las víctimas en casos de ciberacoso,[190] y SeguridadCableada [WiredSafety], un grupo de seguridad online, encontró que las mujeres son los objetivos más probables de los ciberacosadores.[191]

Se espera que los casos de ciberacoso aumenten.[192] Esto puede deberse a diversos factores. En primer lugar, es relativamente fácil recopilar detalles a menudo íntimos sobre una persona, sobre todo si la víctima produce y difunde contenido revelador. Segundo, un atacante es capaz de rastrear a su víctima con bastante facilidad si la víctima no implementa prácticas de seguridad digital que protejan mejor su privacidad. Tercero, un atacante puede difundir información sobre la víctima a través de diversos medios online, llegando rápidamente a un público amplio y potencialmente cautivo. Cuarto, la distancia que proporciona la comunicación online fortalece el "efecto de desinhibición", lo que significa que las consecuencias percibidas de las acciones de un individuo, como abusar verbalmente de un objetivo o revelar detalles íntimos, se reducen drásticamente cuando el perpetrador no tiene los límites normales de decirle a su víctima algo a la cara y ver su reacción.[193] El efecto de desinhibición y la capacidad de mantenerse al menos parcialmente anónimo y potencialmente inimputable puede que influyan también en el grado al que un atacante acosa a su víctima, o su persistencia en hacerlo.

Una laureada periodista de televisión recibió e-mails abusivos de un acosador de quien ella sospecha que hackeó sus cuentas de e-mail privada y profesional. En los mensa-

jes, el acosador describe elementos de su hogar y nombres de familiares. A pesar de la ayuda prestada por expertos en seguridad y tecnología, se sintió obligada a cambiar sus cerraduras, instalar nuevos sistemas de seguridad en su casa y eventualmente mudarse de ciudad. Tras cinco años de acoso constante, dejó su trabajo, esperando que eso detuviera el acoso, pero el ciberacoso continuó.[194]

Consecuencias e importancia

El acoso online y el ciberacoso tienen numerosas consecuencias para sus víctimas, incluyendo las psicológicas, de conveniencia y costos financieros. Tras sufrir amenazas y abusos, las periodistas pueden preocuparse cada vez más por su seguridad personal y empezar a utilizar seudónimos cuando publican, o dejar de escribir por completo sobre una historia o tema. Otras pueden dejar de informar desde localidades específicas y se ven obligadas a reubicarse. Algunas periodistas tienen que abandonar el periodismo o abandonar sus empleos por completo.[195]

El acoso online puede también provocar importantes perturbaciones emocionales que conduzcan a trastornos psicológicos como la depresión.[196] Las periodistas quizá tengan que gastar dinero para pagar abogados mientras se enfrentan a perpetradores en un tribunal; también deven invertir en servicios de protección online que eliminen sistemáticamente la información personal de sitios web. Además, pueden sufrir pérdidas de ingresos por estar demasiado traumatizadas psicológicamente para continuar con su profesión.[197]

Las amenazas sexistas pueden también impactar en el bienestar de las mujeres.[198] En un estudio de estudiantes universitarias de EUA, muchas de las participantes reportaron un mayor nivel de enojo y depresión, y menor autoestima, a partir de su exposición a comportamientos sexistas.[199] Lo mismo puede aplicarse a la experiencia online y a mujeres que emplean Internet para hacer periodismo.

Asimismo, cuando se trata con grupos o foros, se pueden producir fenómenos de comportamientos en masa: individuos, al ver que otros atacan a alguien, se unen para ser parte del grupo.[200]

Campañas e iniciativas

Al menos un estudio, que implicaba a estudiantes universitarias de EUA, ha mostrado que hacer algo frente al sexismo reduce los prejuicios y la discriminación a largo plazo.[201] Otro estudio mostró que confrontar el sexismo en el ámbito offline hace que aquellas que alzan la voz se sientan mejor que las que eligen permanecer en silencio.[202]

Recientemente se encuentran coberturas por parte de los medios de comunicación con las que se han documentado diversas campañas lanzadas por mujeres en Twitter como respuesta al acoso y las amenazas online. En 2011, una escritora feminista inició un *hashtag* de Twitter, #MenCallmeThings, para documentar el acoso y las amenazas. Dedicó un sitio web a registrar las experiencias de las mujeres y encontró que “los hombres están utilizando los mismos insultos y sentimientos para ignorar a las mujeres y a las personas ‘femeninas’ en todas partes… es un tema de género”.[203] La campaña concientizó sobre los diferentes tipos de amenazas que las mujeres enfrentan online. Otra periodista creó el *hashtag* #silentnomore, que inició para animar a las mujeres a expresarse acerca de sus experiencias y confrontar los comentarios generalizados y maliciosos.[204] Blogueras de Egipto, Sudán, Siria y Líbano han animado a las personas a denunciar el acoso y la violencia de género utilizando el *hashtag* #EndSH en Twitter. Además, se han creado campañas para confrontar el sexismo y la misoginia, como #ShoutingBack y #MisogynyAlert, que permiten a cualquiera llamar la atención sobre el abuso verbal y responder a los perpetradores.[205]

Un proyecto de investigación en Tumblr, llamado “Dicho a Damas Periodistas” (Said to Lady Journos), consiste en un catálogo de comentarios anónimos hacia mujeres periodistas. Estas campañas resultan útiles porque buscan cambiar la norma existente de lo

que se percibe como aceptable, al tratar de trasladar la responsabilidad de la abusada a los abusadores.

Otra campaña que se esfuerza por reducir la violencia de género contra mujeres es la campaña colaborativa "Reclama la Tecnología" (Take Back the Tech), que empezó en enero del 2009 y pretende reivindicar las tecnologías de la información y las comunicaciones para poner fin a la violencia contra las mujeres.[206] La campaña aporta importantes recursos a 12 países en desarrollo para documentar violaciones online de los derechos de las mujeres, proporciona desarrollo de capacidades para activistas y supervivientes en el uso creativo y seguro de la tecnología, y aboga por políticas para fortalecer la protección de los derechos online. El proyecto forma parte de un esfuerzo global para lograr la igualdad de género, según se planteó en los Objetivos de Desarrollo del Milenio de las Naciones Unidas.[207] La campaña tiene lugar durante el evento "16 Días de Activismo Contra la Violencia de Género" (del 25 de noviembre al 10 de diciembre de cada año).

La campaña apela a todos los usuarios de Tecnologías de la Información y las Comunicaciones (TIC), pero especialmente a mujeres y niñas, para que asuman el control de la tecnología utilizando estratégicamente las plataformas TIC (i.e. teléfonos celulares, blogs, etcétera) para un activismo contra la violencia de género. Pretende:

- Crear espacios digitales seguros que protejan el derecho de todas a participar libremente, sin acoso o amenazas a la seguridad;
- Hacer realidad los derechos de las mujeres para dar forma, definir, participar, utilizar y compartir conocimientos, información y TIC;
- Abordar la intersección entre derechos a la comunicación y derechos humanos de las mujeres, sobre todo frente a la violencia contra las mujeres; y
- Reconocer la participación histórica y crucial de las mujeres y su contribución al desarrollo de las TIC.

El artículo de Reclama la Tecnología, "Ciberacoso y cómo prevenirlo"[208] es un buen recurso sobre las formas de prevenir el ciberacoso. Reclama la Tecnología cuenta también con un proyecto de mapeo que documenta el acoso, las amenazas y el abuso.[209] Otra iniciativa centrada en concientizar sobre el acoso sexual es Harassmap, que recopila SMS y reportes online de acoso y asalto sexual y los ubica en Harassmap. Utiliza información y análisis de esta investigación para crear campañas de comunicación que aborden el acoso y asalto sexual. Al hacerlo, Harassmap busca ahuyentar los mitos y estereotipos sobre el acoso y asalto sexual, cambiar las percepciones que echan la culpa a la acosada/asaltada y movilizar a las personas para hacer frente al acoso.[210]

Responsabilidad corporativa

Los sitios web de redes sociales y blogs están construidos de forma tal que fomentan la libertad de expresión. Como tales, conllevan un riesgo inherente de uso indebido por parte de actores que busquen acosar o ciberacosar. En lugar de restringir arbitrariamente la libertad de expresión, las redes sociales y los blogs deberían asegurarse de ofrecer a sus clientes términos de uso claros y oportunidades de reparar el daño a las mujeres victimizadas. Dos organizaciones que han dado pasos en esta dirección incluyen a Tumblr y Twitter, aunque puede que haya muchas más. El acuerdo de términos de servicio más explícito de Tumblr,[211] que aporta un resumen de lo que es aceptable y lo que no, puede resultar disuasorio en algunos casos.[212] Los botones de bloqueo y "reportar abuso" de Twitter permiten a los usuarios tener más control sobre el contenido dirigido a ellos.

Aunque las corporaciones tienen un papel que desempeñar a la hora de mitigar los abusos en sus plataformas de usuarios, es importante que los periodistas y otros mejo-

ren su alfabetización digital para entender cuántos datos e información personal están compartiendo en redes sociales y blogs. Un estudio ha mostrado que los individuos en general siguen percibiendo que los beneficios de las redes sociales pesan más que los riesgos de revelar información personal. El estudio encontró también una discrepancia entre el entendimiento y precaución reportados por los usuarios con respecto a la privacidad, y la implementación real de medidas específicas para mantener la privacidad. Las personas pueden manifestar que están familiarizadas con las configuraciones de privacidad, pero siguen manifestando conductas (como aceptar en sus redes a personas a quienes no conocen), que ponen en riesgo su privacidad.

En general, tienen que realizarse más investigaciones sobre las formas de abuso online que enfrentan las mujeres periodistas. Estudios de caso y hallazgos de investigaciones a pequeña escala apuntan a que las periodistas se convierten en blancos particulares como reflejo de la jerarquía de poder offline. Sin embargo, un estudio cuantitativo centrado en este tema proporcionaría claves más profundas sobre los fenómenos que aquejan a las mujeres periodistas y apuntaría a algunas posibilidades para la mitigación de estas amenazas.

3. DESAFÍOS Y RECOMENDACIONES

3.1 Introducción

Esta sección del informe identifica desafíos específicos que enfrentan los actores periodísticos que interactúan con la tecnología digital y ofrece recomendaciones concretas a la serie diversa de actores implicados. La protección del periodismo conlleva acciones en tres niveles: a) poder estatal, b) políticas de las instituciones de medios de comunicación, y, c) el comportamiento de individuos y sus asociados. Las recomendaciones que vienen a continuación ponen de relieve el potencial de las siguientes organizaciones e individuos:

- Organismos de las Naciones Unidas,
- Organizaciones internacionales (gubernamentales y no gubernamentales),
- Organizaciones regionales,
- Gobiernos,
- Corporaciones,
- Agencias de noticias,
- Escuelas de periodismo y otras instituciones educativas y de capacitación,
- Asociaciones de periodistas, y
- Periodistas y otros que contribuyen al periodismo.

El objetivo último de estos desafíos es mejorar la seguridad y la protección de todos aquellos que contribuyen al periodismo. La cuestión de la seguridad digital es compleja porque se extiende a lo largo de toda la cadena de valor de las comunicaciones digitales. Desde los dispositivos a la infraestructura utilizada para transmitir y almacenar datos, incluye también las entrevistas electrónicas y la investigación, así como la transmisión de datos, la publicación y la interacción. Ello no significa que se trate de un ámbito puramente digital; por ejemplo, los dispositivos pueden ser robados o destruidos físicamente, no simplemente estar sujetos a robo o perturbación electrónica. Los datos de localización y redes sociales pueden utilizarse para determinar el objetivo y el momento oportuno para ataques físicos.

Las dimensiones de la seguridad son muchas, y abarcan aspectos tan diversos como el tecnológico, el institucional y el económico, así como el político, el jurídico y el psicosocial.

3.2 Desafíos y recomendaciones[213]

1. Desafíos tecnológicos, institucionales y económicos

Los periodistas y otros que contribuyen al periodismo se enfrentan a diversos desafíos tecnológicos cuando llevan a cabo su labor. Éstos pueden ir desde los prácticos –como la limitada utilización de las herramientas de seguridad digital o la falta de un modelo de financiación sostenible para apoyar la compra regular o la actualización de herramientas de seguridad digital– hasta los más complejos, como soportar los ataques y amenazas digitales propiamente dichas.

Desafío 1.1: Algunas herramientas de seguridad digital no son fáciles de usar, lo que puede llevar a que pocos periodistas adopten o implementen las herramientas correctamente o lo hagan en absoluto. Por consiguiente, los investigadores sugieren las siguientes recomendaciones:

- **Recomendación** (corporaciones y otros): Animar a corporaciones y especialistas en tecnología de fuente abierta a construir herramientas útiles a nivel de consumidor y seguridad incorporada.

- **Recomendación** (organizaciones internacionales): Seguir concientizando sobre las amenazas en constante evolución que enfrentan los periodistas que interactúan digitalmente, con el fin de estimular la demanda de herramientas de seguridad digital.

Desafío 1.2: La vigilancia, la capacidad de almacenamiento de datos y las tecnologías para ataques digitales se han vuelto menos caras y más comunes. En respuesta, ha habido un mayor debate entre las principales partes interesadas sobre el desarrollo de protocolos para encriptar el tráfico en Internet en sentido más amplio.

- **Recomendación** (corporaciones): Considerar ampliamente el desarrollo de encriptación de extremo a extremo para los servicios que ofrecen.

- **Recomendaciones** (corporaciones):

    - Garantizar que las páginas web y otros servicios permitan la encriptación por defecto (SSL/TLS), con el fin de proporcionar siempre a los usuarios una versión segura de su sitio web.

    - Encriptar la transferencia de datos de clientes entre centros de datos, no sólo entre un centro de datos y la computadora del usuario.

    - Utilizar “confidencialidad directa perfecta” (PFS), la cual usa claves efímeras generadas al azar. Esto evita que un cuerpo extraño sea capaz de desencriptar la comunicación, aunque logre obtener la clave secreta para tráfico encriptado, debido a que no cuenta con la clave de la sesión específica. La confidencialidad directa perfecta es quizá incluso más importante tras la divulgación del bug Heartbleed, que amenazó la seguridad de los protocolos HTTP en la web.

    - Autenticar y encriptar los canales de descargas cuando se proporcionan servicios de actualización de *software* para evitar que estas actualizaciones sean secuestradas y utilizadas para descargar *malware*.

    - Aumentar la transparencia y proporcionar términos de uso claros para servicios que recopilan datos de usuarios. Aunque la recopilación de datos supone un modelo de negocio para muchas corporaciones, procurar minimizar y anonimizar la recopilación de datos a partir de servicios.

- Considerar el desarrollo de más tecnologías de fuente abierta para facilitar la transparencia y ayudar a garantizar que el código de producto no haya sido debilitado por parte de gobiernos u otras entidades.

- **Recomendación** (todas las partes interesadas): Utilizar y promover el uso de tecnologías de encriptación de fuente abierta, como HTTPS Everywhere, de modo que faciliten canales más seguros.

Desafío 1.3: Los actores periodísticos a menudo no pueden permitirse *software* comercial que proporcione seguridad digital; por tanto, tienen que depender de tecnologías de fuente abierta que son gratuitas. Sin embargo, las tecnologías de seguridad digital de fuente abierta a menudo se conceptualizan y desarrollan sin la posibilidad de una financiación sostenible, haciendo problemático su uso si carecen de financiación para mantenerse actualizadas contra vulnerabilidades.

- **Recomendación** (todas las partes interesadas): Animar a los donantes a proporcionar fondos u otros recursos para ayudar a facilitar el mantenimiento y actualización de herramientas de seguridad digital de fuente abierta para periodistas y defensores de los derechos humanos, lo que ayudará a garantizar que estas tecnologías se mantengan disponibles y actualizadas. Aunque los desarrolladores que trabajan en tecnología de fuente abierta generalmente lo hacen de forma voluntaria, los recursos dirigidos a ayudar a que el proyecto se vuelva sostenible ayudarían a garantizar que los periodistas y defensores de los derechos humanos puedan utilizar herramientas de fuente abierta actualizadas y verificables.

Desafío 1.4: Los ataques DoS pueden dar lugar a pérdidas financieras para agencias de noticias o periodistas en particular.

- **Recomendación** (organizaciones internacionales y gobiernos): Ayudar a financiar a aquellas organizaciones que proporcionan apoyo gratuito a periodistas y agencias de noticias que enfrentan ataques DoS.

- **Recomendación** (agencias de noticias e instituciones de periodismo): Contratar administradores de sistemas que tengan conocimientos sobre estrategias de mitigación con el fin de limitar o evitar los perjuicios ocasionados por ataques DoS.

Desafío 1.5: Muchos de quienes se desempeñan en el periodismo digital no conocen a especialistas en tecnología dispuestos a ayudarlos si sufren una amenaza o ataque digital, y muchos de estos especialistas que sí están dispuestos a ayudar a los periodistas no saben cómo contactar a aquellos que necesitan ayuda.

- **Recomendación** (organizaciones internacionales, agencias de noticias, escuelas de periodismo y organizaciones educativas y de capacitación): Contratar a especialistas de planta que puedan proporcionar asistencia de respuesta inmediata a los agentes de medios de comunicación que sufren ataques digitales o establecer contacto con centros o especialistas locales que puedan ayudar.

- **Recomendación** (organizaciones internacionales): Considerar el proporcionar una línea directa para seguridad digital que enlace a periodistas con especialistas en tecnología en diferentes áreas de todo el mundo, proporcionando asistencia 24 horas los 365 días del año.

- **Recomendación** (ONG de libertad de prensa y organizaciones internacionales): Apoyar la creación de una comunidad internacional de expertos en seguridad de medios de la que puedan hacer uso las agencias de noticias y los periodistas.

Desafío 1.6: Una falta de datos disponibles públicamente que documenten los tipos de ataques y amenazas digitales que enfrentan los periodistas y otros que hacen periodismo.

- **Recomendación** (organizaciones internacionales): Desarrollar una base de datos integral y anonimizada que catalogue el número y el tipo de ataques digitales contra periodistas.

- **Recomendación** (Naciones Unidas y organizaciones internacionales): Desarrollar indicadores para medir cómo los actores periodísticos que interactúan con tecnología digital están siendo amenazados y atacados, incluyendo amenazas digitales y amenazas transmitidas digitalmente, con el fin de crear mejores estrategias para informarlos y protegerlos.

Desafío 1.7: La tecnología de rastreo de localizaciones puede identificar a los periodistas y sus fuentes, con el objetivo de acabar con su confidencialidad entre ellos o para organizar ataques físicos.

- **Recomendación** (organizaciones internacionales, instituciones de capacitación en periodismo y agencias de noticias): Instruir a los periodistas que interactúan digitalmente sobre cómo inhabilitar el rastreo de localizaciones en sus dispositivos electrónicos (aunque los dispositivos con baterías que no pueden quitarse pueden no ofrecer esta posibilidad). Los profesionales deberían estar conscientes sobre cómo las aplicaciones y sitios web pueden geolocalizar de forma sigilosamente.

Desafío 1.8: La seguridad digital, tanto de aquellos que hacen periodismo como de sus asociados (fuentes, familias y colegas), puede a menudo verse comprometida fácilmente mediante campañas de *phishing*.

- **Recomendación** (agencias de noticias e instituciones de periodismo): Proporcionar capacitación regular para periodistas y otros sobre mejores prácticas en seguridad digital; además, crear una cultura de aprendizaje sobre una sólida seguridad de la información para reducir riesgos.

Desafío 1.9: Las cuentas de usuario y dispositivos comprometidos pueden utilizarse para identificar a las fuentes y redes de quienes hacen periodismo, llevando a una mayor inseguridad para los periodistas y sus fuentes.

- **Recomendación** (agencias de noticias, organizaciones internacionales e instituciones de periodismo): Capacitar a los periodistas sobre cómo asegurar sus laptops y otros dispositivos electrónicos en caso de que sean confiscados o robados. Enseñar a los periodistas cómo instalar y utilizar regularmente tecnologías para ocultar información sensible en sus dispositivos electrónicos de acuerdo con el tipo de amenaza al que se puedan enfrentar.

- **Recomendación** (corporaciones): Considerar ofrecer autenticación de dos factores para evitar un *hacking* no autorizado en los datos de usuario –por ejemplo, contraseña y mensaje de texto–, teniendo en cuenta que un teléfono inteligente puede invalidar dichos sistemas al combinar servicios en un único dispositivo.

2. Desafíos políticos y/o jurídicos

Cualquier impedimento legítimo a la libertad de expresión o la privacidad debe ser estrictamente definido, proporcionado y justificado para garantizar que quienes hacen periodismo puedan seguir desempeñando su labor proporcionando y difundiendo información que ayude a informar a la sociedad y al gobierno. Desafortunadamente, existen muchas leyes y políticas rigurosas con interpretaciones excesivamente amplias que pueden servir para restringir indebidamente la libertad de expresión y la privacidad. Además, las leyes y las políticas públicas no van al ritmo acelerado del cambio tecnológico, lo que genera huecos en la protección de los periodistas. Los desafíos políticos y jurídicos que ellos enfrentan incluyen leyes ambiguas y opacas en torno a la retención de datos y la vigilancia, pocos controles a la exportación de tecnologías que se han

utilizado para reprimir derechos humanos y una falta de voluntad política para abordar los delitos contra ellos.

Tras las revelaciones que en 2013 sorprendieron al mundo sobre el espionaje que algunos Estados ejercen sobre los habitantes del mundo, el público, los actores políticos, los periodistas y las agencias de noticias han mostrado un creciente interés en los conocimientos, las herramientas y los cursos de capacitación en seguridad digital; sin embargo, tiene que producirse más concientización y consolidación normativa a nivel global para garantizar que los periodistas y otros que contribuyen al periodismo tengan un respaldo contextual para llevar a cabo su labor de la forma más segura posible.

Esta sección resumirá estos desafíos y propondrá recomendaciones para mitigarlos.

Desafío 2.1: Tienen que aumentarse los niveles de conocimientos y la capacidad de defensa para la implementación de estándares políticos y jurídicos referentes a la seguridad digital.

- **Recomendación** (todas las partes interesadas): Mantenerse al tanto de las evoluciones en los estándares internacionales, como resoluciones del Consejo de Derechos Humanos de las Naciones Unidas, iniciativas de la sociedad civil (por ejemplo, Necessaryandproportionate.org) y medidas por parte del sector (por ejemplo, la Iniciativa para Redes Globales). Utilizar éstos para esfuerzos de defensa con el fin de que se promocione y respete la importancia de la seguridad digital.

- **Recomendación** (gobiernos): Se debería tomar conciencia de las resoluciones de la Asamblea General de las Naciones Unidas sobre el Derecho a la Privacidad en la Era Digital.[214] Éstas llaman a los estados a "revisar sus procedimientos, prácticas y legislación referente a la vigilancia de las comunicaciones y su interceptación, y a la recopilación de datos personales, incluyendo vigilancia, interceptación y recopilación masiva, con vistas a defender el derecho a la privacidad". Llaman además a todos los Estados a establecer o mantener mecanismos existentes de supervisión doméstica independientes, eficaces, suficientemente dotados e imparciales, capaces de garantizar la transparencia, según corresponda, y la rendición de cuentas para la vigilancia de comunicaciones por parte de Estados, su interceptación y la recopilación de datos personales. También se debería tomar conciencia de la resolución 37 C/52 de la UNESCO, la cual menciona que "la privacidad es fundamental para proteger a las fuentes periodísticas, lo que permite que una sociedad se beneficie del periodismo de investigación, para fortalecer la buena gobernanza y el estado de derecho, y que dicha privacidad no debería estar sujeta a interferencias arbitrarias o ilícitas".[215]

Desafío 2.2: Las tecnologías de vigilancia en ocasiones son exportadas a países con malos historiales de derechos humanos y supuestamente utilizadas para convertir en objetivo a agentes periodísticos y miembros de la sociedad civil.

- **Recomendación** (gobiernos): Monitorear la clasificación de tecnologías de vigilancia conforme a los acuerdos de Wassenaar y actuar en consecuencia.

- **Recomendación** (organizaciones internacionales de protección a la prensa/libertad de prensa): Abogar para que los gobiernos y otros actores tomen en consideración los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.

- **Recomendación** (organizaciones internacionales): Animar a las empresas para que hagan pública la lista de los países a los que venden tecnologías de vigilancia.

- **Recomendación** (corporaciones): Comprometerse a no vender tecnologías de vigilancia a clientes allí donde podría abusarse de éstas.

- **Recomendación** (organizaciones regionales y gobiernos): Incorporar la promoción y protección de los derechos humanos online en las relaciones exteriores, incluyendo programas de desarrollo y asistencia, negociaciones de acuerdos comerciales y procesos de licitación pública donde corresponda.

Desafío 2.3: Falta de voluntad política para abordar los delitos contra quienes hacen periodismo digital, lo que da como resultado un clima de impunidad.

- **Recomendación** (gobiernos): Como prerrequisito, condenar rotundamente todos los ataques y violencia contra periodistas y trabajadores de medios de comunicación, según se plantea en la Resolución sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad de las Naciones Unidas, adoptada en diciembre de 2013.[216]

- **Recomendación** (Naciones Unidas y organizaciones internacionales): Seguir abogando porque los gobiernos eviten los ataques contra periodistas y quienes contribuyen al periodismo. Fomentar investigaciones completas, imparciales y prontas por parte de funcionarios y analistas, según corresponda a la situación, y de acuerdo a las leyes nacionales e internacionales.

- **Recomendación** (gobiernos): Crear mecanismos nacionales monitoreados de forma independiente que promuevan la transparencia, la rendición de cuentas y los procesos judiciales en lo referente a ataques contra periodistas, incluyendo ataques digitales, y reportar sobre el seguimiento judicial en casos de ataque letal, de acuerdo a la solicitud de la Directora General de la UNESCO bajo mandato de los Estados Miembros de la Organización.

Desafío 2.4: La integridad y seguridad de las redes debería respetarse y protegerse, y las vulnerabilidades repararse en lugar de explotarse.

- **Recomendación** (gobiernos): Las autoridades deberían abstenerse de explotar vulnerabilidades y de crear "puertas traseras", puesto que dichas acciones pueden permitir abusos, excesos y oportunidades para que otros actores entren a los sistemas informáticos.

- **Recomendación** (gobiernos): Allí donde los proveedores de servicios de Internet, incluyendo los operados por empresas de telecomunicaciones estatales, sean manipulados para redireccionar a los usuarios hacia sitios web con contenido falso y sitios web que contienen *malware*, los gobiernos deberían emprender acciones para detener esto.

Desafío 2.5: Los ataques digitales, incluyendo la vigilancia y el *malware* dirigido, son difíciles de atribuir, lo que conduce a una mayor impunidad de los atacantes.

- **Recomendación** (organizaciones internacionales): Fomentar la financiación de organizaciones que tengan la capacidad técnica para analizar ataques digitales.

- **Recomendación** (escuelas de periodismo e instituciones educativas): Animar a los estudiantes de periodismo a mejorar su experiencia en seguridad digital y análisis de *malware* para empoderarse y combatir las amenazas y ataques digitales.

- **Recomendación** (Naciones Unidas): Instar a los gobiernos a aumentar la transparencia en torno a la exportación de sistemas de vigilancia.

- **Recomendación** (periodistas): Si se sospecha de un ataque digital, enviar los equipos a reconocidos especialistas en seguridad digital para que sean analizados. Ellos pueden identificar el *malware*, limpiar el dispositivo y utilizar la muestra identificada para mejorar el *software* de detección.

Desafío 2.6: Enormes cantidades de datos pueden almacenarse y extraerse fácilmen-

te para poner al descubierto las redes y fuentes de los agentes de los medios de comunicación.

Recomendación (corporaciones y gobiernos): Revisar las políticas de retención de datos con vistas a la privacidad y la minimización de datos relacionada con cuentas de clientes (por ejemplo, limitar el periodo que se guardan los datos y registros de actividad y reforzar la seguridad contra el *hacking*).

Recomendación (corporaciones): Cuando corresponda, combatir las solicitudes irrazonables de datos por parte de gobiernos u otros en busca de información personal de usuarios. Asimismo, solicitar consejo a reputadas organizaciones sin ánimo de lucro. Hacerlo puede dar lugar a una mayor concientización pública sobre cuestiones de privacidad y que se establezcan normas para la transparencia.

Desafío 2.7: Las sanciones pueden dar como resultado una limitada disponibilidad de tecnología o de actualizaciones, necesarias para que los agentes periodísticos se mantengan seguros.

Recomendación (Naciones Unidas y gobiernos): Evaluar el costo de las sanciones tanto desde la perspectiva de los derechos humanos como desde la perspectiva de la seguridad, teniendo en cuenta las potenciales consecuencias.

3. Psicosociales

Los actores periodísticos que no conocen mejores prácticas en seguridad digital podrían encontrarse exponiendo inconscientemente a sus fuentes, aunque realicen una estricta seguridad operativa. Sin embargo, los agentes periodísticos, incluyendo las organizaciones de medios de comunicación, también tienen que responsabilizarse de garantizar la adopción de una mentalidad de seguridad para sus actividades periodísticas.

La seguridad operativa y digital no puede ser un añadido de último minuto a su labor. Por el contrario, necesitan adoptar una postura que garantice la protección de su cadena de comunicaciones y de sus redes. Al hacerlo, los agentes de los medios de comunicación necesitan adoptar un nivel de seguridad adecuado, de modo que no se queden paralizados ante la indecisión.[217]

El problema es que muchos periodistas y productores de periodismo online desconocen las amenazas a la seguridad digital que pueden enfrentar cuando reportan o difunden información. Otros puede que se sientan abrumados por el ritmo acelerado del cambio tecnológico y la necesidad de adaptarse continuamente a nuevas redes de distribución, modelos de negocio y amenazas a la seguridad digital.[218] Las herramientas de seguridad digital a menudo resultan complejas y no son fáciles de usar. La falta de herramientas fáciles de usar, junto con la abrumadora cantidad de información sobre los riesgos y las diferentes herramientas a utilizar, puede dar lugar a una incertidumbre que produzca fatiga y un enfoque de todo o nada. Sumándose a la confusión, hay una falta de entendimiento fundamental sobre cómo funcionan las comunicaciones y las redes digitales. Es más fácil para los productores de periodismo no implementar herramientas de seguridad digital si las repercusiones no resultan obvias o parecen improbables. Los periodistas enfrentan muchos desafíos, incluyendo una falta de entendimiento sobre cómo la "higiene digital" puede afectar a la seguridad física y el bienestar psicológico, y también sobre cómo las experiencias traumáticas no resueltas pueden reducir la capacidad de un periodista para realizar con éxito prácticas de seguridad física y digital.

Desafío 3.1: Los periodistas puede que apliquen indebidamente o eviten implementar herramientas de seguridad digital porque no son conscientes en general de las amenazas, o no son conscientes de la conexión entre la higiene en seguridad digital y la seguridad física y bienestar psicológico. También puede que carezcan de herramientas de seguridad digital fáciles de usar.

- **Recomendación** (organizaciones internacionales, escuelas de periodismo e instituciones educativas y de capacitación): Garantizar que la capacitación en seguridad digital sea integral e incluya seguridad operativa y atención psicosocial. Incluir también una perspectiva sensible al género y sensible al trauma durante la capacitación para acceder a periodistas que hayan sufrido eventos traumáticos relacionados con su seguridad, o que debido a su género no hayan recibido capacitación anteriormente.

- **Recomendación** (corporaciones): Recordar a los usuarios establecer las configuraciones de seguridad de sus cuentas para garantizar una navegación más segura, recibir notificaciones de acceso para sus cuentas y explicarles cómo pueden monitorear la actividad de sus cuentas.

- **Recomendación** (corporaciones): Encriptar los programas de *software*, aplicaciones y otras tecnologías por defecto.

Desafío 3.2: Muy pocos actores de medios de comunicación online entienden los principios de seguridad digital o su aplicación.

- **Recomendación** (actores periodísticos): Un punto de partida lógico para cualquier práctica de seguridad digital es realizar una evaluación de riesgos individualizada y desarrollar un plan de seguridad para llevarla a cabo, con el fin de garantizar una práctica de higiene digital razonable y viable.[219]

- **Recomendación** (Naciones Unidas, organizaciones internacionales, gobiernos, periodistas y escuelas de periodismo): Considerar la integración de lo que la UNESCO llama Alfabetización Mediática e Informacional (MIL) como una competencia fundamental para los ciudadanos, junto con otras alfabetizaciónes.[220] Hacerlo contribuirá a informar y empoderar a los agentes periodísticos que interactúan con tecnología digital para que hagan uso y protejan sus derechos y libertades. En un nivel más amplio, la UNESCO ha realizado una labor considerable a la hora de desarrollar el "Marco de Evaluación para la Alfabetización Mediática e Informacional Global", el cual proporciona un marco conceptual y teórico y ofrece la lógica y metodología para realizar una evaluación de la preparación de un país y sus competencias a nivel nacional. Esta información es relevante no sólo para el periodismo, sino para todos los usuarios públicos de comunicaciones digitales. El marco puede ayudar a los Estados Miembros de la UNESCO a monitorear la eficacia de las prácticas y políticas actuales, y a diseñar planes orientados a acciones que estén relacionadas con contextos y condiciones específicas de cada país. Un público con experiencia en MIL es sumamente benéfico para los periodistas, incluso a través de medios digitales. Por este motivo, los periodistas y capacitadores en seguridad digital tienen interés particular en fomentar prácticas seguras en el conjunto de la sociedad.

- **Recomendación** (organizaciones internacionales, agencias de noticias, escuelas de periodismo e instituciones educativas y de capacitación): Proporcionar un marco general que explique cómo funcionan las redes y comunicaciones digitales, y mapear cómo determinadas acciones por parte de productores digitales de periodismo podrían acarrear inseguridad.

- **Recomendación** (agencias de noticias): Proporcionar capacitación en seguridad digital a periodistas, con el fin de mitigar la amenaza de *phishing* y otros ataques.

- **Recomendación** (agencias de noticias): Adoptar una cultura favorable a la seguridad de la información y fomentar prácticas de higiene digital.

- **Recomendación** (agencias de noticias y periodistas): Compartir más información sobre riesgos y capacitación en seguridad digital entre colectivos de medios de comunicación, agencias de noticias, periodistas independientes y otros productores online de periodismo (por ejemplo, ofrecer links en su sitio web a recursos

como el CPJ, Fondo Rory Peck, etcétera, para dar a conocer a quienes hacen periodismo qué recursos de seguridad digital son relevantes y están disponibles).

- **Recomendación** (agencias de noticias): Animar a los actores de medios de comunicación a compartir entre pares recomendaciones sobre seguridad digital.

- **Recomendación** (agencias de noticias y periodistas): Formar redes o asociaciones para plantear posiciones consolidadas sobre políticas y actos que impacten la seguridad digital y la legislación que protege la seguridad del periodismo digital y los actores de medios de comunicación, sus fuentes y su labor en todas las plataformas.

- **Recomendación** (agencias de noticias): Invertir en recursos para seguridad online, incluyendo contratar a tecnólogos de planta que puedan ayudar a detectar y analizar *malware* y otras preocupaciones para la seguridad digital.

- **Recomendación** (organizaciones internacionales): Proporcionar a los reporteros autónomos y otros actores informales que generan periodismo los recursos y conocimientos necesarios para reportar o archivar historias de ubicaciones que no comprometen su seguridad.

- **Recomendación** (agencias de noticias): Capacitar a periodistas sobre formas de subir archivos de forma segura y protegida.

- **Recomendación** (agencias de noticias y periodistas): Mantener la propiedad sobre el nombre del dominio bloqueando su transferencia y procurar elegir un registro de dominios que no sea vulnerable a las interferencias.

- **Recomendación** (actores periodísticos y agencias de noticias): Proporcionar comentarios específicos a los especialistas en tecnología sobre herramientas de seguridad digital: lo que funciona, lo que es demasiado complicado y por qué.

- **Recomendación** (actores periodísticos): Convertir en un hábito la higiene digital y mantenerse al tanto de las cambiantes amenazas.

- **Recomendación** (actores periodísticos): Concientizar sobre mejores prácticas de seguridad de la información entre colegas y fuentes.

Desafío 3.3: La mayoría de las fuentes de periodistas no están versadas en utilizar la encriptación u otras formas de comunicaciones seguras.

- **Recomendación** (agencias de noticias y actores periodísticos): Adoptar tecnologías seguras para compartir información y archivos, que permitan una comunicación anónima y encriptada de las fuentes al periodista en el sitio web de una agencia de noticias o un bloguero. Las fuentes necesitan ser instruidas acerca de los riesgos de la comunicación digital.

Desafío 3.4: Las experiencias traumáticas pueden dar lugar a que quienes hacen periodismo tomen decisiones equivocadas que conduzcan a una mayor inseguridad.

- **Recomendación** (organizaciones internacionales, agencias de noticias, escuela de periodismo e instituciones educativas y de capacitación): Garantizar que los actores periodísticos entienden el vínculo entre seguridad digital y física, y animarlos a implementar regularmente buenas prácticas.

Lineamientos para agentes de medios de comunicación que hacen periodismo en un contexto digital

En general, todos los agentes periodísticos que interactúan con tecnología digital deberían:

1. Desarrollar un plan de evaluación de riesgos o "modelo de amenazas" y desarrollar un plan de seguridad personal con herramientas y técnicas necesarias para implementarlo satisfactoriamente.

2. Reconocer que la seguridad supone siempre un sacrificio de recursos y priorizar necesidades de seguridad basadas en una evaluación de riesgos individualizada; evitar los extremos de paranoia por un lado y la sensación de inutilidad por el otro.

3. Entender que la seguridad digital y física están vinculadas y adoptar medidas para mejorar ambas.

4. Tratar la higiene digital como un hábito y una práctica.

5. Entender que lo caro no siempre resulta mejor. Los periodistas deberían considerar la implementación de tecnologías de fuentes abiertas y otras tácticas sencillas.

6. Darse cuenta de que la seguridad digital está cambiando constantemente. Hay una necesidad de mantenerse actualizado y de entender las virtudes y defectos de navegadores, proveedores de e-mail, medios sociales, *software* y *hardware*.

4. Capacitación en seguridad digital

Los capacitadores en seguridad digital deberían abordar la capacitación de manera integral e incluir capacitación normativa, psicosocial y física junto con la capacitación digital, debido a que todos los componentes resultan esenciales para sintetizar las muchas dimensiones de la seguridad. También es importante garantizar que quienes hacen periodismo conozcan las normas sobre seguridad digital y libertad de expresión, además de poder garantizar que su seguridad operativa o su estado psicosocial no comprometan sus prácticas de seguridad digital.

Además, los capacitadores deberían subrayar la importancia de los comportamientos cambiantes que ponen en riesgo a personas y datos. También deberían enfocarse en una planeación de contingencias y en protocolos de seguridad. Todo esto además de las herramientas específicas que pueden mantener segura la labor periodística.[221]

Desafío 4.1: La capacitación en seguridad digital a menudo se enseña según sea necesario, si es que se hace en absoluto, y tiene que ser más sistemática e integral para que sea eficaz para los periodistas.

- **Recomendaciones** (agencias de noticias, organizaciones internacionales e instituciones de periodismo):

    - Enseñar seguridad digital de manera integral. Por ejemplo, incluir consideraciones de seguridad física y psicológica cuando la seguridad digital se interrelacione con ambas.

    - Incluir una visión general de Internet y de las redes en los cursos de capacitación en seguridad digital para establecer satisfactoriamente el contexto para preocupaciones de seguridad digital.

    - Utilizar un enfoque equilibrado y amigable hacia la enseñanza. Evitar un lenguaje excesivamente técnico, que puede abrumar al periodista y llevarle a no implementar herramientas y técnicas digitales.

    - Fomentar la investigación sobre mejores prácticas de los cursos de capacitación en seguridad digital.

Desafío 4.2: Las guías de seguridad digital se repiten, se vuelven obsoletas y se encuentran en pocos idiomas.

- **Recomendaciones** (agencias de noticias, organizaciones internacionales e instituciones de periodismo):

    - En lugar de destinar recursos a la creación de más guías de capacitación, las organizaciones deberían considerar el invertir recursos para actualizar las existentes, traducirlas a más idiomas y concientizar sobre ellas. Esto puede que lleve a menos confusión entre periodistas y otros agentes que hacen periodismo, y podría también generar más información actualizada, disminuyendo de ese modo la probabilidad de que los periodistas puedan operar con una falsa sensación de seguridad.

Idealmente, los capacitadores en seguridad digital tienen que ser a partes iguales:

- animador, garantizando que los individuos se vean reforzados en las normas de una expresión libre y segura;

- doctor, diagnosticando las vulnerabilidades y síntomas digitales de una persona;

- traductor, convirtiendo los conocimientos tecnológicos en lenguaje fácil de usar que conecte con sus públicos.

Esta mezcla de roles puede ayudar a garantizar que los participantes sean capaces de implementar protocolos de seguridad para una situación específica.

Debido a que la seguridad digital para el periodismo no es una cuestión exclusivamente técnica, los cursos de capacitación en seguridad digital pueden incluir provechosamente las dimensiones de la Alfabetización Mediática e Informacional (MIL) en sus programas. Muchos periodistas carecen de conocimientos básicos sobre el comportamiento digital adecuado; por ejemplo, haciéndose vulnerables mediante sus posts en redes sociales. Por consiguiente, cometen simples errores que podrían acarrear costosas consecuencias. La MIL busca modificar esto proporcionando conocimientos básicos sobre cómo actuar online e instruyendo a los usuarios sobre peligros que pueden evitarse fácilmente.

Diversas organizaciones han escrito ampliamente acerca de herramientas y tácticas que deberían utilizar los periodistas para su seguridad digital. Sin embargo, los lineamientos generales que quienes hacen periodismo deberían implementar resultan menos evidentes. A continuación se incluyen algunas sugerencias:

Lineamientos para mejores cursos de capacitación en seguridad digital

Cuando se realizan cursos de capacitación en seguridad digital, los capacitadores deberían incluir:

1. Una introducción a los estándares normativos internacionales. Como se planteó anteriormente en esta publicación, hay muchas declaraciones de las Naciones Unidas –así como regionales– que son directamente relevantes para la libertad de expresión, la libertad de prensa y la seguridad de los periodistas, y que deberían aplicarse al periodismo en todas las tecnologías. Por ejemplo, una que resulta particularmente relevante es la referencia ya citada dentro de una resolución de la UNESCO sobre cuestiones de Internet de noviembre de 2013: “La privacidad es fundamental para proteger a las fuentes periodísticas, lo que permite que una sociedad se beneficie del periodismo de investigación, para fortalecer la buena gobernanza y el estado de derecho”. [222] También particularmente relevante para la seguridad digital es la resolución del Consejo de Derechos Humanos de las Nacio-

nes Unidas de septiembre de 2014, que reconocía "la particular vulnerabilidad de los periodistas a convertirse en objetivo de vigilancia ilícita o arbitraria y/o interceptación de comunicaciones en violación de sus derechos a la privacidad y la libertad de expresión".[223] La capacitación debería garantizar que los periodistas sean empoderados para conocer y utilizar estas declaraciones, y las citadas anteriormente, en sus actividades de monitoreo, reporte y defensa.

2. Un enfoque integral de la seguridad digital, incluyendo el panorama jurídico y conocimientos exhaustivos de cómo funcionan las redes y de la estructura de Internet. Las protecciones legales para periodistas no han seguido el ritmo del cambio tecnológico y los periodistas a menudo no son conscientes de cómo las redes interactúan entre sí o de la infraestructura de Internet; ambos aspectos son necesarios para garantizar que se utilicen las herramientas de seguridad digital adecuadas para proteger la información.

3. Una evaluación de riesgos o ejercicio de modelo de amenazas. Los periodistas tienen que desarrollar una evaluación de riesgos personalizada para garantizar que las herramientas y prácticas de seguridad digital que utilizan sean eficaces para su situación concreta. Los capacitadores pueden empoderar a los periodistas para que se adapten a nuevos entornos de seguridad enseñando a los periodistas cómo realizar una evaluación de riesgos y elaborar respuestas para su situación concreta.

4. Añadir cuestiones sobre modelo de amenazas o evaluación de riesgos a los cursos de capacitación significa que los periodistas puedan llevarse consigo una serie de habilidades adaptables que pueden ajustarse para satisfacer su situación de seguridad específica.

5. Un enfoque sensible al género. Las amenazas que enfrentan las mujeres que hacen periodismo pueden a veces diferir de las amenazas que enfrentan los hombres que hacen periodismo, de modo que es importante que los capacitadores adapten su instrucción y garanticen que enseñan con un enfoque sensible al género. Esto debería también aplicarse a la distribución logística de los cursos de capacitación, ya que la accesibilidad puede variar para hombres y mujeres dependiendo de dónde se organice la capacitación, de cómo se lleve a cabo y, en algunos casos, de si hay disponibles capacitadores del mismo sexo o no.

6. Material actualizado que refleje una realidad cambiante. La tecnología cambia rápidamente, al igual que lo hacen las tácticas de los atacantes digitales. Los capacitadores en seguridad digital y los periodistas deben adaptarse si no quieren que sus conocimientos y herramientas se vuelvan irrelevantes. Por tanto, es importante que los capacitadores mantengan sus materiales actualizados para adaptarse al cambiante panorama de la seguridad.

7. Incluir estrategias de mitigación como parte de la capacitación. Una vez que una persona se da cuenta de que su seguridad digital o integridad tecnológica está comprometida, él o ella debería saber qué medidas adoptar y qué opciones alternativas hay disponibles.

4. ORGANIZACIONES ESCOGIDAS

Más abajo se incluyen descripciones de algunas de las organizaciones e iniciativas mencionadas en este informe. La lista no pretende ser integral, sino que está dirigida a servir como un recurso básico, así como un estímulo para futuras investigaciones y el listado de actores adicionales.

Access. Una ONG internacional que defiende y amplía los derechos digitales de los usuarios en riesgo de todo el mundo. Combinando políticas innovadoras, implicación de usuarios y apoyo técnico directo, Access lucha por comunicaciones abiertas y seguras para todos.

Apoyo para Medios de Comunicación Internacionales (IMS). Una organización sin ánimo de lucro que trabaja para apoyar a medios de comunicación locales en países afectados por conflictos armados, inseguridad humana y transiciones políticas.

Artículo 19. Establecida en 1987, Artículo 19 es una ONG internacional centrada en proteger la libertad de expresión y opinión.

Asociación para la Defensa de los Derechos de los Periodistas Iraquíes (IJRDA). Una organización con sede en Irak centrada en la seguridad de los periodistas.

Asociación para las Comunicaciones Progresistas. Una asociación internacional y una red que trabaja para empoderar y apoyar a organizaciones, movimientos sociales e individuos en el uso de Tecnologías de la Información y las Comunicaciones (TIC) y a través de éstas.

BoloBhi. Una organización sin ánimo de lucro con sede en Pakistán dirigida hacia la defensa, políticas e investigación en las áreas de derechos de género, transparencia gubernamental, acceso a Internet, seguridad digital y privacidad.

Bytes para Todos Pakistán. Una organización con sede en Pakistán centrada en las Tecnologías de la Información y las Comunicaciones (TIC) para el desarrollo, la democracia y la justicia social.

Centro Dart para Periodismo y Traumas. Una red global de periodistas, profesores de periodismo y profesionales de la salud dedicada a mejorar la cobertura de traumas, conflictos y tragedias por parte de los medios de comunicación.

Centro de Formación en Periodismo Digital (CFPD). El Centro de Capacitación en Periodismo Digital de la Universidad de Guadalajara apoya a periodistas a la hora de aprender a trabajar con nuevos medios de comunicación y fomenta la capacitación de periodistas ciudadanos. Ofrece cursos y talleres, así como instrucción presencial y recursos online.

Centro para la Democracia y la Tecnología (CDT). Una organización con sede en EUA dedicada a impulsar resultados de políticas que mantengan Internet abierto, innovador y gratuito. El CDT trabaja de forma inclusiva abarcando varios sectores y el espectro político para encontrar soluciones tangibles a los desafíos más acuciantes de las políticas sobre Internet actuales.

Centro SKeyes para Medios de Comunicación y Libertad Cultural. Una organización con sede en Líbano que monitorea violaciones de la libertad de prensa y cultural y defiende los derechos y la libertad de expresión de periodistas e intelectuales.

Centro Tow de Periodismo Digital de la Escuela de Periodismo de Columbia. El Centro Tow explora cómo el desarrollo de la tecnología está cambiando el periodismo, su práctica y su consumo; sobre todo a medida que los consumidores de noticias buscan formas de juzgar la fiabilidad, los estándares y la credibilidad de la información.

Citizen Lab. Un laboratorio interdisciplinario con base en la Escuela Munk de Asuntos Globales de la Universidad de Toronto, Canadá, que se centra en investigaciones y desarrollos avanzados en la intersección entre Tecnologías de la Información y las Comunicaciones, derechos humanos y seguridad global.

Colectivo para una Tecnología Táctica (Tactical Tech). Una organización dedicada al uso de información en el activismo. Tactical Tech se centra en el uso de datos, diseño y tecnología en campañas y ayuda a los activistas a entender y gestionar sus riesgos en seguridad digital y privacidad.

Comité para la Protección de Periodistas (CPJ). Una organización sin ánimo de lucro, con sede en Nueva York y fundada en 1981, que promueve la libertad de prensa en todo el mundo defendiendo los derechos de los periodistas a reportar las noticias sin temor a represalias.

CommunityRED. Una organización que trabaja para mejorar la seguridad de los periodistas, activistas y reporteros ciudadanos en zonas de conflicto, y promover el compartir información donde más se necesita sin poner en peligro vidas o medios de vida.

Defensores de Primera Línea. Fundada en Dublín en 2001, Defensores de Primera Línea trabaja para proporcionar acciones rápidas y eficaces para ayudar a proteger a los defensores de derechos humanos de modo que puedan seguir con su labor como agentes clave del cambio social.

Deutsche Welle Akademie. La principal organización de Alemania para el desarrollo de medios de comunicación internacionales. Los capacitadores y consultores de la DWA han estado promoviendo medios de comunicación libres e independientes desde 1965.

eQualit.ie. Fundada en 2006, eQualit.ie proporciona experiencia en seguridad digital y gestión de la información a organizaciones de la sociedad civil y de medios de comunicación independientes de primera línea con recursos limitados, trabajando en entornos de Internet sumamente hostiles. El programa de eQualit.ie, Deflect, proporciona ayuda gratuita contra ataques DDoS.

Federación Internacional de Periodistas (IFJ). Una organización que promueve las acciones internacionales para defender la libertad de prensa y la justicia social a través de sindicatos de periodistas sólidos, libres e independientes.

Fondo Rory Peck. Una organización con sede en Londres que brinda apoyo práctico directo a periodistas autónomos, periodistas en peligro y familias.

Free Press. Una organización que está creando un poderoso movimiento a nivel nacional para cambiar las políticas de medios de comunicación y tecnología, promover el interés público y fortalecer la democracia. Free Press aboga por un acceso a Internet universal y asequible, propiedad de los medios de comunicación diversificada, medios de comunicación públicos dinámicos y periodismo de calidad.

Free Press Unlimited. Establecida en Holanda en 2011 como una fusión de tres grupos holandeses sin ánimo de lucro, Free Press Unlimited es una organización sin ánimo de lucro que apoya a profesionales y periodistas de medios locales y pretende ayudar a las personas a obtener y mantener un acceso a la información suficiente para sobrevivir y desarrollarse. Recientemente, desarrolló el Laboratorio para la

Protección de Internet, que ofrece apoyo concreto y dirigido para periodistas, blogueros y activistas que son amenazados en todo el mundo.

Freedom House. Una organización de vigilancia independiente dedicada a la ampliación de la libertad en todo el mundo.

Fundación de la Libertad de Prensa. Una ONG con sede en EUA dedicada a ayudar a apoyar y defender el periodismo de interés público enfocado en divulgar la mala gestión, la corrupción y las infracciones en el gobierno.

Fundación Fronteras Electrónicas. Una ONG con sede en EUA que lucha para proteger las libertades civiles en la era digital. Combinando la experiencia de abogados, analistas políticos, activistas y especialistas en tecnología, lucha por la libertad principalmente en los tribunales, emprendiendo y defendiendo demandas contra agencias gubernamentales y corporaciones.

Fundación Internacional de Medios de Comunicación de Mujeres (IWMF). Una red global dedicada a fortalecer el papel de las mujeres en los medios de noticias de todo el mundo como un medio de promover la libertad de prensa.

Fundación Nacional de Prensa. Una fundación con sede en Washington que promueve el conocimiento de cuestiones complejas por parte de los periodistas con el fin de mejorar el entendimiento del público. La fundación reconoce y fomenta la excelencia en el periodismo a través de sus premios y programas.

Fundación para los Derechos Digitales. Una organización pakistaní de defensa orientada a la investigación y sin ánimo de lucro que se centra en las Tecnologías de la Información y las Comunicaciones (TIC) para apoyar derechos humanos, procesos democráticos y gobernanza digital.

Fundación para la Libertad de Prensa (FLIP). Una organización con sede en Bogotá que monitorea la libertad de prensa y la seguridad de los periodistas en Colombia a través de su red de alerta y protección. La FLIP proporciona también asesoría gratuita a periodistas que han sido víctimas de ataques o asaltos o que sufren de estrés.

Fundaciones para una Sociedad Abierta. Un grupo de fundaciones privadas concesionarias de becas, la primera de las cuales fue establecida por el filántropo George Soros en 1984. El Programa de Periodismo de las Fundaciones para una Sociedad Abierta ayuda en el desarrollo y establecimiento de sistemas de medios de comunicación señalados por su libertad, pluralismo y la inclusión de voces y opiniones de minorías, ya que promueve medios de comunicación independientes y viables y un periodismo profesional de calidad en países que están atravesando un proceso de democratización y desarrollando mercados de medios de comunicación funcionales.

Índice sobre Censura. Una organización con sede en Londres que promueve y defiende el derecho a la libertad de expresión.

Iniciativa Red Abierta. Una sociedad de cooperación entre tres instituciones: el Citizen Lab de la Escuela Munk de Asuntos Globales, Universidad de Toronto; el Centro Berkman para Internet y Sociedad de la Universidad de Harvard; y el Grupo SecDev (Ottawa), con el objetivo de investigar, divulgar y analizar prácticas de filtrado y vigilancia en Internet de manera confiable e imparcial.

Instituto Humanista para la Cooperación al Desarrollo (Hivos). Una organización con sede en Holanda orientada por valores humanistas que trabaja con organizaciones locales de la sociedad civil en países en desarrollo para contribuir a un mundo libre, justo y sostenible.

Instituto Internacional de Prensa (IPI). Una red global, con sede en Viena, de editores, ejecutivos de medios de comunicación y destacados periodistas. Fundada en la Universidad de Columbia de Nueva York en 1950, el IPI se dedica al fomento y salvaguarda de la libertad de prensa, la libertad de expresión y la mejora de las prácticas de periodismo.

Instituto Internacional para la Seguridad de la Prensa (INSI). Una coalición de agencias de noticias, grupos de apoyo a periodistas e individuos exclusivamente dedicada a la seguridad del personal de medios de noticias que trabaja en entornos peligrosos.

Instituto para el Reporte de la Guerra y la Paz (IWPR). Una organización con sede en Londres que forja las habilidades y capacidad del periodismo local, fortalece las instituciones de medios locales y se implica con la sociedad civil y los gobiernos para garantizar que la información logre un impacto.

Intercambio Internacional por la Libertad de Expresión (IFEX). Una red sin ánimo de lucro con sede en Toronto, compuesta por unas 95 organizaciones independientes, que trabaja para divulgar rápidamente las violaciones a la libertad de expresión en todo el mundo.

Internews. Una organización internacional sin ánimo de lucro cuya misión es empoderar a los medios de comunicación locales a nivel mundial para dar a las personas las noticias e información que necesitan, la capacidad para conectarse y los medios para hacer oír sus voces.

Junta Internacional de Investigación e Intercambios (IREX). Una organización internacional sin ánimo de lucro fundada en Washington en 1968 que proporciona liderazgo de ideas y programas innovadores para promover cambios positivos duraderos a nivel global.

M-Lab. Una iniciativa de investigación de Google que proporciona la mayor recopilación de datos abiertos de desempeño de Internet del planeta. Como consorcio de socios de investigación, industria e interés público, M-Lab se dedica a proporcionar un ecosistema para la medición abierta y verificable del desempeño de redes globales.

PEN International. Una organización internacional para la defensa de los derechos humanos de los escritores que trabaja mundialmente para promover la libertad de expresión y oponerse a la censura.

Periodista en Peligro. Una organización independiente creada en Kinshasa por un grupo de periodistas congoleños dedicada a la defensa y promoción de la libertad de prensa.

Privacy International. Una organización con sede en Londres que defiende mundialmente el derecho a la privacidad y lucha contra la vigilancia y otras intrusiones en la vida privada por parte de gobiernos y corporaciones.

Proyecto Guardian. Una organización que crea aplicaciones de fuentes abiertas fáciles de usar, mejoras en seguridad de sistemas operativos móviles y dispositivos móviles personalizados para personas de todo el mundo, con el fin de ayudarles a comunicarse más libremente, y protegerse de la intrusión y el monitoreo.

Proyecto de Herramientas Abiertas para Internet (OpenITP). Una organización que apoya a los creadores de *software* y comunidades detrás de las herramientas anti vigilancia y anti censura de fuentes abiertas que permiten a los ciudadanos comunicarse directa y libremente entre sí, en sus propios términos.

Proyecto Tor. Una organización y servicio web que ayuda a informantes y disidentes a comunicarse de forma más segura.

Registro de Autónomos de Primera Línea (FFR). Establecido en 2013, el FFR es un organismo representativo para periodistas autónomos, creado y dirigido por periodistas para apoyar el bienestar físico y mental de sus colegas.

Reporteros Sin Fronteras. Una organización internacional sin ánimo de lucro que lucha por la libertad de prensa.

RiseUp. Una organización que proporciona herramientas de comunicación online para personas y grupos que trabajan sobre cambios sociales liberadores.

Seguridad Global para Periodistas. Una organización con fines lucrativos que se sirve de prácticas civiles, policiales y militares de vanguardia para proporcionar capacitación en seguridad a periodistas, ciudadanos, activistas de derechos humanos y trabajadores de ONG.

Small World News. Una organización con sede en EUA, creada en 2005, que apoya, equipa y capacita a poblaciones desatendidas para convertirse en periodistas, narradores y documentalistas.

Voces Globales. Una comunidad virtual de más de 500 blogueros y traductores de todo el mundo que trabajan conjuntamente para difundir informes de todo el mundo, con especial énfasis en voces que no se escuchan habitualmente en los medios de comunicación internacionales.

Witness. Una organización internacional sin ánimo de lucro que ha estado utilizando el poder del video y la narración durante 20 años para abrir los ojos del mundo a los abusos a los derechos humanos.

5. ENTREVISTAS

Agradecemos a todos los que accedieron a ser entrevistados para este informe. Favor de tener en cuenta que aunque no se utilizaron citas específicas de todas las entrevistas, éstas proporcionaron antecedentes y contactos útiles para los investigadores.

Anónimo, Asociado, firma consultora de gestión y tecnología

Anónimo, Director Ejecutivo, firma consultora de gestión y tecnología

Anónimo, Director de Ciberseguridad, firma de ciberseguridad

Anónimo, Capacitador y experto en seguridad digital, organización internacional

Aaron Brauer Rieke, Director de Proyectos de Política Tecnológica, Robinson + Yu

Andrew Ford Lyons, Productor Digital y Director de Proyectos, Fondo Rory Peck

Arzu Geybullayeva, bloguera y analista regional, Azerbaiyán

Ayman Mhanna, Director Ejecutivo, Centro SKeyes para Medios de Comunicación y Fundación Cultural

Carole Kimutai, Editora, *Management Magazine*, Kenia

Christopher E. Pogue, Director, SpiderLabs US West, Trustwave

Chris Riley, Ingeniero Superior de Políticas, Mozilla Corporation

Dalia Haj Omar, activista sudanesa de derechos humanos

Dan Meredith, Director, Fondo para Tecnología Abierta de Radio Free Asia

Daniel Ó Clunaigh, Coordinador de Programas, Colectivo para una Tecnología Táctica

Danilo Bakovic, Director, Libertad en Internet, Freedom House

Danny O'Brien, Director Internacional, Fundación Fronteras Electrónicas

Deji Olukotun, Becario de Libertad para Escribir, PEN América

Diana del Olmo Campos, Gerente de Comunicaciones, Proyecto Guardian

Dmitry Vitaliev, Director Ejecutivo, eQualit.ie

Dr. Doug Belshaw, líder de alfabetización web, Mozilla Foundation

Elisa Muñoz, Directora Ejecutiva, Fundación Internacional de Medios de Comunicación de Mujeres

Ellery Roberts Biddle, Editora, Defensa de Voces Globales

Ernest Sagaga, Gerente de Derechos Humanos, Federación Internacional de Periodistas

Eva Galperin, Analista de Políticas Globales, Fundación Fronteras Electrónicas

Faisal Kapadia, bloguero, Voces Globales

Frank Smyth, Director, Seguridad Global para Periodistas

Gayathry Venkiteswaran, Directora Ejecutiva, Alianza de la Prensa del Sureste Asiático

Gerard Harris, Comunicaciones y Divulgación, eQualit.ie

Gigi Alford, Oficial Superior de Programas, Libertad en Internet, Freedom House

Gus Andrews, Asociado Superior de Programas, Proyecto de Herramientas Abiertas para Internet

Gustaf Björksten, Director de Tecnología, Access

Hannah Storm, Directora, Instituto Internacional para la Seguridad en las Noticias

Hauke Gierow, Jefe, Servicio de Libertad en Internet, Reporteros Sin Fronteras

Ibrahim Al-Sragey, Director, Asociación para la Defensa de los Derechos de los Periodistas Iraquíes

Jon Camfield, Tecnólogo Superior, Internews

Jonathan Stray, Becario, Centro Tow para Periodismo Digital

Josh Levy, Director de Campañas en Internet, Free Press[224]

Josh Stearns, Director de Campañas de Periodismo y Medios públicos, Free Press[225]

Kirsty Hughes, Ex Directora Ejecutiva, Índice sobre Censura

Lamiya Adilgizi, Periodista, *Today's Zaman*, y Redactora, *Turkish Review*

Lindsay Beck, Oficial de Programas, Programas TIC, Instituto Nacional Demócrata[226]

Melissa Chan, Periodista, Al Jazeera América

Michael Carbone, Director de Política Tecnológica y Programas, Access

Mindy Ran, Copresidenta, Consejo sobre Género, Federación Internacional de Periodistas

Nicolas Rouger, Oficial de Programas, África subsahariana, Fondo Rory Trust

Nighat Dad, Directora, Fundación para los Derechos Digitales, Pakistán

Oktavia Jónsdóttir, Directora, SAFE, Junta Internacional de Investigación e Intercambios

Paul Mooney, periodista autónomo[227] Paula Martins, Coordinadora, Artículo 19 Brasil

Peter Nkanga, Asesor para África Occidental, Comité para la Protección de Periodistas

Peter Noorlander, Director Ejecutivo, Iniciativa para la Defensa Legal de Medios de Comunicación

Rebecca MacKinnon, Directora, Proyecto de Clasificación de Derechos Digitales, Fundación New America

Robert Guerra, Asesor Principal, Citizen Lab

Roxana Geambasu, Profesora Adjunta de Informática, Universidad de Columbia

Sarah Giaziri, Responsable de Programas, Oriente Medio y África del Norte, Fondo Rory Peck

Seamus Tuohy, Asociado de Programas Técnicos, Instituto de Tecnologías Abiertas, Fundación New America[228]

Shauna Dillavou, Director Ejecutivo, CommunityRED

Sheryl Mendez, Responsable Principal de Programas, Programa Global de Derechos Humanos, Freedom House

Shiva Gaunle, Presidente, Federación de Periodistas Nepalíes

Steve Kelley, Vicepresidente Primero, Marketing de Productos y Corporativo, Trustwave

Susan McGregor, Profesora Adjunta y Directora Adjunta, Centro Tow para Periodismo Digital

Tom Rhodes, Representante para África Oriental, Comité para la Protección de Periodistas

Wafa Ben Hassine, bloguera, Túnez

Con correspondencia extraída de:

Correspondencia en Twitter con la Escuela de Periodismo de la Academia de la BBC, 20 de marzo de 2014

E-mail de Erin Murrock, 3 de abril de 2014

E-mail de Henrik P. Berggreen, 27 de febrero 2014

E-mail de Ismail Hakki Polat, 23 de marzo de 2014

E-mail de Jane E. Kirtley, 13 de enero de 2014

Correspondencia en Twitter con Jorge Luis Sierra, 19 de marzo de 2014

E-mail del Dr. Michel Cukier, 11 de abril de 2014

E-mail de Privacy International, 15 de enero de 2014

E-mail de Sandeep Junnarkar, 16 de enero de 2014

Respuestas a cuestionarios adicionales por parte de: Apoyo a Medios de Comunicación Internacionales, Comité para la Protección de Periodistas, Reporteros Sin Fronteras, Bytes para Todos, Artículo 19 y la Federación Internacional de Periodistas.

APÉNDICE 1: METODOLOGÍA DE LA ENCUESTA

Objetivo

El objetivo de esta investigación es entender mejor la seguridad de los agentes de medios de comunicación que hacen periodismo con tecnología digital, examinando los desafíos y riesgos específicos que enfrentan en un ambiente tecnológico y político complejo. Para abordar en profundidad estas cuestiones, y proporcionar la información para los capítulos subsiguientes, los investigadores han:

1. Descrito a algunas de las diversas partes interesadas e iniciativas que abordan la seguridad online.

2. Mapeado algunas de las diversas instituciones de formación en periodismo que tratan la seguridad online con sus integrantes.

3. Mapeado algunas de las amenazas y desafíos digitales que enfrentan los periodistas.

4. Explorado algunas de las mejores prácticas y lineamientos que pueden utilizar diversas partes interesadas para abordar estos desafíos.

5. Ofrecido recomendaciones a las principales partes interesadas para ayudarles a hacer frente a estos desafíos.

Los autores utilizaron métodos de investigación cualitativa y cuantitativa a la hora de elaborar este informe, incluyendo entrevistas y encuestas. Entre octubre de 2013 y abril de 2014, los investigadores entrevistaron a más de 50 expertos en libertad de prensa, especialistas en tecnología, académicos y periodistas en persona, de forma electrónica o por teléfono. Los investigadores confeccionaron también dos encuestas para esta investigación. La primera y principal era una encuesta electrónica multilingüe[229] de 52 preguntas que fue difundida a una red de organizaciones internacionales, asociaciones de prensa y redes profesionales relevantes.[230] La encuesta fue aplicada en primer lugar a un pequeño grupo piloto en septiembre de 2013. Tras los comentarios al estudio piloto, los investigadores actualizaron la encuesta y la publicaron en noviembre de 2013. El link de la encuesta permaneció activo hasta agosto de 2014, aunque la difusión de la encuesta terminó en marzo de 2014.

Aproximadamente 2,645 personas vieron el estudio, 478 lo empezaron y 167 lo completaron.[231] El número de completados no incluye a los participantes en el estudio piloto o a individuos que reportaron que no se dedicaban a la recopilación de noticias (y por tanto sus respuestas fueron eliminadas del número total de encuestados). Los participantes invirtieron un promedio de 13 minutos en completar la encuesta.

La segunda encuesta electrónica era de 10 preguntas y se centraba en la capacitación en seguridad digital entre instituciones de periodismo. Los investigadores la enviaron a contactos en la Asociación de Noticias Digitales de Radio y Televisión, la Asociación para la Formación en Periodismo y Comunicación de Masas, la Asociación para la Formación en Radiodifusión, el Centro Internacional para Periodistas, el Consejo de Asesores de Escuelas de Medios de Comunicación y la Red Internacional de Periodistas, aunque los investigadores no recibieron respuestas de todas las organizaciones. Los participantes

en la encuesta incluyeron a individuos de Colombia, Estados Unidos Francia, Mongolia, Nigeria y Pakistán. Un total de 356 individuos vieron el estudio, 46 lo empezaron y 14 lo completaron. La encuesta fue aplicada activamente desde el 14 de enero de 2014 al 4 de febrero de 2014, aunque el link estuvo disponible hasta agosto de 2014.

Limitaciones de la encuesta

La encuesta sobre la seguridad de los actores de medios de comunicación online que hacen periodismo fue difundida a través de ONG, asociaciones de noticias y la red profesional de los investigadores vía Internet, y no representa una muestra aleatoria de la población. El índice de respuesta puede haber estado influido por lo siguiente:

- **Longitud y complejidad de la encuesta.** La encuesta constaba de 52 preguntas, muchas de las cuales implicaban respuestas por escrito. Esta solicitud para una participación en profundidad puede que haya contribuido al número de abandonos (293) de la encuesta.

- **Complejidad de la seguridad digital.** En la página de introducción a la encuesta, los investigadores aconsejaban a los participantes que se sintieran en posibilidad de descargar un servicio de anonimizador proxy como Tor antes de responder a la encuesta. Los investigadores también propusieron la opción de una entrevista segura en lugar de la encuesta a través de un canal de comunicación encriptado, si estaban preocupados por su seguridad.

  Aunque estas advertencias estaban pensadas para crear un entorno digital más seguro para los participantes, así como para generar confianza y participación, los investigadores creen que la terminología específica de seguridad digital puede que haya dado lugar a una menor participación. Algunos participantes puede que no se hayan considerado en riesgo hasta la advertencia, mientras que otros participantes puede que se hayan sentido intimidados por las medidas adicionales que los investigadores sugirieron que adoptaran. Tras haber llegado a estas conclusiones internamente, los investigadores acortaron la página de introducción y eliminaron parte del lenguaje técnico con el fin de generar más respuestas. Además, los investigadores trabajaron en colaboración con la empresa proveedora de la encuesta, QuestionPro, para enviar la encuesta a periodistas que vivían y trabajaban en países de Oriente Medio, Asia y Latinoamérica, puesto que los investigadores tuvieron dificultades en obtener respuestas a través de sus redes para participantes de esos países.

- **Solicitud de datos biográficos.** Para evitar la duplicación de datos, los investigadores solicitaron inicialmente a los participantes que respondieran a preguntas referentes a información biográfica, incluyendo nombre de pila, apellido, dirección de correo electrónico, etcétera. Después de que una organización expresara sus reservas respecto a compartir la encuesta con su red debido a estas preguntas, los investigadores habilitaron la opción de que esta información fuera de carácter voluntario. Para evitar una potencial duplicación de datos, los investigadores evaluaron cada encuesta individualmente de acuerdo con respuestas a preguntas más generales.

- **Limitaciones de difusión.** Al menos una organización optó por no difundir la encuesta online, a pesar de su abierto apoyo al proyecto e intenciones de los investigadores, debido a que dicha organización trabaja con periodistas en riesgo en situaciones muy inestables y les preocupaba la vulnerabilidad de esta población si la completaban online, a pesar de la estricta política de eliminación de datos y garantía de anonimato de la empresa proveedora de la encuesta.

Aun con todas estas reservas, los hallazgos de la investigación han sido útiles a la hora de proporcionar una casuística, y para extrapolar la clase de amenazas y respuestas que conlleva. El resultado es un mejor entendimiento de cómo impactan las cuestiones digitales en la seguridad y protección del periodismo.

APÉNDICE 2:
CUESTIONARIO

A continuación se incluye el cuestionario de la encuesta que los investigadores hicieron llegar a los participantes. Favor de tener en cuenta que el lenguaje de la introducción cambió a raíz de los comentarios de los participantes y otros involucrados. Los participantes recibieron en primer lugar dos preguntas de filtro antes de que pudieran continuar con la encuesta.

Hola: Se le invita a participar en una encuesta global patrocinada por la UNESCO sobre la seguridad de los agentes de medios de comunicación online dedicados al periodismo. Su participación en este estudio es completamente voluntaria y sus respuestas a la encuesta serán confidenciales. Los datos de esta investigación serán reportados principalmente en el informe consolidado. Si decidimos utilizar alguna cita extraída de la investigación, citaremos una fuente anónima, o nos pondremos primero en contacto con usted para que dé su aprobación. Si, en cualquier momento, se siente incómodo respondiendo a una o más preguntas, puede retirarse de la encuesta, o puede ponerse en contacto con la Especialista Individual para la UNESCO, Jennifer Henrichsen, en JournalistSafety@gmail.com (Clave GPG: 0xD-4D03F57) para concertar una entrevista confidencial. Como agradecimiento por su participación, tendrá la oportunidad de ganar una suscripción anónima pre pago al servicio de encriptación móvil global de Silent Circle. Elegiremos aleatoriamente a un ganador en febrero de 2014. (Favor de tener en cuenta que Silent Circle no está de ningún modo involucrada en esta encuesta o investigación.) Gracias por tomarse el tiempo de compartir sus puntos de vista y experiencias sobre este importante tema. Favor de iniciar la encuesta haciendo clic más abajo en Continuar.

1. ¿Cuál es su nombre de pila? (Opcional)

2. ¿Cuál es su apellido? (Opcional)

3. ¿En qué dirección de correo electrónico podemos ponernos en contacto con usted si necesitamos clarificar algo o buscar una mayor elaboración? (Opcional)

4. ¿En qué número de teléfono podemos localizarle si necesitamos clarificar algo o buscar una mayor elaboración? (Opcional)

5. ¿A qué sexo pertenece?

   - Masculino
   - Femenino
   - Transexual

6. ¿Cuál es su nacionalidad?

7. ¿Qué edad tiene?

- 18-24
- 25-34
- 35-44
- 45-54
- 55-64
- 65-74
- 75 o más
- Si es otra, favor de especificar:

8. ¿En qué país vive actualmente?

9. ¿En qué área de medios de comunicación trabaja? (Elegir todas las que apliquen.)

- TV
- Radio
- Periódico
- Revista
- Internet
- Si es otra, favor de especificar:

10. ¿Cómo está empleado? (Elegir todas las que apliquen.)

- Autónomo
- Periodista de planta
- Bloguero profesional
- Periodista/bloguero ciudadano (voluntario/no remunerado)
- Si es otra, favor de especificar:

11. ¿Cuál es el nombre de la publicación, blog o medio de noticias para el que informa?

12. ¿Qué porcentaje de sus ingresos se derivan de sus actividades de periodismo? (Favor de hacer un cálculo aproximado.)

    - 0-25%
    - 26-45%
    - 46-65%
    - 66-85%
    - Más de 85%

13. Durante los últimos 12 meses, ¿cuánto tiempo ha invertido en actividades de recopilación de información? (Favor de hacer un cálculo aproximado.)

    - 0-25%
    - 26-45%
    - 46-65%
    - 66-85%
    - Más de 85%

14. Favor de describir el tipo de artículos que cubre principalmente:

    - Política y gobernanza
    - Guerras y/o seguridad
    - Nota roja
    - Accidentes y desastres
    - Derechos humanos
      (incluyendo derechos de mujeres, niños, minorías y comunidad LGBT)
    - Salud
    - Educación
    - Negocios
    - Arte y entretenimiento
    - Tecnología e innovación
    - Religión y cultura
    - Deportes
    - Si es otro, favor de especificar:

15. ¿Qué tecnologías y herramientas utiliza a la hora de investigar, distribuir o escribir un artículo? (Elegir todas las que apliquen.)

- Computadora de escritorio
- Laptops/tablets
- Teléfonos celulares
- E-mail
- Herramientas colaborativas (por ejemplo, Google Docs)
- Almacenamiento en la nube (por ejemplo, Dropbox)
- Dispositivos USB
- Sitios web en general, incluyendo motores de búsqueda
- Sitios web de redes sociales (por ejemplo, Facebook, LinkedIn, Weibo, Twitter, etcétera)
- GPS
- Dispositivos de grabación en video/audio
- Si es otra, favor de especificar:

16. ¿Con qué frecuencia utiliza el correo electrónico cuando está:

	Nunca	Casi nunca	A veces	A menudo	Casi siempre
Investigando para un artículo					
Organizando entrevistas					
Entrevistando a sujetos					
Colaborando con un medio de comunicación (si no es aplicable, dejar el control deslizante en el margen izquierdo)					
Discutiendo sobre el artículo con colegas					
Distribuyendo el artículo (si no es aplicable, dejar el control deslizante en el margen izquierdo)					

17. ¿Qué servicio(s) de correo electrónico utiliza para sus interacciones relacionadas con el trabajo? (Elegir todas las que apliquen.)

- Gmail
- Hotmail
- Yahoo
- Una cuenta de e-mail a través de su organización
- Si es otro, favor de especificar:

18. ¿Conoce servicios de e-mail que ofrezcan comunicaciones encriptadas?

- Sí
- No

19. En caso afirmativo, ¿cuál(es)?

20. ¿Utiliza plataformas de redes sociales como Facebook, Twitter, LinkedIn, etcétera, cuando investiga para un artículo?

	Nunca	Casi nunca	A veces	A menudo	Casi siempre
Facebook					
YouTube					
Twitter					
LinkedIn					
Google+					
Flickr					
Orkut					
Weibo					
Otras					

21. Si eligió otras en respuesta a la pregunta anterior, favor de especificar la(s) plataforma(s).

22. ¿Utiliza plataformas de redes sociales como Facebook, Twitter, LinkedIn, etcétera. cuando distribuye un artículo? (Si no es aplicable, favor de dejar en blanco.)

	Nunca	Casi nunca	A veces	A menudo	Casi siempre
Facebook					
YouTube					
Twitter					
LinkedIn					
Google+					
Flickr					
Orkut					
Weibo					
Otras					

23. Si eligió otras en respuesta a la pregunta anterior, favor de especificar la(s) plataforma(s).

24. ¿Su tipo de periodismo/blogging incluye encontrarse con contactos/fuentes sensibles?

- Sí
- No
- No sé

25. En caso afirmativo, ¿modifica la forma de relacionarse con su(s) contacto(s)/fuente(s) sensibles? Si es así, favor de explicar cómo (por ejemplo, sólo utiliza e-mail encriptado, se reúne sólo en persona, etcétera).

26. Como periodista, ¿qué tipo de cuestiones le preocupan?
(Elegir todas las que apliquen.)

- Seguridad personal
- Seguridad de la información
- Seguridad de las personas con quienes trabajo
- Seguridad de las fuentes
- Seguridad de familiares
- No sé
- Si es otra, favor de especificar:

27. ¿Cuáles son las tres principales amenazas que podría enfrentar en su papel de periodista?

- Detención ilegal
- Amenazas en persona
- Amenazas por e-mail
- Amenazas por SMS/mensaje de voz
- Ataque físico
- Vigilancia de sus actividades online
- Amenazas a amistades y/o familiares
- Virus en la computadora que daña datos
- Revelación de identidad (en contra de sus deseos)
- Sitio web/blog personal o sitio web/blog de agencias de noticias hackeado/atacado
- E-mails interceptados
- Datos robados, incluyendo datos almacenados en la nube
- Teléfono pinchado o llamadas grabadas
- Suplantación online
- Campaña de desinformación online
- No sé
- Si es otra, favor de especificar:

28. ¿Qué cree que motiva a las personas a llevar a cabo estas amenazas?

29. ¿Quién cree que podría estar detrás de este tipo de ataques? ¿Por qué?

30. En los últimos 18 meses, ¿ha experimentado alguna consecuencia negativa debido a sus actividades de periodismo y/o blogging?

- Sí
- No
- No sé

31. En caso afirmativo, ¿qué experimentó? (Favor de elegir todas las que apliquen.)

- Fui detenido ilegalmente
- Fui amenazado en persona
- Fui amenazado por e-mail
- Fui amenazado por SMS/mensaje de voz
- Fui atacado físicamente

- Mis actividades online fueron vigiladas
- Mis amistades o familiares fueron amenazados
- Mi computadora fue infectada con un virus y mis datos resultaron dañados
- Mi identidad fue revelada en contra de mis deseos
- Mi publicación, sitio web o blog fue atacado o hackeado (por ejemplo, ataques DDOS, de *phishing*/*spear phishing*)
- Mis e-mails fueron interceptados
- Mis datos fueron robados
- Mi teléfono fue pinchado y/o mis llamadas fueron grabadas
- Alguien me suplantó online
- Alguien realizó una campaña de desinformación online en mi contra
- Si es otra, favor de especificar:

32. Favor de proporcionar una breve descripción de lo que experimentó. Si prefiere hablar sobre su(s) experiencia(s) directamente con la Especialista Individual de la UNESCO, Jennifer Henrichsen, favor de indicarlo aquí o enviarle un e-mail (JournalistSafety@gmail.com, GPG Key: 0xD4D03F57) para concertar una entrevista segura.

33. ¿Hace clic en cualquier link contenido en un mensaje de correo electrónico, si el remitente es desconocido?

- No
- Casi nunca
- A veces
- A menudo
- Casi siempre
- Sí, pero sólo después de comprobar la ubicación
- No sé
- Si es otra, favor de especificar:

34. ¿Hace clic en cualquier link contenido en un mensaje de correo electrónico, si el remitente es conocido?

- No
- Casi nunca
- A veces
- A menudo
- Casi siempre
- Sí, pero sólo después de comprobar la ubicación del enlace
- No sé
- Si es otra, favor de especificar:

35. ¿Con qué frecuencia hace clic en archivos adjuntos de correo electrónico si conoce al remitente?

- Nunca
- Casi nunca
- A veces
- A menudo
- Casi siempre
- Si es otra, favor de especificar:

36. ¿Con qué frecuencia hace clic en archivos adjuntos de correo electrónico si no conoce al remitente?

- Nunca
- Casi nunca
- A veces
- A menudo
- Casi siempre
- Si es otra, favor de especificar:

37. Hay una variedad de formas para incrementar la seguridad de la información y de los individuos que utilizan plataformas y herramientas online. ¿Conoce alguno de esos métodos?

- Sí
- No
- No sé

38. En caso afirmativo, ¿cuál de los siguientes utiliza para proteger sus datos y/o a sus fuentes?

- Utilizar contraseñas difíciles de descifrar para su e-mail y otras cuentas en Internet
- Encriptar datos, incluyendo e-mails
- Utilizar *software* antivirus de fuentes abiertas
- Mantener actualizado su sistema operativo con los parches y actualizaciones de seguridad más recientes
- Utilizar ocultadores/bloqueadores de IP
- Utilizar *software* anticensura (una aplicación de *software* que permite a un usuario eludir los filtros de redes y acceder a recursos de Internet que estarían normalmente prohibidos por su proveedor de servicios)
- Utilizar una VPN (Red Privada Virtual, una versión virtual de una red física segura. Básicamente, se trata de una red de computadoras conectadas entre sí para compartir archivos y otros recursos)
- Si es otro, favor de especificar:

39. ¿Cuál es la característica más importante que busca cuando elige personalmente o recibe un servicio de e-mail de su organización?

- Seguridad
- Espacio de almacenamiento
- Facilidad de uso
- No es aplicable
- Si es otra, favor de especificar:

40. ¿Cuál es la característica más importante que busca cuando elige o recibe un servicio de *blogging* o *microblogging* de su organización?

- Popularidad
- Diseño/apariencia
- Capacidad de personalizar
- Costos
- Seguridad/privacidad
- Facilidad de uso
- No es aplicable
- Si es otra, favor de especificar:

41. ¿Ha oído hablar del concepto de *blogging* anónimo?

- Sí, lo utilizo
- Sí, pero nunca lo he utilizado
- No

42. ¿Ha oído hablar del concepto de modelo de amenazas en lo que se refiere a protegerse online?

- Sí
- Sí, pero no recuerdo lo que significa
- No
- No sé
- Si es otra, favor de especificar:

43. ¿Cómo evita la manipulación no autorizada de sus contenidos?

- Utilizando contraseñas difíciles de descifrar para su e-mail y otras cuentas en Internet
- Utilizando autenticación de dos factores para su e-mail y otras cuentas en Internet
- Encriptando datos
- Utilizando *software* antivirus de fuentes abiertas
- Manteniendo su sistema operativo actualizado con los parches y actualizaciones de seguridad más recientes
- Utilizando ocultadores/bloqueadores de IP
- Utilizando *software* anticensura (una aplicación de *software* que permite a un usuario eludir los filtros de redes y acceder a recursos de Internet que estarían normalmente prohibidos por su proveedor de servicios)
- Utilizando una VPN (Red Privada Virtual –una versión virtual de una red física segura. Básicamente, se trata de una red de computadoras conectadas entre sí para compartir archivos y otros recursos)
- Protección *firewall*
- Eliminación segura de datos
- Respaldos seguros para evitar cualquier pérdida de información
- Si es otro, favor de especificar:

44. Favor de indicar el nivel de seguridad digital que cree que ofrece cada una de las siguientes estrategias. (1=No sabe, 2=No segura, 3=Algo insegura, 4=Algo segura, 5=Totalmente segura)

	1	2	3	4	5
Utilizar contraseñas difíciles de descifrar para su e-mail y otras cuentas en Internet					
Utilizar autenticación de dos factores para su e-mail y otras cuentas en Internet					
Encriptar datos					
Utilizar *software* antivirus de fuentes abiertas					
Mantener su sistema operativo actualizado con los parches y actualizaciones de seguridad más recientes					
Utilizar ocultadores/bloqueadores de IP					
Utilizar *software* anticensura					
Utilizar una VPN					

45. ¿Qué herramientas de seguridad utiliza para asegurar los datos de su computadora? (Elegir todas las que apliquen.) Protección con contraseñas

- Eliminación segura de datos
- Asegurar los datos en unidades de almacenamiento externas
- Encriptación
- *Software* antivirus de fuentes abiertas
- Si es otra, favor de especificar:

46. ¿Qué medidas de seguridad, si las hubiere, emplea para asegurar los datos de su teléfono celular? (Elegir todas las que apliquen.)

- Protección con contraseñas
- Eliminación segura de datos
- Encriptación
- *Software* antivirus de fuentes abiertas
- Si es otra, favor de especificar:

47. ¿Ha participado en algún curso de capacitación en seguridad digital que le enseñara cómo utilizar Internet de manera segura y cómo proteger sus datos?

- Sí, en los últimos 12 meses
- Sí, pero fue hace más de 12 meses
- No

48. En caso afirmativo, ¿qué tipo de capacitación u orientación recibió? (Elegir todas las que apliquen.)

- Recomendaciones de colegas
- Curso(s) presencial(es) por parte de una reputada organización
- Curso(s) online por parte de una reputada organización
- Recomendaciones de empleadores
- Autodidacta
- Si es otra, favor de especificar:

49. Si tomó un curso, ¿cuál era el nombre de la organización que lo patrocinó?

50. ¿Qué tan satisfecho quedó con la enseñanza impartida en los cursos sobre lo siguiente?

	Muy Insatisfecho	Insatisfecho	No sé	Satisfecho	Muy satisfecho	No es aplicable
Seguridad con contraseñas						
Encriptar datos						
Utilizar *software* antivirus						
Mantener su sistema operativo actualizado con los parches de seguridad más recientes						
Utilizar ocultadores/ bloqueadores de IP						
Utilizar *software* anticensura						
Utilizar una VPN						

51. En una escala del 1 al 5, ¿cómo calificaría su conocimiento general de prácticas digitales seguras? (1= Mediocre, 5= Excelente)

	Mediocre	Razonable	Bueno	Satisfecho	Por encima de la media	Excelente

52. ¿Qué apoyo podrían brindar los empleadores o legisladores a los periodistas para ayudarles a sentirse más seguros cuando se dedican a su profesión online?

Notas

1. El cargo de Samantha Barry ha cambiado desde su involucramiento en este proyecto; en 2014 era Encargada de Información Social y Directora Principal de Estrategia para Noticias y Medios Sociales de CNN.
2. UNESCO. (2014) Tendencias mundiales en libertad de expresión y desarrollo de medios de comunicación. UNESCO. http://unesdoc.unesco.org/images/0022/002270/227025e.pdf (con acceso el 8 de diciembre del 2015.)
3. Kovach, B. y Rosensteil, R., Los elementos del periodismo. Todo lo que los periodistas deben saber y los ciudadanos esperar, 1a ed. (Madrid: Aguilar, 2012.) pp. 5-6.
4. Norris, P. (2006). "The role of the free press in promoting democratization, good governance, and human development". Artículo presentado en la Reunión Anual de la Asociación de Ciencias Políticas del Medio Oeste, 20-22 de abril del 2006, Chicago, Palmer House.
5. Banco Mundial. (2002). *The right to tell: The role of mass media in economic development*. http://elibrary. worldbank.org/doi/pdf/10.1596/0-8213-5203-2
6. UNESCO: Programa Internacional para el Desarrollo de la Comunicación. (15 de marzo de 2014.) "Why free, independent and pluralistic media deserve to be at the heart of a post-2015 development agenda". http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/free_media_post_2015.pdf (con acceso el 8 de diciembre del 2015.)
7. *Journalism Ethics: A Philosophical Approach*, editado por Christopher Meyers. Oxford University Press. Nueva York: Nueva York, 2010. p. 78.
8. Sindicato Internacional de Telecomunicaciones. 2013. "The World in 2013: ICT Facts and Figures". http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2013-e.pdf (con acceso el 8 de diciembre del 2015.)
9. *Journalism Ethics: A Philosophical Approach*, editado por Christopher Meyers. Oxford University Press. Nueva York: Nueva York, 2010. p. 111.
10. Tehranian, M. "Peace Journalism: Negotiating Global Media Ethics". Harvard International Journal of Press/Politics 7, No. 2 (2002): pp. 58-83.
11. Entrevista con Oktavía Jónsdóttir, 18 de noviembre del 2013.
12. La Rue, F. (4 de junio de 2012.) Informe del Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, A/HRC/20/17 http://www.acnur.org/t3/fileadmin/Documentos/BDL/2014/9691.pdf?view=1 (con acceso el 8 de diciembre del 2015.)
13. UNESCO. (12 de abril de 2012.) Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/UN-Plan-on-Safety-Journalists_ES_UN-Logo.pdf (con acceso el 8 de diciembre del 2015.)
14. UNESCO. (4 de noviembre de 2013.) "Indicadores de seguridad de los periodistas: Nivel nacional". http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Indicadores_de_la_Seguridad_de_los_Periodistas_Nacional.pdf (con acceso el 8 de diciembre del 2015.)
15. Oficina del Alto Comisionado para los Derechos Humanos. (1 de julio del 2013.) La seguridad de los periodistas: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/153/22/PDF/G1315322.pdf?OpenElement (con acceso el 8 de diciembre del 2015.)
16. Entrevista con Tom Rhodes, 2 de enero de 2014.
17. UNESCO. (12 de abril de 2012.) Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/UN-Plan-on-Safety-Journalists_ES_UN-Logo.pdf (con acceso el 8 de diciembre del 2015.)

18. Naciones Unidas. (12 de abril del 2012.) Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad: Estrategia de implementación 2013-2014. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/official_documents/Implementation_Strategy_2013-2014.pdf (con acceso el 8 de diciembre del 2015.)
19. McGregor, S. y Ag., M. (17 de marzo del 2014.) "TA3M on JournoSec with Susan McGregor of Columbia and Magnus Ag of Committee to Protect Journalists". https://www.youtube.com/watch?v=tu0_ySgLgys (con acceso el 8 de diciembre del 2015.)
20. Beiser, E. (18 de diciembre del 2013.) Second worst year on record for jailed journalists. Comité para la Protección de Periodistas. https://cpj.org/reports/2013/12/second-worst-year-on-record-for-jailed-journalists.php (con acceso el 8 de diciembre del 2015.)
21. Entrevista con Gustaf Björksten, 20 de diciembre del 2013.
22. Internews. (7 de agosto del 2012.) Digital Security and Journalists: A Snapshot of Awareness and Practice in Pakistan. Internews. https://innovation.internews.org/research/digital-security-and-journalists-snapshot-awareness-and-practice-pakistan (con acceso el 8 de diciembre del 2015.)
23. Estas organizaciones solicitaron no ser identificadas para este informe.
24. Symantec Corporation. (Abril del 2013.) "Internet Security Threat Report 2013". Symantec Corporation. http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf (con acceso el 8 de diciembre del 2015.)
25. Marquis-Boire, M. (10 de octubre del 2012.) "Backdoors are Forever: Hacking Team and the Targeting of Dissent?". The Citizen Lab. https://citizenlab.org/wp-content/uploads/2012/10/12-2012-backdoorsareforever.pdf (con acceso el 8 de diciembre del 2015.)
26. Deibert, R. (2013.) Black Code: Surveillance, Privacy, and the Dark Side of the Internet. McClelland & Stewart. Toronto: Ontario. p. 165.
27. Íbid.
28. Björksten, G. (27 de marzo del 2014.) "Innovating our future: Gustaf Björksten". Innovating Our Future. https://www.youtube.com/watch?v=pMae8pZC4DE (con acceso el 8 de diciembre del 2015.)
29. Wagstaff, J. (28 de marzo del 2014.) Journalists, media under attack from hackers: Google researchers. http://www.reuters.com/article/2014/03/28/us-media-cybercrime-idUSBREA2R0EU20140328?irpc=932 (con acceso el 2 de abril del 2014.)
30. Íbid.
31. Íbid.
32. Access. (Enero del 2012) Global Civil Society At Risk: An Overview of Some of the Major Cyber Threats Facing Civil Society. https://s3.amazonaws.com/access.3cdn.net/3aa0654d836dbffdf6_drm6ibn8c.pdf (con acceso el 8 de diciembre del 2015.)
33. Citizen Lab. (21 de octubre del 2013.) "Monitoring Information Controls During the Bali IGF". https://citizenlab.org/2013/10/monitoring-information-controls-bali-igf/ (con acceso el 8 de diciembre del 2015.)
34. Íbid.
35. La Rue, F. (4 de junio del 2012.) Informe del Relator Especial sobre la Promoción y Protección del Derecho a la Libertad de Opinión y Expresión, A/HRC/20/17 http://www.acnur.org/t3/fileadmin/Documentos/BDL/2014/9691.pdf?view=1 (con acceso el 8 de diciembre del 2015.); Citizen Lab. (21 de octubre del 2013.) "Monitoring Information Controls During the Bali IGF." https://citizenlab.org/2013/10/monitoring-information-controls-bali-igf/ (con acceso el 8 de diciembre del 2015.)
36. Privacy International. Big Brother Inc. https://www.privacyinternational.org/node/9 (con acceso el 8 de diciembre del 2015.)

37. Wikileaks. Spy Files 3. http://wikileaks.org/spyfiles3p.html (con acceso el 8 de diciembre del 2015.)
38. Consejo de Derechos Humanos, Sesión Vigésimo Quinta, A/HRC/25/L.12. http://daccess-dds-ny.un.org/doc/UNDOC/LTD/G14/123/30/PDF/G1412330.pdf?OpenElement (con acceso el 8 de diciembre del 2015.)
39. Consejo de Derechos Humanos, Sesión Vigésimo Séptima, A /HRC/27/37. http://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Pages/ListReports.aspx (con acceso el 8 de diciembre del 2015.)
40. Bell, E., Coronel, S., Stray, J., Schudson, M., y Zuckerman, E. (4 de octubre del 2013.) Comment to Review Group on Intelligence and Communications Technologies Regarding the Effects of Mass Surveillance on the Practice of Journalism. http://towcenter.org/wp-content/uploads/2013/10/Letter-Effect-of-mass-surveillance-on-journalism.pdf (con acceso el 8 de diciembre del 2015.)
41. Bell, E., Coronel, S., Stray, J., Schudson, M., y Zuckerman, E. (4 de octubre del 2013.) Comment to Review Group on Intelligence and Communications Technologies Regarding the Effects of Mass Surveillance on the Practice of Journalism. http://towcenter.org/wp-content/uploads/2013/10/Letter-Effect-of-mass-surveillance-on-journalism.pdf (con acceso el 8 de diciembre del 2015.); Downie Jr., L. (10 de octubre del 2013.) Investigaciones sobre filtraciones y vigilancia en Estados Unidos post 11-s. https://www.cpj.org/es/2013/10/el-gobierno-de-obama-y-la-prensa.php (con acceso el 8 de diciembre del 2015.)
42. PEN American Center. (12 de noviembre del 2013.) "Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor". http://www.pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf (con acceso el 8 de diciembre del 2015.)
43. Bell, E., Coronel, S., Stray, J., Schudson, M., y Zuckerman, E. (4 de octubre del 2013.) Comment to Review Group on Intelligence and Communications Technologies Regarding the Effects of Mass Surveillance on the Practice of Journalism. http://towcenter.org/wp-content/uploads/2013/10/Letter-Effect-of-mass-surveillance-on-journalism.pdf (con acceso el 8 de diciembre del 2015.)
44. Privacy International, en colaboración con Access, la Fundación Fronteras Electrónicas, Artículo 19, la Asociación para las Comunicaciones Progresistas, Human Rights Watch y la Fundación World Wide Web; Privacy International. (2 de abril del 2014.) UN must reject mass surveillance to protect global privacy rights. https://www.privacyinternational.org/node/356 (con acceso el 8 de diciembre del 2015.)
45. Gallagher, R. y Greenwald, G. (12 de marzo del 2014.) "How the NSA Plans to Infect 'Millions' of Computers with *Malware*". https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-malware/ (con acceso el 8 de diciembre del 2015.)
46. Favor de tener en cuenta que el cargo y la afiliación de Seamus Tuohy han cambiado desde que se realizó esta entrevista, y en 2014 era Asesor Técnico de Internews.
47. Citizen Lab. (15 de enero del 2013.) Planet Blue Coat: Mapping Global Censorship and Surveillance Tools. https://citizenlab.org/2013/01/planet-blue-coat-mapping-global-censorship-and-surveillance-tools/ (con acceso el 8 de diciembre del 2015.); Citizen Lab. (25 de octubre del 2013.) IGF 2013: Exploring Communications Surveillance in Indonesia. (Part 3 of 4). https://citizenlab.org/2013/10/igf-2013-exploring-communications-surveillance-indonesia/ (con acceso el 8 de diciembre del 2015.); Silver, V. (25 de julio del 2012.) "Cyber Attacks on Activists Traced to FinFisher Spyware of Gamma". http://www.bloomberg.com/news/articles/2012-07-25/cyber-attacks-on-activists-traced-to-finfisher-spyware-of-gamma (con acceso el 8 de diciembre del 2015.); Marquis-Boire, M. (25 de julio del 2012.) "From Bahrain With Love: FinFisher's Spy Kit Exposed?". https://citizenlab.org/2012/07/from-bahrain-with-love-finfishers-spy-kit-exposed/ (con acceso el 8 de diciembre del 2015.)

48. Marquis-Boire, M., Marczak, B., Guarnieri, C., y Scott-Railton, J. (30 de abril del 2013.) “For Their Eyes Only: The Commercialization of Digital Spying”. https://citizenlab.org/2013/04/for-their-eyes-only-2/ (con acceso el 8 de diciembre del 2015.)
49. Wikileaks. Spy Files 3. http://wikileaks.org/spyfiles3p.html (con acceso el 8 de diciembre del 2015.)
50. Fundación Fronteras Electrónicas. (2014.) “Pen Registers” and “Trap and Trace Devices”. Fundación Fronteras Electrónicas. https://ssd.eff.org/wire/govt/pen-registers (con acceso el 5 de febrero del 2014.); Fundación Fronteras Electrónicas. (2014.) Surveillance Self-Defense. Fundación Fronteras Electrónicas. https://ssd.eff.org/wire/govt (con acceso el 7 de febrero del 2014.)
51. Bu, Z. (24 de abril del 2014.) Zero-Day Attacks are not the same as Zero-Day Vulnerabilities. http:// www.fireeye.com/blog/corporate/2014/04/zero-day-attacks-are-not-the-same-as-zero-day-vulnerabilities.html (con acceso el 8 de diciembre del 2015.)
52. Entrevista con Oktavía Jónsdóttir, 18 de noviembre del 2013.
53. de Montjoye, YA., Hidalgo, C., Verleysen, M. y Blondel, V. (25 de marzo del 2013.) “Unique in the Crowd: The privacy bounds of human mobility”. Nature. http://www.nature.com/srep/2013/130325/srep01376/full/srep01376.html (con acceso el 8 de diciembre del 2015.)
54. Morisy, M. (3 de julio del 2014). “NSA’s Xkeyscore program targeted visitors to MIT server, Tor project for enhanced security”. BetaBoston. http://betaboston.com/news/2014/07/03/nsas-xkeyscore-program-targeted-visitors-to-mit-server-tor-project-for-enhanced-scrutiny/ (con acceso el 8 de diciembre del 2015.)
55. E-mail de Eva Galperin, 21 de abril del 2014.
56. Entrevista con Nighat Dad, 5 de abril del 2014.
57. Galperin, E. y Marquis-Boire, M. (29 de marzo del 2012.) Syrian Activists Targeted with Facebook *Phishing* Attack. https://www.eff.org/deeplinks/2012/03/pro-syrian-government-hackers-target-syrian-activists-facebook-phishing-attack (con acceso el 8 de diciembre del 2015.)
58. Entrevista con Seamus Tuohy, Tecnólogo adjunto, Instituto de Tecnologías Abiertas, 16 de abril del 2014.
59. Rights Con 2014. (4 de marzo del 2014.) Sesión de panel. “Watching the Observers: The Impact of Surveillance on Human Rights”. https://www.youtube.com/watch?v=rbqHyNtj9XU&list=PLprTand RM9601CNiMd4VVTglZ1YSglKGx (con acceso el 8 de diciembre del 2015.)
60. Access. One of these things is not like the other: A report on fake domain attacks. Access. https://s3.amazonaws.com/access.3cdn.net/a80a7cabdf0ddadc85_vdm6brria.pdf p. 8 (con acceso el 8 de diciembre del 2015.)
61. Íbid, p.10
62. Íbid, p.7
63. Björksten, G. (4 de marzo del 2014.) “Reports from the Frontlines” Panel. RightsCon.
64. Access. “Fake Domain Detective”. https://fakedomains.accessnow.org/ (con acceso el 8 de diciembre del 2015.)
65. Access. Access. One of these things is not like the other: A report on fake domain attacks. Access. https://s3.amazonaws.com/access.3cdn.net/a80a7cabdf0ddadc85_vdm6brria.pdf p. 8 (con acceso el 8 de diciembre del 2015.)
66. Fisher, D. (10 de abril del 2013.) “What is a Man-in-the-Middle Attack?”. Kaspersky Lab Daily. https://blog.kaspersky.com/man-in-the-middle-attack/1613/ (con acceso el 8 de diciembre del 2015.)
67. Íbid.
68. Access. (enero del 2012) Global Civil Society At Risk: An Overview of Some of the Major Cyber Threats Facing Civil Society. https://s3.amazonaws.com/access.3cdn.net/3aa0654d836dbffdf6_drm6ibn8c.pdf (con acceso el 8 de diciembre del 2015.); E-mail de Eva Galperin, 21 de abril del 2014.

69. McDowell, M. (6 de febrero del 2013.) Security Tip (ST04-015). Understanding Denial-of-Service Attacks. Equipo de Preparación ante Emergencias Informáticas de Estados Unidos. https://www.us-cert.gov/ncas/tips/ST04-015 (con acceso el 8 de diciembre del 2015.)
70. Martinez, J. (17 de abril del 2014.) "DDoS attacks increase 47% in Q1: Akamai". TechRadar Pro. http://www.techradar.com/us/news/internet/ddos-attacks-increase-47-in-q1-akamai-1243471 (con acceso el 8 de diciembre del 2015.); Arbor Networks. (14 de febrero del 2014.) "Worldwide Infrastructure Security Report". http://www.arbornetworks.com/resources/infrastructure-security-report (con acceso el 8 de diciembre del 2015.)
71. Perlroth, N. y Wortham, J. (3 de abril del 2014.) "Tech Start-Ups Are Targets of Ransom Cyberattacks" http://bits.blogs.nytimes.com/2014/ 04/03/ tech-start-ups-are-targets-of-ransom-cyberattacks/?ref=technology (con acceso el 4 de abril del 2014.)5
72. Security-FAQs. "DoS vs DDoS – What is the difference?". http://www.security-faqs.com/dos-vs-ddos-what-is-the-difference.html (con acceso el 27 de julio del 2014.)
73. Deibert, R., Palfrey, J., Rohozinski, R., y Zittrain, J. (septiembre del 2009.) Access Contested: Toward the Fourth Phase of Cyberspace Controls. Cap. 7, p. 139. http://www.idrc.ca/EN/Resources/Publications/openebooks/507-6/index.html#page_133 (con acceso el 8 de diciembre del 2015.)
74. Entrevista con un capacitador en seguridad digital de una organización internacional, que desea permanecer anónimo, enero del 2014.
75. Björksten, G. (4 de marzo del 2014.) "Reports from the Frontlines" Panel. RightsCon.
76. Whitcomb, D. (2 de enero del 2014.) Syrian Electronic Army Says It Hacked Into Skype's Twitter. Reuters. http://www.huffingtonpost.com/2014/01/02/syrian-electronic-army-skype_n_4529292.html (con acceso el 8 de diciembre del 2015.)
77. Fisher, D. (10 de abril del 2013.) "What is a Man-in-the-Middle Attack?". Kaspersky Lab Daily. https://blog.kaspersky.com/man-in-the-middle-attack/1613/ (con acceso el 8 de diciembre del 2015.)
78. Schneier, B. (22 de septiembre del 2009) "Hacking Two-Factor Authentication". Schneier on Security. https://www.schneier.com/blog/archives/ 2009/09/hacking_two-fac.html (con acceso el 8 de diciembre del 2015.)
79. Íbid.
80. Honan, M. (3 de agosto del 2012.) "Yes, I was hacked. Hard". Emptyage. http://www.emptyage.com/post/28679875595/yes-i-was-hacked-hard (con acceso el 8 de diciembre del 2015.)
81. Popkin, H. (23 de abril del 2013.) AP latest victim in string of Twitter break-ins by Syrian Electronic Army. NBCNews.com. http://news.ca.msn.com/top-stories/ap-latest-victim-in-string-of-twitter-break-ins-by-syrian-electronic-army (con acceso el 2 de febrero del 2014.)
82. Entrevistas con el Comité para la Protección de Periodistas, Reporteros Sin Fronteras, la Federación Internacional de Periodistas, y el Instituto Internacional para la Seguridad Informativa, enero del 2014.
83. Comité para la Protección de Periodistas. (2014.) 1046 Journalists Killed since 1992. Comité para la Protección de Periodistas. https://www.cpj.org/killed/. (con acceso el 8 de diciembre del 2015.) Según la metodología del CPJ, "periodistas amenazados" incluye "todas las formas de amenaza en cualquier momento antes de que un periodista fuese asesinado".
84. Kyiv Post. (4 de septiembre del 2013.) "Ukrainska Pravda demands investigation of clone site, paper". http://www.kyivpost.com/content/ukraine/ ukrainska-pravda-demands-investigation-of-clone-site-paper-329009.html (con acceso el 8 de diciembre del 2015.)

85. Aikins, M. (3 de mayo del 2012.) “The spy who came in from the code”. Columbia Journalism Review. http:// www.cjr.org/feature/the_spy_who_came_in_from_the _c.php?page=all (con acceso el 22 de febrero del 2014.)
86. Search SQLServer. “Data mining” [Extracción de datos]. http://searchsqlserver.techtarget.com/ definition/data-mining (con acceso el 8 de diciembre del 2015.)
87. Rights Con 2014. (4 de marzo del 2014.) Panel Session. “Watching the Observers: The Impact of Surveillance on Human Rights.” https://www.youtube.com/watch?v=rbqHyNtj9XU&list=PLprTand RM9601CNiMd4VVTglZ1YSglKGx (con acceso el 8 de diciembre del 2015.)
88. Czuchnowski, W. (8 de octubre del 2010.) Dziennikarze na celowniku służb specjalnych [Periodistas convertidos en objetivo por fuerzas especiales]. *Gazeta Wyborcza.* http://wyborcza.pl/Polityka/1,103835,8480752,D ziennikarze_na_celowniku_sluzb_specjalnych.html (con acceso el 8 de diciembre del 2015.); Fundación para los Derechos Humanos de Helsinki. (13 de octubre del 2010.) “Letter from the Helsinki Foundation for Human Rights to Donald Tusk, Prime Minister of Poland”. http://www.europapraw.org/en/news/list-do-premiera-w-sprawie-raportu-dotyczacego-wykonywania-wyrokow-etpcz (con acceso el 8 de diciembre del 2015.); Human Rights House. (14 de enero del 2011.) “Surveillance of Polish journalists case – new developments”. http://humanrightshouse.org/noop/page.php?p=Articles/15761.html&d=shdbylgzokyw (con acceso el 8 de diciembre del 2014.); Downie Jr., L. (10 de octubre del 2013.) Investigaciones sobre filtraciones y vigilancia en Estados Unidos post 11-s. https://www.cpj.org/es/2013/10/el-gobierno-de-obama-y-la-prensa.php (con acceso el 8 de diciembre del 2015.)
89. Consejo de Derechos Humanos. Promoción, protección y disfrute de los derechos humanos en Internet A/HRC/20/L.13, 29 de junio de2012. http://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_20_L13.pdf. (con acceso el 8 de diciembre del 2015).
90. Asamblea General de las Naciones Unidas (21 de septiembre del 2012.) La seguridad de los periodistas y la cuestión de la impunidad. http://www.acnur.org/t3/fileadmin/Documentos/BDL/2015/9631.pdf?view=1 (con acceso el 8 de diciembre del 2015.)
91. Íbid.
92. UNESCO. (2013.) Declaración de San José. Safe to Speak: Securing Freedom of Expression in all Media. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/WPFD/WPFD-San-Jose-Declaration-2013-en.pdf (con acceso el 8 de diciembre del 2015.)
93. Conferencia General de la UNESCO, 37ª sesión, noviembre del 2013. Resolución sobre cuestiones relacionadas con Internet, con inclusión del acceso a la información y el conocimiento, la libertad de expresión, la privacidad y las dimensiones éticas de la sociedad de la información. http://unesdoc.unesco.org/images/0022/002261/226162s.pdf (p. 58) (con acceso el 8 de diciembre del 2015.)
94. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (1 de julio del 2013.) “La seguridad de los periodistas. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.” http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/153/22/PDF/G1315322.pdf?OpenElement (con acceso el 8 de diciembre del 2015.)
95. Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. (30 de junio del 2014.) “La privacidad en la era digital”. www.ohchr.org/EN/HRBodies/HRC/.../A-HRC-27-37_sp.doc (con acceso el 8 de diciembre del 2015.)
96. Ministros de la Coalición por la Libertad Online. (28 de abril del 2014.) “Recommendations for Freedom Online”. https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf (con acceso el 8 de diciembre del 2015.)

97. Access. (2014.) RightsCon. https://www.rightscon.org/ (con acceso el 8 de diciembre del 2015.)
98. Global Voices. (1 de enero del 2014.) 4ª Reunión de Blogueros Árabes. Global Voices. http://ab14.globalvoicesonline.org/english (con acceso el 8 de diciembre del 2015.)
99. Reunión del Consejo de Asuntos Exteriores. (12 de mayo del 2014.) "EU Human Rights Guidelines on Freedom of Expression Online and Offline". http://eeas.europa.eu/delegations/documents/eu_human_rights_guidelines_on_freedom_of_expression_online_and_offline_en.pdf (con acceso el 8 de diciembre del 2015.)
100. Nils Muiznieks. (19 de mayo del 2014.) https://twitter.com/CommissionerHR/status/468298394092699648 (con acceso el 8 de diciembre del 2015.)
101. Organización para la Seguridad y la Cooperación en Europa. (2 de mayo del 2014.) Safety for Journalist. Guidebook (2ª edición). http://www.osce.org/fom/118052?download=true. (con acceso el 9 de diciembre del 2015.)
102. Comisión Nacional del Reino Unido para la UNESCO. (2014.) http://www.unesco.org.uk/journalist_safety (con acceso el 11 de marzo del 2014.)
103. E-mail de Privacy International, 15 de enero del 2014.
104. Comisión Africana sobre Derechos Humanos y de las Personas. (2014.) "Activity Report of Advocate Pansy Tlakula as the special rapporteur on freedom of expression and access to information in Africa". http://www.achpr.org/sessions/55th/intersession-activity-reports/faith-pansy-tlakula/ (con acceso el 9 de diciembre del 2015.)
105. Unwanted Witness. (1 de febrero del 2014.) https://unwantedwitness.or.ug/about-us/ (con acceso el 9 de diciembre del 2015.)
106. Iniciativa para Medios de Comunicación Africanos. (12 de julio del 2014.) http://africanmediainitiative.org /about (con acceso el 9 de diciembre del 2015.)
107. Justin Arenstein. (12 de julio del 2014.) http://www.linkedin.com/in/justinarenstein (con acceso el 9 de diciembre del 2015.)
108. Centro de Medios de Comunicación Independientes del Kurdistán. (16 de enero del 2014) Start training for Iraqi Journalists on Ethnic and Religious minorities. http://imckiraq.blogspot.com/ (con acceso el 9 de diciembre del 2015.)
109. http://www.internews.org/research-publications/digital-security-and-journalists-snapshot-awareness-and-practice-pakistan
110. Véase "The Safety of Journalists and the Danger of Impunity". Informe del Director General del Consejo Intergubernamental del IPDC (Sesión Vigésimo Novena). CI-14/CONF.202/4 Rev2. http:// unesdoc.unesco.org/images/0023/002301/230101E.pdf
111. UNESCO. (10 de marzo del 2014.) "Training on digital security for Tunisian journalists". http://www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/all-news/news/training_on_digital_security_for_tunisian_journalists/#.VmhE77h97IU (con acceso el 9 de diciembre del 2015.)
112. IREX. (1 de febrero del 2014.) SAFE – Securing Access to Free Expression. IREX. https://www.irex.org/projects/safe (con acceso el 9 de diciembre del 2015.)
113. Artículo 19. (20 de diciembre del 2012.) Kenya: Safety training for journalists in response to increasing dangers in region. Artículo 19. http://www.article19.org/resources.php/resource/3570/en/kenya:-safety-training-for-journalists-in-response-to-increasing-dangers-in-region (con acceso el 9 de diciembre del 2015.)
114. Seguridad Global para Periodistas. (julio del 2014.) Curso de julio: Seguridad digital para reporteros sobre seguridad nacional. https://www.journalistsecurity.net/2013/07/03/digital-safety-for-national-security-reporters/ (con acceso el 9 de diciembre del 2015.)

115. Instituto Internacional de Prensa. (17 de enero del 2014.) IPI'S news innovation platform is almost here. http://www.ipinewsinnovation.org/news/ipis-news-innovation-platform-is-almost-here.html (con acceso el 9 de diciembre del 2015.)
116. Entrevista con Andrew Ford Lyons, 13 de diciembre del 2013.
117. Instituto Internacional para la Seguridad Informativa. (5 de febrero del 2014.) Seguridad en el periodismo: Amenazas a los trabajadores de medios de comunicación y medidas para protegerlos. INSI. http://www.newssafety.org/uploads/Good%20Practice%20INSI%20Final%20Feb2014.pdf (con acceso el 09 de diciembre del 2014.)
118. Derechos Digitales. (2013.) Derechos digitales. Reporte anual. Derechos Digitales ONG 2013. https://www.derechosdigitales.org/wp-content/uploads/DDigitales-Memoria-Anual-2013.pdf (con acceso el 9 de diciembre del 2015.)
119. http://www.fopea.org/seguridad-periodistas/
120. http://periodismocide.org/curso-de-seguridad-digital/
121. http://www.sipiapa.org/notas/1154059-redes-sociales-seguras-su-uso-personal-profesional-e-institucional
122. Reporteros Sin Fronteras. (1 de febrero del 2014.) Era of the digital mercenaries. Reporteros Sin Fronteras. http://surveillance.rsf.org/es/ (con acceso el 9 de diciembre del 2015.)
123. Comité para la Protección de Periodistas. (2014.) Technology security. http://www.cpj.org/reports/2012/04/information-security.php (con acceso el 9 de diciembre del 2015.); Lee, M. (2 de julio del 2013.) Encryption Works: How to Protect Your Privacy in the Age of NSA Surveillance. https://pressfreedomfoundation.org/encryption-works (con acceso el 9 de diciembre del 2015.); Fundación Fronteras Electrónicas. (2013.) Autoprotección Digital Contra La Vigilancia: Consejos, Herramientas y Guías Para Tener Comunicaciones Más Seguras https://ssd.eff.org/es (con acceso el 9 de diciembre del 2015.); Fundación Fronteras Electrónicas. (2014.) Deeplinks. https://www.eff.org/deeplinks (con acceso el 9 de diciembre del 2015)
124. Asociación para las Comunicaciones Progresistas. (2014.) "Kit Digital de primeros auxilios para defensores de los Derechos Humanos". https://www.apc.org/es/irhr/kit-digital-de-primeros-auxilios (con acceso el 9 de diciembre del 2015.)
125. Centro SKeyes para Medios de Comunicación y Libertad Cultural. (1 de febrero del 2014.) The Journalist Survival Guide: An Animated Video Guide. http://video.skeyesmedia.org/ (con acceso el 9 de diciembre del 2015.)
126. Aryal, M. y Jones, D. (24 de marzo del 2014.) "SaferJourno: Digital Security Resources for Media Trainers". Internews. http://www.internews.org/research-publications/saferjourno-digital-security-resources-media-trainers (con acceso el 9 de diciembre del 2015.)
127. Internews. (24 de marzo del 2014.) SaferJourno Toolkit Provides Digital and Online Safety Resources for Journalism and Media Trainers. https://Internews.org/saferjourno-toolkit-provides-digital-and-online-safety-resources-journalism-and-media-trainers (con acceso el 9 de diciembre del 2015.)
128. Banda, F. (2013.) Plan modelo de estudios de periodismo. Colección de la UNESCO sobre los estudios de periodismo. http://unesdoc.unesco. org/images/0022/002211/221199e.pdf (con acceso el 9 de diciembre del 2015.)
129. Los investigadores enviaron la encuesta a contactos en la Asociación de Noticias Digitales de Radio y Televisión, la Asociación para la Formación en Periodismo y Comunicación de Masas, la Asociación para la Formación en Radiodifusión, el Centro Internacional para Periodistas, el Consejo de Asesores para Escuelas de Medios de Comunicación y la Red Internacional de Periodistas. La mayoría de los encuestados eran de Estados Unidos, pero también hubo participantes de Pakistán, Francia, Nigeria, Mongolia y Colombia. La encuesta estuvo activa desde el 14 de enero del 2014 hasta el 4 de febrero del 2014, aunque el link permaneció activo hasta agosto del 2014.

130. Revelación: el principal autor de este informe del 2015 formaba parte del Centro Tow para Periodismo Digital de la Escuela de Periodismo de Columbia.
131. McGregor, S. (29 de octubre del 2013.) Register for the Tow Center's Journalism Security Workshop. http://towcenter.org/blog/register-for-the-tow-centers-journalism-security-workshop/ (con acceso el 9 de diciembre del 2015.)
132. Benton, J. (26 de marzo del 2014.) Columbia's Year Zero, aiming to give journalists literacy in data, is now called the Lede Program. http://www.niemanlab.org/2014/03/columbias-year-zero-aiming-to-give-journalists-literacy-in-data-is-now-called-the-lede-program/ (con acceso el 9 de diciembre del 2015.)
133. E-mail de Jane E. Kirtley, 13 de enero del 2014.
134. E-mail de Sandeep Junnarkar, 16 de enero del 2014.
135. Kirchner, L. (15 de noviembre del 2013.) CJR: Teaching j-school students cyber. Columbia Journalism Review. http://www.cjr.org/behind_the_news/teaching_cybersecurity_in_jsch.php (con acceso el 9 de diciembre del 2015.)
136. Íbid.
137. E-mail de Ismail Hakki Polat, 23 de marzo del 2014.
138. Universidad Kadir Has. Syllabus for NM 204 Information Security. http://www.khas.edu.tr/en/uploads/makser/NM204_syllabus_2012.pdf (con acceso el 22 de marzo del 2014.)
139. Correspondencia en Twitter con Jorge Luis Sierra, 19 de marzo del 2014.
140. E-mail de Henrik P. Berggreen, Uddannelsesleder, Danmarks Medie – Og Journalist Hojskole, 27 de febrero del 2014.
141. Correspondencia en Twitter con la Escuela de Periodismo de la Academia de la BBC, 20 de marzo del 2014.
142. Smyth, F. (2013.) Digital Security Basics for Journalists. Medill National Security Zone: A Resource for Covering National Security Issues. http://nationalsecurityzone.org/site/digital-security-basics-for-journalists/ (con acceso el 9 de diciembre del 2015.)
143. Comité Internacional de la Cruz Roja. (1 de enero del 2006.) LÍNEA DIRECTA: asistencia para periodistas en misión peligrosa. https://www.icrc.org/es/document/linea-directa-asistencia-para-periodistas-en-mision-peligrosa (con acceso el 9 de diciembre del 2015.)
144. E-mail de Erin Murrock, 3 de abril del 2014.
145. Hammad, A. (18 de febrero del 2014.) Hackathon: Hacking for a Better World. Guardian Liberty Voice. http://guardianlv.com/2014/02/hackathon-hacking-for-a-better-world/ (con acceso el 9 de diciembre del 2015.)
146. Open ITP. 18 de febrero del 2014. About Us. Open ITP. https://openitp.org/openitp/about-the-open-internet-tools-project.html (con acceso el 18 de febrero del 2014.)
147. Open ITP Wiki. (12 de febrero del 2014.) Techno-Activism 3rd Mondays. Open ITP. https://wiki.openitp.org/doku.php?id=events:techno-activism_3rd_mondays (con acceso el 9 de diciembre del 2015.)
148. Hacks/Hackers. (18 de febrero del 2014.) About. Hack/Hackers. http://hackshackers.com/about/ (con acceso el 9 de diciembre del 2015.)
149. Íbid.
150. "Hancel: Creando redes para proteger periodistas". http://hanselapp.com/index.html (con acceso el 9 de diciembre del 2015.)
151. Romero, C. (febrero del 2014.) What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World. Freedom House. https://freedomhouse.org/report/special-reports/what-next-quest-protect-human-rights-defenders-and-journalists-digital-world (con acceso el 9 de diciembre del 2015.)
152. PEN America (13 de noviembre del 2013.) The Rise of Digital Repression: a PEN Interactive Report.

153. Comité para la Protección de Periodistas. (12 de febrero del 2014.) Ataques a la prensa: periodismo bajo fuego cruzado en 2013. https://cpj.org/es/2014/02/ataques-a-la-prensa-en-2013.php (con acceso el 9 de diciembre del 2015.); Phillips, K. (6 de febrero del 2014.) CPJ-Lista de Riesgo: Donde peligra la libertad de prensa. https://cpj.org/es/2014/02/ataques-a-la-prensa-en-2013-cpj-lista-de-riesgo-donde-peligra-la-libertad.php (con acceso el 9 de diciembre del 2015.)
154. Ritchin, A. (21 de marzo del 2013.) "Los ataques contra Mujeres Periodistas del Enfoque de Grupo de la ONU". Dart Blog. http://dartcenter.org/blog/attacks-on-women-journalists-focus-un-panel#.Uu1atHddVgL (con acceso el 9 de diciembre del 2015.)
155. Instituto Internacional para la Seguridad de la Prensa y Fundación Internacional de Medios de Comunicación de Mujeres. (10 de marzo del 2014.) Global Report on the Status of Women in the News Media. https://www.iwmf.org/wp-content/uploads/2013/09/IWMF-Global-Report-Summary.pdf (con acceso el 9 de diciembre del 2015.)
156. El acoso sexual fue definido por los siguientes actos: 1) Contacto físico no deseado (como toqueteos u otro tocamiento de áreas sensibles); 2) Invasión del espacio personal; 3) Comentarios o sonidos insinuantes; 4) Comentarios no deseados sobre la vestimenta o la apariencia; 5) Bromas de naturaleza sexual; 6) Despliegue de material sexualmente ofensivo; 7) Descarga inapropiada de material pornográfico o sexualmente abusivo y degradante mediante la computadora; 8) Amenazas verbales (de naturaleza sexual); 9) Otros.
157. Instituto Internacional para la Seguridad de la Prensa y Fundación Internacional de Medios de Comunicación de Mujeres. (10 de marzo del 2014.) Global Report on the Status of Women in the News Media. https://www.iwmf.org/wp-content/uploads/2013/09/IWMF-Global-Report-Summary.pdf (con acceso el 9 de diciembre del 2015.)
158. Wolfe, L. (febrero del 2012.) "More Discussion but Few Changes on Sexual Violence". Comité para la Protección de Periodistas. https://www.cpj.org/2012/02/attacks-on-the-press-in-2011-the-changing-views-on.php (con acceso el 9 de diciembre del 2015.); Wolfe, L. (7 de junio del 2011.) "El Crimen Silenciado: Violencia Sexual y Periodistas" . Comité para la Protección de Periodistas. https://cpj.org/es/2011/06/el-crimen-silenciado-violencia-sexual-y-periodista.php (con acceso el 9 de diciembre del 2015.)
159. Padte Kaul, R. (5 de julio del 2013.) "Walking Down A Virtual Boulevard". http://richakaulpadte.com/ category/gender/ (con acceso el 9 de diciembre del 2015.)
160. Padte Kaul, R. (29 de junio del 2013.) "Keeping women safe? Gender, online harassment and Indian law". http://internetdemocracy.in/media/keeping-women-safe-gender-online-harassment-and-indian-law-2/ (con acceso el 9 de diciembre del 2015.)
161. Halt Abuse. (2000-2012.) WHOA (haltabuse.org) Comparison statistics 2000-2012. Halt Abuse. http://www.haltabuse.org/resources/stats/Cumulative2000-2012.pdf (con acceso el 9 de diciembre del 2015.)
162. Meyer, R. y Cukier, M. (2006.) "Assessing the Attack Threat due to IRC Channels". Actas de la Conferencia Internacional sobre Sistemas y Redes Fiables. http://www.umiacs.umd.edu/publications/assessing-attack-threat-due-irc-channels (con acceso el 9 de diciembre del 2015.)
163. E-mail del Dr. Michel Cukier, 11 de abril del 2014.
164. Instituto Internacional para la Seguridad de la Prensa y Fundación Internacional de Medios de Comunicación de Mujeres. (10 de marzo del 2014.) Global Report on the Status of Women in the News Media. https://www.iwmf.org/wp-content/uploads/2013/09/IWMF-Global-Report-Summary.pdf (con acceso el 9 de diciembre del 2015.)

165. Citron Keats, D. (25 de noviembre del 2009.) “Law’s Expressive Value in Combating Cyber Gender Harassment”. Michigan Law Review. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1352442 (con acceso el 9 de diciembre del 2015.)
166. íbid.
167. Íbid.
168. Índice sobre Censura. (1 de abril del 2014.) “Twitter trolls in India: Sexist abuse as a tool to muzzle women”. https://www.ifex.org/india/2014/04/04/trolls_muzzle_women/ (con acceso el 5 de abril del 2014.)
169. Íbid.
170. Anand, A. (8 de febrero del 2014.) “Kavita Krishnan: ‘I was accused by one minister of standing for free sex”. The Observer. http://www.theguardian.com/politics/2014/feb/09/kavita-krishnan-communist-india-accused-minister-free-sex (con acceso el 2 de abril del 2014.)
171. Penny, L. (4 de noviembre del 2011.) “Laurie Penny: A woman’s opinion is the mini-skirt of the Internet” [Laurie Penny: La opinión de una mujer es la minifalda de Internet]. The Independent. http://www.independent.co.uk/voices/commentators/laurie-penny-a-womans-opinion-is-the-miniskirt-of-the-internet-6256946.html (con acceso el 3 de abril del 2014.)
172. Índice sobre Censura. (1 de abril del 2014.) “Twitter trolls in India: Sexist abuse as a tool to muzzle women.” https://www.ifex.org/india/2014/04/04/trolls_muzzle_women/ (con acceso el 5 de abril del 2014.)
173. Wallace, Amy. (19 de enero del 2014.) Life as a Female Journalist: Hot or Not? [Mi vida como mujer periodista: ¿Caliente o no?]. New York Times. http:// www.nytimes.com/2014/01/20/opinion/life-as-a-female-journalist-hot-or-not.html (con acceso el 22 de febrero del 2014.)
174. Íbid.
175. Vittal, V. (27 de julio del 2013.) “Online Abuse of Women: Why trolls have it so easy” [Abuso online de mujeres: ¿Por qué los trolls lo tienen tan fácil?]. http://indiatogether. org/internet-women (con acceso el 4 de abril del 2014.)
176. Masters, J. (6 de marzo del 2014.) “Sexism in sport: Why do Internet trolls target women?” [Sexismo en el deporte: ¿Por qué los trolls de Internet convierten a las mujeres en objetivo?]. CNN. http:// edition.cnn.com/2014/03/06/sport/sexism-in-sport-female-journalists-abuse/ (con acceso el 4 de abril del 2014.)
177. Democracia Alimentaria Ahora! “New York Times Writer Amy Harmon travels to Hawaii…falls in love with GMOs” [Amy Harmon, escritora del New York Times, viaja a Hawái…se enamora de los GMOs]. Página de Facebook de Democracia Alimentaria Ahora! https://www.facebook.com/photo.php?fbid=10152209502794388&set=a.10150644870149388.450934.162878479387&type=1&theater (con acceso el 20 de marzo del 2014.)
178. Wallace, Amy. (19 de enero del 2014.) ‘Life as a Female Journalist: Hot or Not?’ New York Times. http://www.nytimes.com/2014/01/20/opinion/life-as-a-female-journalist-hot-or-not.html (con acceso el 22 de febrero del 2014.)
179. IREX. (21 de noviembre del 2013.) “Gender-Based Violence Against Journalists: Realities and Responses” [Violencia de género contra mujeres: Realidades y respuestas]. http://www.irex.org/news/gender-based-violence-against-journalists-realities-and-responses (con acceso el 22 de enero del 2014.)
180. Comité para la Protección de Periodistas. (2013.) “Janet Hinostroza, Ecuador: 2013 CPJ International Press Freedom Awardee” [Janet Hinostroza, Ecuador: Galardonada con el Premio a la Libertad de Prensa Internacional 2013 del CPJ]. https://www.cpj.org/awards/2013/janet-hinostroza-ecuador.php (con acceso el 12 de marzo del 2014.)

181. Freeman, H. (30 de julio del 2013.) How to use the Internet without being a total loser [Cómo utilizar Internet sin ser un perdedor total]. The Guardian. http://www.theguardian.com/commentisfree/ 2013/jul/30/how-use-internet-loser-twitter (con acceso el 29 de julio del 2014.)
182. Williams, H. (9 de agosto del 2013.) "Twitter bomb threats: Online and offline, female journalists face abuse 'all the time.'" [Amenazas de bomba en Twitter: Online y offline, las periodistas se enfrentan a abusos 'todo el tiempo']. Reuters. http://www.trust.org/item/20130809124626-79zhw/?source=shtw (con acceso el 9 de febrero del 2014.)
183. Conversión por e-mail con un tecnólogo en seguridad digital que pidió permanecer anónimo.
184. El ciberacoso puede también incluir: amenazas reiteradas o falsas acusaciones vía e-mail o teléfono celular, realizar posts amenazantes o falsos en sitios web, robar la identidad o datos de una persona o espiar y monitorear la computadora y el uso de Internet de una persona. A veces las amenazas pueden elevarse de categoría hasta espacios físicos.
185. Kee, J. "Cultivating Violence through Technology? Exploring the Connections between Information Communication Technologies (ICT) and Violence Against Women (VAW.)" [¿Cultivando la violencia a través de la tecnología? Explorando las conexiones entre las Tecnologías de la Información y las Comunicaciones (TIC) y la violencia contra las mujeres]. Programa de Apoyo a Redes de Mujeres de la Asociación para Comunicaciones Progresistas. http://www.genderit.org/sites/default/ upload/VAW_ICT_EN.pdf. (con acceso el 12 de marzo del 2014.)
186. Strawhun, J., Adams, N., y Huss, M. (2013.) "The Assessment of Cyberstalking: An Expanded Examination Including Social Networking, Attachment, Jealousy, and Anger in Relation to Violence and Abuse" [La evaluación del ciberacoso: Un amplio examen incluyendo redes sociales, apego, celos e indignación en relación con la violencia y el abuso]. Violence and Victims. Springer Publishing Company. 28.4: 715-30.
187. Strawhun, J., Adams, N., y Huss, M. (2013.) "The Assessment of Cyberstalking: An Expanded Examination Including Social Networking, Attachment, Jealousy, and Anger in Relation to Violence and Abuse". *Violence and Victims*. Springer Publishing Company. 28.4: 715-30; Anónimo. (abril del 2000.); "Beware of cyberstalking—the latest workplace threat" [Cuidado con el ciberacoso – la más reciente amenaza en el lugar de trabajo]. HR Focus 77.4. Con acceso a través de ProQuest.
188. Asociación para las Comunicaciones Progresistas (APC) Mujeres (1 de noviembre del 2010.) "How Technology is Being Used to Perpetrate Violence against Women – and to Fight It" [Cómo la tecnología se está utilizando para perpetrar violencia contra las mujeres – y cómo combatirlo]. http://www.comminit.com/content/how-technology-being-used-perpetrate-violence-against-women-and-fight-it (con acceso el 3 de abril del 2014.)
189. Moore, A. (3 de febrero del 2014.) "Cyberstalking and Women – Facts and Statistics: Few Laws in Place to Deal With This Rapidly Growing Threat" [Ciberacoso y mujeres – Hechos y estadísticas: Pocas leyes vigentes para abordar esta amenaza en rápido aumento]. http://womensissues.about.com/od/ violenceagainstwomen/a/CyberstalkingFS.htm (con acceso el 2 de abril del 2014.)
190. Universidad Estatal Sam Houston. (9 de febrero del 2013.) "New Study Compares Stalking, Cyberstalking" [Nuevo studio compara acoso y ciberacoso]. US Fed News Service. HT Media Ltd. Con acceso a través de ProQuest.
191. Rupley, S. (17 de junio del 2003.) "Cyberstalking On the Rise: Stay alert when online" [Ciberacoso en auge: Manténgase alerta cuando esté online]. PC Magazine. Ziff-Davis Media Inc. Vol. 22, No. 10. Con acceso a través de ProQuest.

192. Pittaro, M. (2007) “Cyberstalking: An Analysis of Online Harassment and Intimidation” [Ciberacoso: Un análisis del acoso y la intimidación online]. International Journal of Cyber Criminology. Vol. 1 (2): 180-197. http://www.cybercrimejournal.com/pittaroijccvol1is2.htm (con acceso el 1 de abril del 2014.)
193. Ginty, M. (2 de mayo del 2011.) “Cyberstalking Turns Web Technologies into Weapons” [El ciberacoso convierte las tecnologías web en armas]. WeNews. http://womensenews.org/story/crime-policylegislation/110501/cyberstalking-turns-web-technologies-weapons?page=0,1#.UvjrKkJdUeY (con acceso el 12 de marzo del 2014.)
194. Quick, A. (2012.) “The Village Founder, Vickie Newton, Targeted by Internet Stalker” [La fundadora de The Village, Vickie Newton, convertida en objetivo de un acosador de Internet]. The Village Celebration. http://www.thevillagecelebration.com/thevillage-founder-vickie-newton-targeted-by-internet-stalker/ (con acceso el 11 de marzo del 2014.)
195. Instituto Internacional para la Seguridad de la Prensa y Fundación Internacional de Medios de Comunicación de Mujeres. (10 de marzo del 2014.) Violence and Harassment Against Women in the News Media: A Global Picture [Violencia y acoso contra las mujeres en los medios de noticias: Un retrato global]. http://www.iwmf.org/intimidation-threats-and-abuse/ (con acceso el 2 de abril del 2014.)
196. Friedersdorf, C. (7 de enero del 2014.) “When Misogynist Trolls Make Journalism Miserable for Women” [Cuando los trolls misóginos convierten el periodismo en un infierno para las mujeres]. The Atlantic. http://www.theatlantic.com/politics/archive/2014/01/when-misogynist-trolls-make-journalism-miserable-for-women/ 282862/ (con acceso el 12 de marzo del 2014.)
197. Hess, A. (6 de enero del 2014.) “Why Women Aren’t Welcome on the Internet” [¿Por qué las mujeres no son bienvenidas en Internet?]. Pacific Standard. http://www.psmag.com/navigation/health-and-behavior/women-arent-welcome-internet-72170/ (con acceso el 14 de marzo del 2014.)
198. Íbid.
199. Swim, J. K., Hyers, L. L, Cohen, L. L, y Ferguson, M. J. (2001). Everyday sexism: Evidence for its incidence, nature, and psychological impact from three daily diary studies [Sexismo cotidiano: Evidencias de su incidencia, naturaleza e impacto psicológico a partir de tres estudios de agendas diarias]. *Journal of Social Issues*, 57, 31-53.
200. Vittal, V. (27 de julio del 2013.) “Online Abuse of Women: Why trolls have it so easy.” http://indiatogether. org/internet-women (con acceso el 4 de abril del 2014.)
201. Halvorson, H. (6 de septiembre del 2011.) “Reasons Why It Pays to Not Let Sexist Comments Slide” [Razones por las que compensa no dejar pasar los comentarios sexistas] Forbes. http://www.forbes.com/sites/ heidigranthalvorson/2011/09/06/3-reasons-why-it-pays-to-not-let-sexist-comments-slide/2/ (con acceso el 20 de marzo del 2014.); Hillard, A. (1 de julio del 2011.) “Why Confronting Sexism Works: Applying Persuasion Theories to Confronting Sexism” [¿Por qué funciona confrontar el sexismo?: Aplicando teorías de la persuasión para confrontar el sexismo] Universidad de Nebraska-Lincoln. http://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1035& context=psychdiss (con acceso el 3 de abril del 2014.)
202. Hyers, L. L. (2007). Resisting prejudice every day: Exploring women’s assertive responses to anti-Black racism, anti-Semitism, heterosexism, and sexism [Contrarrestando los prejuicios a diario: Explorando las respuestas asertivas de las mujeres al racismo contra negros, al antisemitismo, al heterosexismo y al sexismo]. Sex Roles, 56, 1-12.
203. Tiger Beatdown. “But How Do You Know It’s Sexist? The #MenCallMeThings Roundup” [¿Pero cómo sabe que es sexist?: El compendio del *hashtag* #LosHombresMeLlamanDeTodo]. http:// tigerbeatdown.com/2011/11/10/ but-how-do-you-know-its-sexist-the-mencallmethings-round-up/ (con acceso el 29 de marzo del 2014.)

204. Chemaly, S. (28 de enero del 2013.) “The Digital Safety Gap and the Online Harassment of Women” [El vacío en la seguridad digital y acoso online a mujeres]. The Huffington Post. http://www.huffingtonpost.com/soraya-chemaly/women-online-harassment_b_2567898.html?utm_hp_ref=tw (con acceso el 29 de marzo del 2014.)
205. Padte Kaul, R. (5 de julio del 2013.) ‘Walking Down A Virtual Boulevard’. http://richakaulpadte.com/ category/gender/ (con acceso el 1 de abril del 2014.)
206. Colectivo para una Tecnología Táctica. “About the Campaign: What is Take Back the Tech?” [Acerca de la campaña: ¿Qué es Reclamar la Tecnología]. https://www.takebackthetech.net/page/about-campaign (con acceso el 2 de abril del 2014.)
207. Asociación para Comunicaciones Progresistas. “How Technology is Being Used to Perpetrate Violence Against Women – And to Fight it.” https://www.apc.org/en/system/files/How-Technology-is-Being-Used-to-Perpetrate-Violence-Against-Women-––-And-to-Fight-it.pdf (con acceso el 14 de marzo del 2014.)
208. Asociación para Comunicaciones Progresistas. “Cyberstalking and how to prevent it” [El ciberacoso y cómo evitarlo]. Take Back the Tech. https://www.takebackthetech.net/be-safe/2-cyberstalking-and-how-prevent-it (con acceso el 12 de marzo del 2014.)
209. Asociación para Comunicaciones Progresistas. “Map it. End it” [Mapéalo. Acaba con ello]. Take Back the Tech. https://www. takebackthetech.net/mapit/ (con acceso el 12 de marzo del 2014.)
210. HarassMap. Lo que nosotros hacemos. http://harassmap.org/en/what-we-do/ (con acceso el 4 de abril del 2014.)
211. Tumblr. (27 de enero del 2014.) Lineamientos comunitarios. http://www.tumblr.com/policy/en/community (con acceso el 21 de marzo del 2014.)
212. Fernando, A. (31 de enero del 2014.) “How to Stop the Online Harassment of Female Journalists” [Cómo acabar con el acoso online de las mujeres periodistas]. 10,000 Words. http://www.mediabistro.com/10000words /harassment-female-journalists_b25653 (con acceso el 22 de marzo del 2014.)
213. Estas recomendaciones se extraen de entrevistas en profundidad con diversas fuentes, así como publicaciones de Access, Derechos Digitales Europeos (EDRi), Reporteros Sin Fronteras, el Comité para la Protección de Periodistas y la TED Talk de marzo del 2014 con Edward Snowden (reportada por Wired).
214. Resoluciones A/RES/68/167 y A/RES/69/116 de la Asamblea General de las Naciones Unidas.
215. Conferencia General de la UNESCO (noviembre del 2013.) Resolución sobre cuestiones relacionadas con Internet: incluyendo acceso a la información y el conocimiento, libertad de expresión, privacidad y dimensiones éticas de la sociedad de la información. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_internet.pdf (con acceso el 29 de julio del 2014.)
216. Naciones Unidas. (21 de febrero del 2014.) La seguridad de los periodistas y la cuestión de la impunidad. http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/163 (con acceso el 30 de julio del 2014.)
217. Björksten, G. (27 de marzo 2014.) “Innovating our Future: Gustaf Björksten.” Innovating Our Future. https://www.youtube.com/watch?v=pMae8pZC4DE (con acceso el 31 de marzo del 2014.)
218. McGregor, S. y Ag, M. (17 de marzo 2014.) “TA3M on JournoSec with Susan McGregor of Columbia and Magnus Ag of Committee to Protect Journalists.” https://www.youtube.com/watch ?v=tu0_ySgLgys&feature=youtu.be (con acceso el 20 de marzo del 2014.)
219. Stray, J. (21 de agosto del 2014.) Security for Journalists, Part Two: Threat Modeling [Seguridad para periodistas, Parte 2: Modelo de amenazas]. https://source.opennews.org/en-US/learning/security-journalists-part-two-threat-modeling/ (con acceso el 22 de agosto del 2014.)

220. Banda, F. 2013. Model Curricula for Journalism Education: A Compendium of New Syllabi. Serie de la UNESCO sobre Formación en Periodismo. http://unesdoc.unesco.org/images/0022/002211/ 221199e.pdf (con acceso el 30 de julio del 2014.)
221. Romero, C., (febrero del 2014.) "Conference Report: What Next? The Quest to Protect Journalists and Human Rights Defenders in a Digital World." Freedom House. http://www.freedomhouse.org/report/special-reports/what-next-quest-protect-human-rights-defenders-and-journalists-digital-world#.U_D45FbrPa5 (con acceso el 8 de marzo del 2014.)
222. Conferencia General de la UNESCO. (noviembre del 2013.) Resolución sobre cuestiones relacionadas con Internet: incluyendo acceso a la información y el conocimiento, libertad de expresión, privacidad y dimensiones éticas de la sociedad de la información. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_internet.pdf (con acceso el 1 de agosto del 2014.)
223. Resolución A/HRC/27/L.7 de la Asamblea General de las Naciones Unidas, adoptada por el Consejo de Derechos Humanos, sesión vigésimo séptima.
224. Josh Levy en 2014 era Director de Defensa en Access.
225. Josh Stearns en 2014 era Director de Periodismo y Sostenibilidad de la Fundación Geraldine R. Dodge.
226. Lindsey Beck en 2014 era Director de Programas para el Fondo de Tecnologías Abiertas de Radio Free Asia.
227. Paul Mooney en 2014 era Corresponsal Jefe de Reuters en Rangún.
228. Seamus Tuohy en 2014 era Asesor Técnico de Internews.
229. La encuesta se ofreció en inglés, francés, chino, árabe y español.
230. Los investigadores pidieron a sus contactos de las siguientes organizaciones que difundieran la encuesta: Instituto Internacional de Seguridad en las Noticias, Junta de Internacional de Investigación e Intercambios, Comité para la Protección de Periodistas, Global Voices, Federación Internacional de Periodistas, CommunityRED, Centro Tow para Periodismo Digital, Asociación de Noticias Online, Poynter, PEN Internacional, Sociedad de Periodistas Profesionales, y Open ITP. QuestionPro difundió también la encuesta a sus panelistas en varios países.
231. Hubo 18 participantes en el estudio piloto que finalizaron la encuesta.

Con el fin de mejorar el entendimiento a nivel global sobre las incipientes amenazas a la seguridad vinculadas a los desarrollos digitales, la UNESCO encargó esta investigación dentro de los esfuerzos actuales de la Organización por implementar el Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad, de carácter interinstitucional y encabezado por la UNESCO. Dicho Plan de las Naciones Unidas nació a partir del Programa Internacional para el Desarrollo de la Comunicación (PIDC) de la UNESCO, que concentra gran parte de su labor en promover la seguridad para los periodistas.

La seguridad de los periodistas, incluyendo la seguridad digital, es un tema de interés público de gran envergadura. Es vital para quienes se dedican al periodismo, para sus familias y para sus fuentes. Es esencial para el bienestar de las instituciones de medios de comunicación, la sociedad civil, el mundo académico y el sector privado en términos más amplios. Si valoramos el libre flujo de información para los ciudadanos, sus gobiernos y sus organizaciones internacionales, entonces la seguridad de los periodistas resulta fundamental.

Getachew Engida
Director General Adjunto de la UNESCO

Organización
de las Naciones Unidas
para la Educación,
la Ciencia y la Cultura

Sector de la Comunicación e Información

978-92-3-300038-4