Capítulo 2

Ciberagresión: una modalidad de ataque a periodistas digitales en Colombia

Mariana Cruz-Luna[1]
mariana.cruz@ucp.edu.co
Mariana López-Beltrán[2]
mariana.lopez@ucp.edu.co
Paula Andrea Rendón-Cardona
paula.rendon@ucp.edu.co[3]

Resumen

Toda acción que atenta contra la integridad laboral, familiar o personal de sujetos en la web se comprende como ciberagresión. Esta se viene consolidando como modalidad de acoso a periodistas, con acciones que van de la exposición y suplantación de la identidad hasta el señalamiento y persecución.

Tal modalidad de acoso desencadena graves consecuencias para el ejercicio de periodistas que se enfrentan a la contaminación de equipos, publicación de datos personales, acceso ilegal a archivos, geolocalización, estigmatización y calumnias en su ejercicio profesional. A pesar de que esta agresión no ha tenido suficiente cubrimiento en el campo mediático, viene ganando espacio en países como México, Nicaragua, Argentina y Colombia; es objeto de análisis en el ámbito del derecho de este último país.

En este sentido, y desde un estudio de caso, la ciberagresión a periodistas se convierte en el centro de atención de la investigación periodística a profundidad narrada en el siguiente capítulo.

1 Comunicadora Social-Periodista de la Universidad Católica de Pereira (UCP). Intereses relacionados a la Radio y Periodismo Musical. Experiencia en investigación y participación en semilleros.
2 Comunicadora Social-Periodista de la Universidad Católica de Pereira (UCP), con intereses en comunicación pública y narrativas gráficas. Experiencia en proyectos para el desarrollo y periodismo comunitario.
3 Magíster en Comunicación Educativa, comunicadora Social–Periodista, docente de la Universidad Católica de Pereira (UCP), en el área de medios sonoros, coordinadora del proyecto Radio UCP.

Introducción

El periodismo ha enfrentado importantes retos asociados a la seguridad: investigar, producir y socializar información. Históricamente ha generado riesgos para el libre desarrollo del trabajo y la protección de la vida de sus profesionales.

Con el auge del internet y la migración de medios al campo digital, los riesgos antes confinados al campo físico mutan a lo digital. Por ello, en el siguiente capítulo se reconstruirán aspectos teóricos relacionados con la "ciberagresión" como categoría de análisis del periodismo virtual. Allí conceptos como *exploits*, hostigamientos, espionaje y *doxing*, entre otros, serán fundamentales para plantear la discusión en el gremio.

Posteriormente, y bajo una metodología práctica propia de la investigación periodística, se contrastarán las implicaciones de las indagaciones conceptuales frente a la vida de un grupo de periodistas cuyo trayecto y relevancia en medios como *El Tiempo*, *El Espectador* y *Canal Uno* los ha convertido en blanco de diferentes tipos de ciberagresión.

"La ciberagresión: una modalidad de ataque a periodistas digitales en Colombia" hace un llamado de atención frente a la importancia de abordar el fenómeno en ascenso de manera integral, donde intervengan actores que posibiliten acciones de control social y jurídico.

Palabras clave: ciberagresión, periodistas, investigación periodística, agresión digital.

Ciberagresión, un campo de observación

Como herramienta de difusión de mensajes e información, la web se ha posicionado de manera exitosa. Como bien estableció Rheingold (2004), es una revolución social, el mayor sistema de publicación conocido. Diecisiete años después de su adopción masiva, ha significado para el campo periodístico un paso de lo tradicional a lo multimedia; los medios han aceptado el imparable auge del internet como herramienta comunicativa.

El periodismo puede integrar todos los recursos y servicios que ofrece la web a su labor. Según Villalba y Corchado (2017), los aspectos positivos del uso del ciberespacio son numerosos: la nueva generación de capacidades en campos como la comunicación, la investigación científica, los procesos industriales o la gestión del conocimiento suelen hacerse evidentes para una gran parte de la población.

Además de las ventajas mencionadas, la web también trae riesgos que los periodistas deben enfrentar en su cotidianidad. Estos contemplan la recepción de amenazas por medio de comentarios que no se quedan allí, sino que trascienden en acciones que comprometen su integridad humana y real.

La compañía israelí Check Point se ha encargado de investigar a profundidad la seguridad informática, con el fin de proponer soluciones que aportan a la protección. En una de sus investigaciones ha establecido una lista de ciberagresiones; dentro de las más problemáticas presume que la nube puede ser un blanco fácil de ataque, pues es donde hay más datos e información almacenada.

Infectar con un virus a una plataforma de comunicación digital podría afectar a todos los que hacen parte del medio. Si se tratara del periodista, no solo se conseguiría acceso a los datos guardados, sino también al resto de información que se posee desde el ordenador, lo que incluye datos de protección de la identidad y rastreo.

Hoy en día los Estados deben prestar atención a los ataques que se presentan en los sistemas de información, administrados por el gobierno, las

empresas y los ciudadanos. Esta situación ha conformado un nuevo escenario que precisa atención de los diferentes actores políticos para adaptarse adecuadamente (Villalba y Corchado, 2017).

Según el mismo Villalba, entre los desafíos y retos que trae consigo el ciberespacio, se encuentran la protección y recuperación de los sistemas de infraestructuras críticas ante agresiones que se utilizan como nave para interferir e intervenir, en las actividades de ciudadanos y/u organizaciones.

El derecho a la intimidad debe conservar una estrecha relación con la libertad de expresión, el honor, la igualdad y el derecho a la información, como establece el art. 20 de la Constitución Política 1991 de Colombia. Sin embargo, en la actualidad ambos derechos se han visto perjudicados por la evolución de los medios en la web 2.0.

La facilidad que los avances tecnológicos brindan a los ciudadanos para publicar datos e imágenes personales, incluso sin autorización de sus titulares, se constituye en un fenómeno que precisa de acompañamiento jurídico en aquellos casos en los que el derecho a la intimidad se ve vulnerado (Castro *et al.*, 2016).

En línea con los planteamientos de Castro, la publicación de información personal de datos a través de las redes sociales puede presentar situaciones o riesgos que podrían vulnerar los derechos de las personas, tales como suplantación de identidad, manipulación de fotografías, obtención y envío de información sin autorización del titular, tergiversación del buen nombre, etc.

En el auge actual de la web 2.0, la información, la regulación y la normativa deben avanzar de manera simultánea. De igual forma, es necesario comprender la manera en la que los ciudadanos establecen vínculos personales desde cualquier parte del mundo. Con las nuevas tecnologías se hace necesario considerar cómo solucionar conflictos donde se vea perjudicado el derecho a la intimidad y al buen nombre. Santos (2008) expone que en el pasado la acción-reacción compartían la misma dimensión espaciotemporal, a diferencia de lo que ocurre con la acción tecnológica, pues puede prolongar sus consecuencias tanto en el tiempo como en el espacio.

Ortiz (2008, citado por Ávila et al, 2014) establece que la web 2.0 es un fenómeno informático y social enfocado en la creación y distribución de contenidos a través de internet, principalmente caracterizado por una comunicación abierta, global e inmediata, una descentralización de la autoridad al estar permitido la libre opinión en la red y la libertad de compartir casi cualquier contenido (p. 32).

En el año 2010, el Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia (MinTIC) hacen alusión a la web con su proyecto Introducción al uso de la web 2.0 en el Estado colombiano, definiendo que esta no solo es una revolución y un fenómeno social, sino también una transición que dio el internet, con el fin de acercarse más a los que estaban del otro lado de la pantalla. Su principal objetivo fue enfocar su producción en beneficio del usuario consumidor, aportando contenidos, desarrollos y aplicaciones que lograran suplir las necesidades de la población.

En el intento de comprender la inseguridad de la información almacenada en la web en un escenario aceptable para su evolución, es necesario analizar alguna de las categorías y/o variables que abarca la dinámica del ciberespacio.

Nissenbaum (2013) propone que la privacidad ha sido el grito de guerra en contra de otro conjunto de tecnologías: las computadoras basadas en las tecnologías electrónicas digitales, que día a día incrementan el poder de cada uno de los usuarios sobre la información, pues hoy brindan la posibilidad de reunir, almacenar, comunicar, analizar, manipular y usar datos sin autorización de quien la brinda, a partir de organizaciones, instituciones, sociedades o individuos.

Remolina (2005), por su parte, plantea que las TIC han contribuido de manera significativa al aceleramiento del fenómeno del tratamiento de la globalización y la transferencia internacional de datos personales. Gracias a la necesidad de circular internacionalmente datos personales, han surgido reglas que deben observarse de forma detallada, ya que los esfuerzos internos de protección no deben desvanecerse cuando son objeto de exportación.

Así mismo, al igual que la mayoría de los países latinoamericanos, Colombia aún no se ha considerado como un Estado que garantice un nivel

adecuado de protección. Según la Comisión Europea, para un país es importante asimilar ese nivel en tres puntos: 1) aumentar el grado de protección jurídica de la información ciudadana, ya que el modelo europeo tradicional se ha caracterizado por ser garantista, riguroso y efectivo en dichos aspectos. 2. Generar un espacio más competitivo para que el país sea un lugar en el que puedan realizarse negocios que implican transferencia de datos e información personal desde Europa. Por ejemplo, tal como sucede en los *call centers* internacionales. 3. Para finalizar, la protección efectiva de datos e información personal es considerada como un elemento consustancial de las sociedades democráticas (Remolina. 2005).

Ahora bien, a partir de la inseguridad y las falencias de protección que surgen con la era digital, surge el término ciberagresión, el cual se desarrolla en el mundo digital y atenta contra la integridad de los usuarios que la reciben. En el gremio del periodismo digital, este tipo de agresión afecta la labor, y perjudica tanto su trabajo como la vida personal. Este integra diferentes acciones de intimidación, que tienen como consecuencia la censura, la falta de acceso a la información e intercepción de esta, y otras consecuencias de carácter personal como la sensación constante de inseguridad.

La ciberagresión se materializa en acciones de suplantación de la identidad, exposición de datos personales en la web, acceso ilegal a archivos privados, así como la ubicación por geolocalización. Esta termina generando exposición de la vida personal, señalamientos y calumnias que afectan la identidad de periodista.

Tal agresión contempla toda acción o mensaje por parte del agresor que atente contra la integridad laboral o personal de la víctima. Hoy en día algunas de las diferentes agresiones tradicionales han migrado al ciberespacio, adaptándose a las modalidades que trae consigo el internet (FLIP, 2018).

A partir de la descripción planteada por Reporteros sin Fronteras y la Unesco (2015) en el Manual de Seguridad para Periodistas, la seguridad digital, tanto del periodista como de su círculo social, puede comprometerse fácilmente; por ejemplo, a través de campañas de *phising*, suplantación la identidad del usuario, con la intención de adquirir información confidencial a través de páginas o plataformas falsas. La capacitación sobre seguridad digital se considera según

la urgencia, hasta ahora, como algo sistemático e integral; es decir, excluye la seguridad operativa y la atención psicosocial.

Henrichsen, Betz y Lisosk (2016) deja en claro que las experiencias traumáticas previas pueden dar como resultado que los periodistas tomen decisiones equivocadas que lleven a una mayor inseguridad. Aun sabiendo de los riesgos con que corren los periodistas al ser amenazados por medio del ciberespacio, hay una falta de datos disponibles de manera pública que den registro de los tipos de ataques y amenazas digitales a las que se enfrentan día a día.

Retomando a la Unesco, la seguridad de los periodistas, sin hacer a un lado la seguridad digital, es un tema de interés general. Además, es de gran importancia para el bienestar de los diferentes medios de comunicación, la sociedad civil, el mundo académico y el sector privado. Si se da valor al libre flujo de la información, podría llegarse a la conclusión de que las garantías de seguridad para los periodistas son fundamentales.

La investigación periodística, como método de abordaje de la ciberagresión

El siguiente capítulo da cuenta de una investigación que, priorizando la praxis periodística como método, detectó a la ciberagresión, una práctica de vulneración al trabajo de periodistas en la red, como categoría de análisis. Los conceptos que giran alrededor de esta fueron determinantes en el estudio, así como la contrastación de estos en el campo periodístico, tomando como muestra un grupo de profesionales colombianos participantes en medios y con enfoques diversos, pero que compartían una misma situación: su experiencia con la ciberagresión.

Al analizar un proceso en desarrollo, la investigación buscó aportar elementos de disfunción al campo no solo desde la categoría sino del debate que requiere la acción de diversas esferas que incluyen, pero trascienden el campo periodístico. Es así como las agresiones detectadas se vincularon a unas subcategorías comunes, según sus implicaciones y formas de afectación: de lo tangible a lo digital, parásitos cibernéticos, al desnudo en la web y agresiones

confinadas en el ciberespacio. Estas fueron posteriormente analizadas bajo la experiencia de los periodistas y otros profesionales aportantes en la discusión.

Es claro que la experiencia o praxis (Morles, 2002) en esta investigación periodística se entendió como camino para lograr conocimiento nuevo, lo que da prioridad a métodos de naturaleza empírica como el trabajo de campo, análisis documental y experimentación, como caminos para acercarse a la realidad indagada.

Por la sensibilidad de los datos expuestos, los nombres de los periodistas y medios de comunicación participantes se mantendrán en anonimato y se referencian bajo una codificación como fuente. Además del análisis mencionado, los resultados de esta investigación, fruto de un trabajo de grado para optar por el título de Comunicación Social-Periodismo de la Universidad Católica de Pereira, se presentan en serie de reportajes sonoros, que se puede consultar en la página web del proyecto: https://www.ciberagredidos.com/.

Dando piel a la ciberagresión periodística

El trabajo de campo acá reportado se desarrolló durante el segundo semestre del año 2019, en las ciudades de Bogotá, Manizales y Pereira, con periodistas que han ocupado cargos directivos en importantes medios de comunicación nacionales, tales como *El Tiempo*, *El Espectador* y *Canal Uno*, al igual que han participado de investigaciones que han sido galardonadas por importantes organizaciones como Amnesty Media Awards.

Los trayectos en sus carreras profesionales y relevancia de los roles ejercidos convierten a estos periodistas en blanco de diferentes tipos de ciberagresión. Para llevar a cabo la discusión de este documento, y en coherencia con la protección de datos y la petición de los periodistas de proteger su identidad, los testimonios se presentarán de forma concreta, bajo la identificación de 'periodista 1 al 5'. A continuación, algunos datos relevantes de sus perfiles, que en el desarrollo del capítulo dejarán de ser generales, para personificar desde la experiencia a la ciberagresión objeto de análisis.

El periodista identificado como uno (1) ocupa un cargo directivo en la versión digital de uno de los medios de prensa más leídos en el país. En su desarrollo profesional, ha realizado publicaciones donde expone de forma abierta denuncias de corrupción que comprometen a diferentes gremios, en momentos coyunturales como épocas de elecciones. Este tipo de contenido se considera como riesgoso, ya que ha expuesto al profesional a diferentes ciberagresiones que incluyen amenazas, hostigamiento, invasión y espionaje. Agresiones que han afectado su tranquilidad mental, el libre desarrollo de su profesión y su vida personal.

El periodista identificado como dos (2), para la fecha es subdirector en el noticiero independiente con más *rating* en Colombia, cuenta con un amplio recorrido periodístico en el que suma su trabajo para *El Espectador* y la Fundación para la Libertad de Prensa. El importante rol que ha desarrollado en el gremio lo ha hecho merecedor de importantes premios otorgados por organizaciones internacionales. Así mismo, ha sido víctima en diferentes ocasiones de agresiones que han comprometido su integridad física y laboral. Su información personal ha sido vulnerada en diversas ocasiones, afrontando el robo, contaminación e interceptación de sus dispositivos electrónicos.

El periodista identificado como tres (3) ha trabajado en procesos gubernamentales, su labor se desenvuelve en distintas plataformas multimedia, donde tiene una fuerte presencia en la práctica del debate; también ha hecho parte de programas en reconocidas emisoras como Blu Radio. El hecho de atreverse a abrir espacios para la discusión y el debate ha implicado que tanto su integridad profesional como su vida privada se encuentren en constante riesgo; ha sido víctima de ataques, donde su información personal se ha expuesto al público y ha recibido amenazas e intimidaciones.

El periodista identificado como cuatro (4) se hace cargo de la dirección en un portal digital de noticias con centro en la ciudad de Pereira. El comunicador es referente para los ciudadanos y para otros medios de su tipo, como escenario de denuncia y participación desde lo local. Su desempeño en temas álgidos a nivel local y con la inclusión de ciudadanos como denunciantes ha puesto su integridad en peligro. A esto se suma el hecho de trabajar para una plataforma

digital cuyo medio de expansión principal es Facebook, lo que incrementa el riesgo que corre de recibir ciberagresiones.

Finalmente, el periodista identificado como cinco (5) ejerce un rol de asesoría para la protección, específicamente hacia periodistas. Se encarga de brindar un acompañamiento a reporteros que se encuentran en situación de vulnerabilidad. Este conoce las denuncias de primera mano, por los procesos de acompañamiento que ha realizado a nivel país; desde su relato se evidencian los crecientes riesgos del ejercicio periodístico en la web.

De lo tangible a lo digital: amenazas, hostigamientos, espionaje e invasión

Ciber, en línea o web, independientemente de su denominación, el periodismo en internet posibilita la creación de espacios para la libre expresión, incubándose escenarios de retroalimentación. La interactividad (Urdaneta, 2007) es un rasgo que se traduce en la posibilidad de que todos los interlocutores en el proceso comunicativo, tanto periodistas como el público, interaccionen recíprocamente con el medio y entre sí.

Sin embargo, y como se viene planteando, el uso de nuevas tecnologías como herramienta de comunicación humana abre las puertas a nuevos tipos de ataque enmarcados en la categoría de ciberdelito, que es:

> […] cualquier infracción punible, en el que se involucra un equipo informático y en el que el ordenador, teléfono, televisión, reproductor de audio o vídeo o dispositivo electrónico, en general, puede ser usado para la comisión del delito o puede ser objeto del mismo delito. (Rayón y Gómez Hernández, 2014).

En el trabajo de campo realizado, el periodista 1 compartió la experiencia que vivió al recibir una amenaza: después de realizar publicaciones sobre corrupción, en épocas electorales, recibió un correo electrónico proveniente de su cuenta corporativa, que lleva el nombre del medio en el que trabaja. En dicho correo, se le informó que su equipo había sido *hackeado* y el agresor tenía en su poder imágenes explícitas del periodista observando contenido pornográfico.

En el aviso, se le indicó que debía seguir una serie de indicaciones para evitar la difusión de este contenido en cuentas de su círculo social y corporativo.

Esta agresión experimentada por el periodista se considera como amenaza, al generar una intimidación directa o a través de terceros, con el anuncio de un ataque web que afectará su vida o integridad. Esta línea de agresión se relaciona con el hostigamiento, que consiste en la persecución y maltratos psicológicos que pueden afectar el mundo tangible del periodista.

La misma fuente periodística 1 afirmó que fue objeto de mensajes difamatorios que llegaban a sus cuentas personales, con la pretensión de acusarlo de cometer acciones ilegales y actos de infidelidad.

El periodista también compartió que una cuenta que aparecía registrada en Buenos Aires le hizo seguimiento a su esposa durante un largo tiempo, a través de redes sociales (Facebook, Twitter y Messenger). Este personaje ha optado por alejar su vida privada y la de su familia de las redes sociales y plataformas digitales, pues tal hostigamiento afectó su relación de pareja, puso en riesgo su buen nombre y la integridad de su familia.

El caso demuestra la posibilidad de que los periodistas se vean afectados por varios tipos de ciberagresión. Estas perjudican su desempeño laboral, con acciones que van de la censura y autocensura, como limitantes al momento de obtener y difundir información, hasta el cambio de sus hábitos en la vida digital, con el objeto de proteger la identidad. Tras recibir las agresiones mencionadas, el periodista 1 tomó la decisión de alejar a su hija de las redes sociales para blindar su información.

Otra manifestación de lo *ciber* a lo tangible reposa en la invasión y el espionaje, agresiones que implican una violación a la privacidad del periodista y tienen como fin interferir en su labor cotidiana. Dentro de esta categoría, se encuentran acciones como la intrusión a oficinas o domicilios, además de la intercepción y vigilancia a las comunicaciones.

La fuente periodística 2 compartió que ha realizado investigaciones políticas que han puesto su vida en riesgo, y como consecuencia, en distintas ocasiones, los atacantes han clonado su locación geográfica para conocer su ubicación directa. El periodista comentó que esta agresión la ha experimentado desde el inicio de su carrera. Dichas acciones se leen como invasión y espionaje atribuidos a su labor. Esta es solo una de las múltiples ciberagresiones experimentadas por el periodista.

Según lo encontrado, los ciberdelitos requieren un constante seguimiento; las labores investigativas policiacas y el empleamiento de nuevas tecnologías fungen como escenarios de contingencia para contrarrestar sus efectos. De lo contrario, pueden arreciar o mutar.

Parásitos cibernéticos: exploits de software y hardware

Las modalidades de ciberagresión no solamente implican una amenaza o un seguimiento directo; también se desarrollan a través de robos de información digital. En el contexto de un gobierno salpicado por supuestos vínculos paramilitares, al trabajar en un importante caso que comprometía una multinacional de alimentos, el periodista 2 experimentó un nuevo ciberataque.

Hacia el 2012, en el desarrollo de su investigación, supo que tal compañía estaba en búsqueda de su información, y en repetidas ocasiones intentaron *hackear* sus datos personales, ingresar a sus dispositivos electrónicos. Además del acecho, el reportero fue víctima del robo físico de 18 computadores.

La fuente compartió su experiencia donde fue víctima de diferentes tipos de ataques a su ordenador. Como medida de contingencia ante la situación, el reportero optó por recurrir a un profesional que le notificaba cuando alguien intentaba irrumpir en su sistema y tenía la tarea constante de poner sus cuentas y dispositivos en modo seguro.

Esto pone en evidencia la teoría de Gallagher y Greenwald (2014), que propone que la tecnología de vigilancia también se utiliza para infectar computadoras a través de implantes de *malware* que permiten el acceso de agresores en redes informáticas específicas.

Así mismo, se hace evidente la descripción realizada sobre la categoría, donde se plantea que dentro de los métodos de monitoreo y vigilancia se utiliza el *software* de intrusión para operar a través de vectores que atacan la seguridad. También se comprueba el planteamiento de la Fundación Fronteras Electrónicas (2014), donde se identifica que el periodista se convierte en un objetivo de vigilancia, ya que corre el riesgo de que le sean implantados de forma ilegal *bugs*, troyanos o dispositivos como micrófonos.

La fuente periodística 2 no solo manifestó ser víctima de *exploits* o virus para obtener acceso a la información almacenada en sus computadores, sino que también se ha visto afectado por hurtos a través del *phising*. Este tiene por objetivo, suplantar la identidad, robando datos personales y recopilando información de cuentas, así como claves.

Al desnudo en la web: doxing

El periodismo se encuentra en un momento histórico, en el que su lugar como guardián de las noticias e información es amenazado, no solo por las nuevas tecnologías, sino por la audiencia que recibe dicha información (Bruns, 2008). Tales audiencias no solo cuentan con herramientas fáciles de usar, diversas conexiones y dispositivos de alta tecnología, sino que también poseen habilidades para navegar e interactuar a través de la web 2.0, disponiendo de medios para pasar de ser receptores a creadores y portadores de la información.

En la investigación se identificó una categoría donde se relatan los obstáculos a los que se enfrentan los periodista para ejercer el derecho fundamental de acceder a la información pública. En el *doxing* se busca hacer públicos los datos de contacto a través de redes sociales, exponiendo teléfonos, direcciones o correos electrónicos.

El periodista 3, desde su reconocimiento como activista en las redes sociales, ha sido blanco de diferentes agresiones por sus opiniones políticas. En el trabajo de campo, compartió que, en una ocasión, después de haber dado una opinión que causó controversia, su número privado fue publicado en redes sociales, y en cuestión de horas recibió en su celular un *spam* de mensajes

con contenido insultante y amenazante que comprometía su integridad. Esta experiencia provocó que el periodista se abstuviera de salir por unas semanas, sentía miedo de que las agresiones virtuales se materializaran en el campo físico.

En la actualidad, el periodista enfrenta el dilema entre reportero e informante ciudadano, como la persona que comunica determinada información por su acceso a los nuevos medios, hecho que sin duda es una de las más importantes razones de la evolución en las últimas tres décadas del periodismo (Lemus *et al*., 2014).

El mismo Lemus plantea en el contexto colombiano la necesidad de que el periodista sea el principal interlocutor entre el medio de comunicación y el público objetivo. Aun así, el medio de comunicación es el espacio donde la información transcurre libre, amplia y de manera inmediata. El periodista pasa a ser también una víctima, pues la información como 'objeto' constante se abre cada día más al público, lo que trae como consecuencia no solo pérdida de valor, sino debilidad del oficio.

Otro caso de *doxing* fue experimentado por el periodista 4, que al trabajar en una plataforma de denuncia ciudadana, ha sufrido amenazas que comprometen su labor e integridad. El periodista 4 relató que al publicar la inconformidad de ciudadanos ante prestación del servicio de taxistas, se enfrentó a diversas agresiones. Los taxistas de su ciudad de residencia lo calificaron públicamente como promotor del transporte ilegal, hasta el punto de acusarlo de trabajar para plataformas informales, manteniendo una flota de transporte.

Se inició en redes y grupos de WhatsApp la circulación de una imagen que revelaba su número telefónico privado, acompañado de un mensaje donde se le señalaba de incitar una pelea directa en contra el gremio, lo que desencadenó el envío de mensajes en su contra. Esto advierte afectaciones sobre la libertad de prensa, ya que un grupo en específico expone al periodista en su vida personal, hasta el punto de perturbar su trabajo, sus investigaciones, el derecho que tiene a ejercer la denuncia, su integridad y credibilidad como profesional.

El *doxing* es peligroso, afecta la privacidad y la seguridad del periodista cuando se utiliza como incitación a la violencia. En Colombia, esta conducta podría constituir el delito de "violación de datos personales", contemplado en el artículo 269F del Código Penal.

Agresiones confinadas al ciberespacio

Es necesario resaltar aquellas ciberagresiones que únicamente se desarrollan en el ciberespacio, pues surgieron de manera específica con el auge de la web 2.0, estas son: el ciberataque a páginas web, vigilancia digital ilegal y solicitud de remoción o bloqueo de contenidos en internet.

El ciberataque a páginas web podría considerarse como el acceso ilegal a usuarios, contraseñas, correos y administradores de contenidos. La falsificación busca suplantar al periodista y atacar a las páginas de los medios de comunicación para dejarlo fuera de servicio.

En su trabajo de asesor para la protección, el periodista 5 compartió que en el año 2018 la FLIP documentó ocho ciberataques a páginas web de medios de comunicación, entendidos como 'DDoS', que corresponden a ataques a las computadoras y denegación de servicio, lo que ocasiona un impedimento al acceso de las redes o los usuarios. Estos ataques provocaron un colapso en las páginas, además de acceso a los administradores de contenido para eliminar información y reemplazarla a su antojo.

El periodista 5 también compartió que en al año 2019 recibió la denuncia de dos remociones de contenido a través de internet, lo que corrobora que esta categoría transgrede los servidores web de medios de comunicación y de usuarios legítimos.

Así mismo, la vigilancia, tal 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 agresores para monitorear (Henrichsen *et al.*, 2016). Por lo regular, se hace uso de diferentes métodos de interceptación para mensajes de

voz, SMS, MMS, *e-mail*, fax y de manera telefónica, lo que termina debilitando derechos humanos como la libertad de expresión, la libertad de asociación y el derecho a la privacidad.

El periodista 5 pone un ejemplo genérico que abarca casos que ha recibido sobre vigilancia y monitoreo, al igual que la categoría de *exploits* de *software* y *hardware*:

> […] Un periodista recibe un correo electrónico aparentemente oficial, remitente de la Fiscalía con una citación importante, él se asusta y no duda en ingresar, pero esto en realidad es un anzuelo para que abra el archivo y descargue un virus o un *malware* que tiene como fin rastrear todo lo que teclea.

Este monitoreo que empieza a recibir afecta de forma directa su seguridad, su privacidad y su derecho. La fuente también comparte que es complejo registrar este tipo de casos, ya que la parte técnica debe verificar si es un virus que se instaló de manera dirigida, o un virus que cualquier persona puede instalar por el manejo del computador.

Hacia un esquema de protección del periodismo 2.0

En el año 2000 Colombia se convirtió en el primer país en el ámbito mundial en crear un esquema de protección a periodistas; inicialmente el mecanismo generó altas expectativas al contribuir a la disminución del alto número de periodistas asesinados en el país. Sin embargo, dicho esquema de protección no se adapta a las nuevas necesidades que abarca el periodismo 2.0, lo que lo ha hecho ineficiente, burocrático e incapaz de asumir las nuevas realidades de violencia y agresiones contra la prensa.

Los sistemas de protección existentes que buscan mitigar las amenazas no han realizado una adaptación que se centre en la prevención y el manejo de casos de ciberagresiones. Se hace evidente la falta de implementación de este tipo de esquemas de seguridad y antiriesgo, que no solo brinden garantías al momento de laborar, sino también en el desarrollo de su identidad digital.

El periodista 5 comentó que sí existe un programa de protección, pero desde su experiencia como asesor de periodistas en riesgo, se ha enfrentado a distintas limitantes al hacer uso de dicho programa, ya que es un modelo donde los casos de amenaza o intimidación son tratados a través de la proporción de escoltas, chalecos y carros blindados o chalecos, celulares y un botón de pánico o de apoyo. Pero estas medidas son insuficientes para abarcar de forma integral las necesidades de los periodistas.

De todas las agresiones reportadas durante el 2017 en Latinoamérica, en Colombia se registraron 0,36%. Son los *bots* (*software* que imita el comportamiento humano, con el fin de comunicarse con el usuario) y los *spam* (se considera como un correo electrónico no solicitado, recibido por el usuario) las estrategias más comunes, pues ocupan el quinto puesto en la región, en ambas acciones.

La información brindada expone la insuficiencia de los sistemas de protección. La fuente periodística 5 consultada ha realizado diferentes llamados para que las medidas sean ampliadas, lo que genera protección colectiva, que abarque periodistas en la periferia y no solo en el centro del país. Como asesor, ha realizado llamados a la Fiscalía, pero los esfuerzos no son suficientes; la denuncia de una ciberagresión frente a un CAI virtual no asegura que el caso sea tratado de forma rigurosa, no existe una investigación real sobre los hechos ni los agresores.

Conclusiones

La ciberagresión es un fenómeno notorio que atenta contra el gremio del periodismo digital. El hecho de hacer parte de la web 2.0 implica que los comunicadores se encuentren expuestos a los riesgos aquí analizados. Esto tiene implicaciones negativas en su desempeño y vida personal.

Los casos abordados en el capítulo representan a una generación de periodistas que contribuyen de forma relevante a la profesión mediante sus investigaciones y rol; sus testimonios evidencian que:

a) No es posible desarrollar la profesión con libertad, si el periodista se encuentra amenazado y bajo situaciones de espionaje u hostigamiento. Si

ocurre hurto de información digital, exposición de datos personales en la web, difamación, ataques a los computadores y el acceso de los atacantes a la ubicación geográfica del comunicador, el riesgo de censura es evidente.

b) Ejercer el periodismo digital requiere que los profesionales tengan una visibilidad en redes sociales y plataformas digitales. Como se hace evidente en la historia del periodista 1, el abstenerse de utilizar estas herramientas de vital importancia para su desempeño laboral se convierte en el único camino de protección posible.

c) La libre expresión y la autonomía son indispensables para el desarrollo de la profesión periodística. Los casos de los periodistas 1, 2, 3 y 4 demuestran que su trabajo se vio obstaculizado, ya que sentían miedo, tomando medidas que podrían leerse como autocensura. Un periodista no puede realizar su labor si conoce que su vida profesional, personal y familiar se encuentran en riesgo por amenazas y hostigamientos.

Así dicho, la violencia en medios y su materialización en actos de intimidación, persecución, exposición y censura a periodistas se transforma y gana nuevos mecanismos de presión. Los testimonios de los comunicadores consultados permiten graficar a la ciberagresión como un fenómeno creciente, multimodal e impune, cuyo abordaje requiere avanzar en materia de exposición social y control judicial. Además de las afectaciones enunciadas frente al ejercicio periodístico, esta pone en riesgo valores como la libertad de expresión y el derecho a la información.

La ciberagresión está en pleno desarrollo en el contexto nacional. En mayo del 2020 un *software* y aplicación informática realizaron un rastreo de información indiscriminada de diferentes objetivos por parte de las unidades de inteligencia del ejército, con el fin de documentar informes. La población afectada incluía más de 130 ciudadanos, entre ellos una cifra significativa de periodistas. En respuesta a tal situación, el 5 de mayo del presente año, Pedro Vaca, director de la FLIP, solicitó protección para los periodistas y para la libertad de prensa, de forma pública y, así mismo, pidió que se garantizara el derecho a la intimidad.

La FLIP sigue recibiendo casos de periodistas que temen por su seguridad y buscan medidas de protección, y, a pesar de que su trabajo es incansable en la exposición pública del fenómeno, este sigue en franco incremento. Para 2018, la Fundación reportó 477 casos de agresiones, de los cuales 84 casos fueron a través de la web. Las cifras muestran un incremento del 53 % al compararse con el 2017, y del 120 %, al 2016. Esto señala que las acciones de denuncia y protección hacia el gremio periodístico deben ser materia en instancias gubernamentales, de control social y penal.

Referencias

Ávila C. B; Bautista R. L y Lemus S. D. (2014). Nuevas dinámicas del periodismo en Colombia desde el surgimiento. [Trabajo de grado, Universidad Santo Tomás]. https://repository.usta.edu.co/bitstream/handle/11634/1671/2014diegolemus.pdf?sequence=1&isAllowed=y

Bruns, A. (2008). The Active Audience: Transforming Journalism from Gatekeeping to Gatewatching. En C. Paterson y D. Domingo (eds.), *Making Online News: The Ethnography of New Media Production* (pp. 171-184). Peter Lang. https://eprints.qut.edu.au/13577/

Castro, A., Guevara, S. y Jaramillo, C. (2016). Análisis sociojurídico del surgimiento y expansión de las redes sociales en internet y la intimidad en Colombia. *Criterio Libre Jurídico*. http://revistasojs.unilibrecali.edu.co/index.php/rclj/article/view/551

Fundación para la Libertad de Prensa-FLIP. (2018). Prensa acorralada: un juego de violentos y poderosos. https://flip.org.co/micrositios/informe-2018/descargas/informe-anual-2018.pdf

Gallagher, R. y Greenwald, G. (2014.) How the NSA Plans to Infect 'Millions' of Computers with Malware. https://theintercept.com/2014/03/12/nsa-plans-infect-millions-computers-*malware*/

Henrichsen, J., Betz, M. y Lisosk, J. (2016). Cómo desarrollar la seguridad digital para el periodismo. http://proledi.ucr.ac.cr/wp-content/uploads/2018/10/Seguridad-digital-para-el-periodismo.pdf

Morles, V. (2002). Sobre la metodología como ciencia y el método científico: un espacio polémico. *Revista de Pedagogía*, *23*(66), 121-146. http://ve.scielo.org/scielo.php?script=sci_arttext&pid=S0798-97922002000100006&lng=es&tlng=es.

Nissenbaum, H. (2013). *Privacidad amenazada*. Editorial Océano.

Rayón, M. y Gómez Hernández, A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico y Económico Escurialense*, *XLVII*. https://dialnet.unirioja.es/descarga/articulo/4639646.pdf

Remolina, N. (2005). Data protection: riesgos y desarrollos (énfasis en el caso colombiano). https://revistas.uchile.cl/index.php/RCHDI/article/view/10761 DOI: 10.5354/0717-9162.2011.10761

Rheingold, H. (2004). *Multitudes inteligentes: la próxima revolución social*. GEDISA.

Reporteros sin Fronteras (2015). Manual de Seguridad para Periodistas, Guía práctica para reporteros en zonas de riesgo. Francia: UNESCO. https://www.rsf-es.org/wp-content/uploads/attachments/RSF_MANUAL_SEGURIDAD_PERIODISTAS_2015.pdf

Urdaneta. J. (2007). Redacción en cibermedios para comunicadores en formación. *Razón y Palabra*, *12*. http://www.razonypalabra.org.mx/anteriores/n57/jurdaneta.html

Villalba, F. y Corchado, R. (2017). Ciberseguridad: la cooperación público-privada. Análisis de ciberamenazas. *Cuadernos de Estrategia*, 185, 97-138. https://dialnet.unirioja.es/servlet/articulo?codigo=6115622