Tecnología y libre expresión: entre el acoso y el espionaje

FRIDA V. RODELO*

Resumen: *a la creciente violencia contra periodistas, en México y a nivel mundial, se ha sumado el surgimiento de nuevas amenazas para el derecho a la libertad de expresión: las tecnologías digitales han impactado, para bien y para mal, la seguridad de los periodistas. El artículo analiza los riesgos asociados con estas tecnologías en México y Jalisco, principalmente a partir de los casos recientes de acoso de periodistas y de adquisición gubernamental de software de vigilancia.*
Palabras clave: *periodismo, tecnología digital, seguridad*

Abstract: *Added to the growing violence against journalists in Mexico and around the world is the emergence of new threats to the right to freedom of expression: digital technologies have had an impact, for better and for worse, on journalists' security. This article analyzes the risks associated with these technologies in Mexico and Jalisco, primarily on the basis of recent cases of harassment of journalists and the government's acquisition of surveillance software.*
Key words: *journalism, digital technology, security.*

* Es doctora en Ciencias Sociales por la Universidad de Guadalajara. Actualmente es profesora titular en la Universidad de Guadalajara y de asignatura en el Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO). Forma parte del Sistema Nacional de Investigadores; su investigación académica versa acerca de las prácticas y coberturas periodísticas. Es integrante de la Asociación Mexicana de Derecho a la Información (Amedi) Capítulo Jalisco, la Asociación Mexicana de Investigadores de la Comunicación y el Observatorio de Participación Política de las Mujeres de Jalisco. Correo electrónico: frida.rodelo@academico.udg.mx

Al incremento de casos de violencia contra periodistas —no solo en México sino a nivel mundial— se ha sumado el surgimiento de nuevas amenazas para el derecho a la libertad de expresión. Este texto intentará dar un panorama sobre la manera en que las tecnologías digitales han impactado, para bien y para mal, en la seguridad de periodistas en México y en el estado de Jalisco, a partir de casos recientes de interés público, como lo son la adquisición gubernamental de los *software* de vigilancia Galileo y Pegasus, y los casos de acoso de periodistas.

El uso social de las tecnologías de la información ha provocado tensiones entre los derechos a la libertad de expresión y a la privacidad. La paradoja que permea a Internet, en palabras de Evgeny Morozov,[1] es que una mayor libertad de Internet implica una mayor libertad de expresión: hay numerosos incentivos para hacer uso de Internet y por primera vez en la historia de las democracias moderna, existe la posibilidad material de que los puntos de vista de cualquier individuo privado, sin importar su estatus, puedan ser escuchados. Sin embargo, al mismo tiempo, la mayor libertad de Internet ha implicado una mayor capacidad de vigilancia (o una menor privacidad) al dar visibilidad y valor monetario a información que, o no existía previamente o bien se consideraba privada —como lo pueden ser las ubicaciones, registros de tiempo y datos de contacto de los sujetos.[2]

En otras palabras, la expansión de la esfera pública mediante Internet no ha estado exenta de contradicciones. Incluso otra interpretación, más pesimista, conceptúa a las tecnologías digitales como "el dispositivo disciplinario por excelencia"; esto debido a que operan sin necesidad de un espacio físico y a que tienen capacidad de acceder a la esfera privada de los individuos,[3] con el resultado de permitir labores

1. Morozov, Evgeny. "Liberation technology: whither Internet control?", en *Journal of Democracy*, vol.22, núm.2, 2011, pp. 62–74.
2. *Ibidem*.
3. Ricaurte–Quijano, Paola, Nájera Valdez, Jacobo & Robles Maloof, Jesús. "Sociedades de control: tecnovigilancia de estado y resistencia civil en México", en *Teknokultura*, vol.11, núm.2, 2014, pp. 259–282.

de vigilancia y castigo que los actores con poder realizan para controlar e imponer un orden social bajo el pretexto de velar por la seguridad nacional y pública.[4]

La tecnología digital se ha usado como herramienta periodística primordialmente para facilitar el trabajo en redes, como fuente de información alternativa o para contrastar y verificar fuentes, así como para conocer y difundir información censurada o sobre temas, asuntos y entornos escasamente cubiertos. Todo esto, como hemos visto, no implica la ausencia de problemas y limitaciones asociados a cada uno de estos usos "benignos". En contraparte, entre los principales riesgos que el uso de las tecnologías de la información implica para periodistas se encuentran, principalmente, la vigilancia, los ataques, el acoso y las amenazas. Todos estos son riesgos preexistentes, pero potenciados en su capacidad por las nuevas tecnologías.

Es en este sentido que, en un estudio comisionado por la Unesco, Jennifer Henrichsen, Michelle Betz y Joanne Lisosky afirmaron que "algunos riesgos de seguridad simplemente se han transferido del mundo fuera de línea al mundo en línea".[5] Lo anterior, se origina debido a que Internet, como tecnología, ha ido con el paso del tiempo abarcando una mayor cantidad de capacidades que van más allá de ser una forma de comunicación entre personas y un ámbito para la expresión. Hoy en día, Internet es, además de lo anterior, un mecanismo de comunicación entre dispositivos, una plataforma para la prestación de servicios y la realización de transacciones comerciales, etcétera.[6]

Como se mencionó, transferir los riesgos del mundo fuera de línea al mundo en línea comparte las "ventajas" (desde el punto de vista de los

4. *Ibidem*.
5. Henrichsen, Jennifer; Betz, Michelle & Lisosky, Joanne. *Building digital safety for journalism: A survey of selected issues*, UNESCO Publishing, París, 2015, p.8.
6. Berger, Guy. "Why the World Became Concerned with Journalistic Safety, and Why the Issue Will Continue to Attract Attention", en Carlsson, U. & Poyhtari, R. (eds.), *The Assault on Journalism. Building Knowledge to Protect Freedom of Expression,* Nordicom, Gotemburgo, 2017.

actores con poder) que en general brindan las tecnologías digitales:[7] la automatización de tareas, la indetectabilidad, así como un bajo costo de operación. Rasgos distinguibles en la siguiente relación de riesgos asociados con el uso de la tecnología digital en México.

El caso emblemático que destapó la vigilancia digital secreta no supervisada de periodistas y defensores de derechos humanos, realizada por varios gobiernos mexicanos, fue el descubrimiento de que al menos tres dependencias del gobierno federal mexicano —la Secretaría de la Defensa Nacional, la Procuraduría General de la República y el Centro de Investigación y Seguridad Nacional (Cisen)— utilizaron el software de espionaje Pegasus, diseñado por la empresa israelí NSO Group, para vigilar a periodistas y defensores de derechos humanos entre 2015 y 2016.[8]

En una última tanda de revelaciones, el grupo de investigación de la Universidad de Toronto Citizen Lab dio a conocer en noviembre de 2018, días antes del cambio de gobierno federal en México, que colegas del periodista asesinado Javier Valdez fueron blancos de intentos de espionaje mediante el uso de este *spyware*.[9] El caso ha permitido exhibir al gobierno federal como indolente y criminal. Pero, además, a esta situación se suma el hecho de que Pegasus no es el único *software* de espionaje utilizado en México por entidades gubernamentales, ni este método la única modalidad de vigilancia practicada con ayuda de la tecnología.

Otro riesgo son los ataques digitales contra periodistas y sus fuentes. *Aristegui Noticias*, *Sin Embargo*, *Mientras Tanto en México* y *Río Doce* son algunos de los sitios web periodísticos que han sido blanco de ca-

7. *Ibidem.*
8. Artículo 19, R3D & Socialtic. *Gobierno espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México*. México, 2017. Recuperado el 1 de septiembre de 2018, de https://articulo19.org/wp-content/uploads/2017/06/Reporte-Gobierno-Espi%CC%81a-Final.pdf
9. The Citizen Lab. "Reckless VI. Mexican Journalists Investigating Cartels Targeted with NSO Spyware Following Assassination of Colleague", 27 de noviembre de 2018. Recuperado el 1 de diciembre de 2018, de https://citizenlab.ca/2018/11/mexican-journalists-investigating-cartels-targeted-nso-spyware-following-assassination-colleague/

sos de ataques de denegación de servicio (ataques DDOS).[10] Un ataque DDOS exitoso puede lograr sacar de línea por completo al sitio web objetivo. El tiempo que tome restaurar el sitio varía, dependiendo del soporte técnico con el que cuente la organización. Como lo menciona Morozov,[11] con frecuencia es difícil determinar con certeza si la "caída" del sitio fue provocada por un ataque DDOS; además, los ataques DDOS perjudican la relación de la organización de medios con el proveedor del servicio de Internet (ISP), porque el ataque puede provocar afectaciones a otros sitios hospedados en el mismo servidor.

Además de "tumbar" los sitios web, los ataques pueden dirigirse hacia individuos, como cuando hablamos del acoso y las amenazas contra periodistas, activistas y usuarios de medios sociales. Por ejemplo, la delincuencia organizada ofreció una recompensa a quien diera información sobre un periodista anónimo de Tamaulipas que publicaba el blog "Valor por Tamaulipas"; el bloguero, poco tiempo después, tomó la decisión de dejar de publicar informaciones sobre el tema de la violencia.[12] En varios estados, periodistas han denunciado que funcionarios públicos han estado involucrados en prácticas de acoso.[13]

El acoso y los ataques digitales contra mujeres periodistas parecen tener rasgos peculiares. Los informes de la Relatoría Especial para la Libertad de Expresión señalan que los ataques contra mujeres periodistas han ido en aumento; además, indican que las mujeres están especialmente expuestas a ser acosadas a través de medios sociales. Otras formas particulares en que las periodistas mujeres son afectadas es al recibir menor remuneración que los periodistas varones, tener

10. López Serrano, Erick. "Ciberataques a la prensa: México frente al ciberdelito", en *Nexos*, 13 de abril de 2015. Recuperado el 1 de septiembre de 2018, de https://eljuegodelacorte.nexos.com.mx/?p=4554; Artículo 19, R3D y Socialtic, *op. cit*.
11. Morozov, Evgeny, *op. cit*.
12. Centro Jurídico por los Derechos Humanos & Freedom House México (coords.). *Informe sobre la libertad de expresión y prensa en México. Estado de las recomendaciones emitidas a México en camino a la sesión 17 del Examen Periódico Universal de Naciones Unidas,* 23 de agosto de 2013. Recuperado de https://freedomhouse.org/sites/default/files/Informe%20sobre%20la%20libertad%20de%20expresion%20y%20prensa%20en%20Mexico.pdf
13. *Ibidem*.

menor oportunidad de escalar a puestos editoriales y directivos, así como el recibir trato particularmente condescendiente de las autoridades.[14] Con todo, falta mayor información que detalle el papel de la variable de género,[15] lo cual se explica por realizarse apenas en 2014 la adopción de la dimensión de género dentro del paradigma de libertad de expresión de la Unesco,[16] y ser también reciente el trabajo de abogacía con perspectiva de género, no solo en México sino también en el resto del mundo.

Los riesgos relacionados con el auge de la tecnología digital poco a poco han dado paso a conductas precautorias de periodistas mexicanos, como el evitar ser monitoreados, establecer redes de comunicación con colegas para compartir ubicación y asistir a entrenamientos de seguridad.[17] Con todo, prácticas como el espionaje y el acoso, además de ser inaceptables en términos legales y democráticos, imponen una pesada carga mental en los actores en riesgo, como se avizora en el testimonio del periodista Ismael Bojórquez durante la conferencia de prensa a propósito del caso Pegasus:

> Nosotros nunca le dimos un clic a ninguno de esos mensajes, pero no estamos tan seguros de que no hayan sido infectados los teléfonos. De repente te sientas en la computadora, lees tu Whatsapp, y te dice que cierres una sesión, y dices: ¿y quién tiene abierta una sesión? [...] No tenemos esa seguridad.[18]

14. Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de los Derechos Humanos. *Informe especial sobre la situación de la libertad de expresión en México*, RELE–CIDH / OEA, junio de 2018.
15. *Ibidem*.
16. Berger, Guy, *op. cit*.
17. Hughes, Sallie & Márquez–Ramírez, Mireya. "How Unsafe Contexts and Overlapping Risks Influence Journalism Practice", en Carlsson, U. & Poyhtari, R. (eds.), *The Assault on Journalism. Building Knowledge to Protect Freedom of Expression*, Nordicom, Gotemburgo, 2017.
18. R3D. "Revelan dos nuevos casos de #GobiernoEspía" [video de YouTube], 30 de noviembre de 2018. Recuperado el 1 de diciembre de 2018, de https://www.youtube.com/watch?v=3eSvwqHsx3U

1. JALISCO: VIEJAS Y NUEVAS MANERAS DE VIGILAR Y ACOSAR

El desarrollo y adopción en los últimos años de tecnologías digitales ha dado paso a nuevos métodos para vigilar y acosar a periodistas, que han sido utilizados principalmente por agentes gubernamentales, como lo demuestran los casos que han cobrado notoriedad y que a continuación abordamos.

Desde 2015, la filtración a WikiLeaks de documentos de la empresa italiana Hacking Team permitió evidenciar que el gobierno de Jalisco compró el *software* de espionaje Galileo, desarrollado por Hacking Team, al proveedor SYM Servicios Integrales, por un monto de 748 mil euros (trece millones de pesos).[19]

Asimismo, documentos obtenidos a partir de la misma filtración revelaron que la licencia vendida al gobierno de Jalisco fue para que dos dependencias diferentes usaran el *software* —la Fiscalía General del Estado de Jalisco y la Secretaría General de Gobierno—, puesto que existe evidencia de que las dos dependencias mencionadas recibieron el producto. Sin embargo, la capacitación para usarlo fue realizada directamente por personal de Hacking Team en la sede de la Coordinación General de Asuntos Sociales de la Secretaría General de Gobierno, lo cual sugiere que el *software* de espionaje se adquirió con el objetivo de realizar espionaje político y no para combatir el secuestro, como aseguró en su momento el subsecretario de la Secretaría de Planeación, Administración y Finanzas del Gobierno de Jalisco, Salvador González.[20]

19. Ángel, Arturo. "El Sabueso: ¿Jalisco compró el sistema de Hacking Team solo para investigar secuestros?", en *Animal Político*, 24 de julio de 2015. Recuperado el 3 de octubre de 2018, de https://www.animalpolitico.com/elsabueso/el-sabueso-jalisco-compro-galileo-solo-para-investigar-secuestros-y-sin-conocer-a-hacking-team/
20. *Ibidem.*

Profundizando en lo anterior, el informe sobre este tema elaborado por la organización no gubernamental R3D[21] precisa que la Fiscalía General del Estado de Jalisco requiere autorización del Poder Judicial para poder realizar la intervención de comunicaciones privadas y añade a lo anterior solicitudes de información pública que demuestran que en el periodo 2014–2015, la citada Fiscalía solicitó autorización judicial para realizar intervenciones de comunicaciones en solo dos ocasiones. De esta manera, R3D concluyó que, o bien se adquirió un *software* que costó 13 millones de pesos para ser usado en dos ocasiones, implicando esto un uso irracional de los recursos públicos, o bien el Gobierno del Estado de Jalisco ha estado utilizando este *software* de manera ilegal.

El entonces alcalde de Guadalajara, perteneciente al partido de oposición Movimiento Ciudadano, Enrique Alfaro Ramírez, mostró un rechazo enérgico hacia el uso ilegítimo de sistemas de vigilancia. En un gesto de protesta, Alfaro abandonó el Secretariado Técnico Local de Gobierno Abierto, justificando de la siguiente manera su acción:

> Renuncio porque no se puede formar parte de un espacio de simulación donde un integrante del Secretariado como el gobernador Aristóteles Sandoval Díaz tiene en su poder y utiliza de manera opaca un *software* como el que el gobierno federal ha usado para espiar activistas, periodistas y opositores políticos. Esto rompe con cualquier posibilidad de diálogo y confianza entre la [*sic*] partes anulando las oportunidades de concretar un ejercicio auténtico de gobierno abierto.[22]

21. R3D. *El Estado de la vigilancia. Fuera de control*, noviembre de 2016. Recuperado el 1 de noviembre de 2018, de https://r3d.mx/estadodelavigilancia/
22. Alfaro Ramírez, Enrique. "Acabo de enviar mi renuncia..." [Publicación de Facebook]. 22 de junio de 2017. Recuperado el 1 de diciembre de 2018, de https://www.facebook.com/EnriqueAlfaroR/posts/acabo-de-enviar-mi-renuncia-como-miembro-propietario-y-representante-de-los-muni/1561094973921669/

A lo que siguió un exhorto del Poder Legislativo, promovido por la bancada del partido Movimiento Ciudadano, para recibir un "informe detallado" del uso gubernamental del *software*.[23] Sin embargo, ante la ausencia de nueva información que aclare cómo se ha usado el *software* Galileo en Jalisco, el tema ha resurgido únicamente ante nuevas revelaciones de evidencias de actos de espionaje gubernamental en el país, como la que el Citizen Lab diera a conocer tras analizar una serie de mensajes SMS enviados a periodistas del semanario sinaloense *Río Doce* después del asesinato del reconocido periodista Javier Valdez.[24]

El hallazgo ha generado incertidumbre acerca de cuáles serán las acciones que tomen los nuevos gobiernos, tanto el federal como el estatal, hacia el tema del espionaje y la vigilancia tecnológica, máxime cuando es sabido que esta es apenas una de entre varias modalidades de vigilancia de opositores políticos practicadas por los gobiernos. Dos ejemplos ilustran lo anterior: por un lado, el descubrimiento de micrófonos ocultos en oficinas gubernamentales, a propósito de revisiones realizadas por órdenes de funcionarios de las administraciones entrantes durante el reciente relevo de gobiernos municipales.[25]

El segundo ejemplo fue el descubrimiento de un "cuarto de guerra", conformado por altos funcionarios del Gobierno del Estado de Jalisco, con el propósito de desarrollar e implementar estrategias para "frenar el avance de [Enrique] Alfaro Ramírez" frente a su creciente popularidad y en vista de las entonces próximas elecciones intermedias de 2015.[26] Este grupo secreto recibía carpetas de información con perfiles de organizaciones de medios, para utilizarlas como insumo de

23. Junta de Coordinación Política del Congreso del Estado de Jalisco. "Acuerdo legislativo 1320–LXI–17", 18 de julio de 2017.
24. The Citizen Lab, *op. cit*.
25. Martínez Macías, Carlos. "¿Y el sistema de espionaje?", en *Milenio Jalisco*, 14 de noviembre de 2018. Recuperado el 1 de diciembre de 2018, de http://www.milenio.com/opinion/carlos-martinez-macias/sin-pedir-audiencia/y-el-sistema-de-espionaje
26. Osorio, Alberto & Reza, Gloria. "La mesa de estrategia... sucia", en *Proceso Jalisco*, 9 de agosto de 2014. Recuperado el 29 de octubre de 2018, de https://www.proceso.com.mx/379201/la-mesa-de-estrategia-sucia

estrategias para controlar la información publicada por las organizaciones de medios. Estrategias de control que incluyeron el uso de gasto gubernamental en publicidad como medida de censura indirecta de los medios de comunicación.

Pero con el incremento del uso de los medios sociales, los gobiernos ya no están únicamente interesados en lo que publican los medios sino que buscan también vigilar y, en la medida de lo posible, incidir sobre los comportamientos de usuarios en los medios sociales. Y para lo anterior, se han destinado cantidades millonarias de recursos públicos.

Ivonne Ojeda relata la existencia de numerosos contratos de varias secretarías del gobierno federal con agencias especializadas en el monitoreo y vigilancia de medios sociales, con objetivos tales como el "servicio de monitoreo y seguimiento de actores de redes sociales los... días de la semana las 24 horas del día".[27] Una de las principales, IONC, S.A.P.I. de C.V., tiene sede en Jalisco y se encuentra en la lista de proveedores del gobierno del estado.

Métodos viejos y nuevos también se superponen cuando hablamos del acoso a periodistas. En 2011, más de dos docenas de periodistas de distintos medios de comunicación firmaron un desplegado para denunciar el acoso reiterado de un funcionario público de la administración del entonces gobernador Emilio González Márquez.[28]

El funcionario en cuestión, Alberto Jiménez Martínez, alias "la Antena", se dedicaba a amenazar y agredir a periodistas a través de llamadas telefónicas y mensajes en medios sociales.[29] El caso de La Antena destacó por el alto perfil del agresor, quien era director de área en la Secretaría de Finanzas, y por la lentitud de sus superiores en

27. Ojeda, Ivonne. "El caso Ayotzinapa detonó un espionaje inédito en las redes a los críticos del Gobierno de EPN", en *Sin Embargo,* 6 de febrero de 2019. Recuperado el 9 de febrero de 2019, de https://www.sinembargo.mx/06-02-2019/3531927

28. Centro de Justicia para la Paz y el Desarrollo. "Periodistas de Jalisco denunciamos hostigamiento y amenazas", en CEPAD, 28 de marzo de 2011. Recuperado el 3 de octubre de 2018, de https://cepad.org.mx/2011/03/periodistas-de-jalisco-denunciamos-hostigamiento-y-amenazas/

29. *Ibidem.*

reaccionar; además, el episodio visibilizó la que entonces podía considerarse una nueva modalidad de agresión a activistas y periodistas, que emergió en un entorno digital en el que actores pueden crear con suma facilidad perfiles y cuentas personales con la intención específica de difamar, acosar o colonizar los medios sociales. Caldo de cultivo en que han surgido *troles*, es decir, cuentas anónimas desde donde se agrede a personas, ya sea de manera individual o coordinada, y entorno en donde se han manifestado también esfuerzos de comunicación más estructurados, desde donde se publican contenidos políticos de forma anónima. Un ejemplo de esto último fue la famosa página "Fisgón Político Jalisco", especializada en publicar informaciones y videos que perjudican al Partido Revolucionario Institucional (PRI), como lo explica la propia persona que la elabora.[30]

Las mujeres pueden ser víctimas de agresiones particularmente virulentas a través de Internet. Durante años, las estadísticas de ataques contra la prensa han mostrado mayor cantidad de agresiones contra periodistas hombres,[31] pero de manera reciente diferentes organizaciones que trabajan el tema de la libertad de expresión han comenzado a reconocer que las mujeres enfrentan formas diferentes de violencia, que pueden ser difíciles de identificar y denunciar, en entornos con actitudes androcéntricas en donde pueden imponerse la normalización de la violencia y el temor a ser revictimizadas.

En el caso del funcionario acusado de hostigamiento, mencionado anteriormente, una periodista manifestó: "Hace algunos años... tuve agresiones físicas... que tuvieron consecuencias de hasta hospitalización de altos niveles. Pero también quiero decirles que en ese momento quizás yo no tenía la misma fortaleza mental que tengo ahora

30. Fisgón Político. "La imparcialidad no existe, existe la veracidad y la transparencia", en *Fisgón Político*, 1 de enero de 2012. Recuperado el 1 de diciembre de 2018, de https://elfisgonpolitico.com/la-imparcialidad-no-existe-existe-la-veracidad-y-la-transparencia/

31. Rodelo, Frida V. "Violaciones de la libertad de expresión de periodistas y trabajadores de medios en Jalisco, 1995–2013", en Paláu Cardona, M.M.S. (coord.), *Medios de comunicación y derecho a la información en Jalisco 2013*, Guadalajara, 2014, pp. 95–112.

para poder platicarlas". Y añadió: "durante un largo periodo, Alberto Jiménez Martínez también en el Facebook agredió a mi persona descalificándola, llamándome prostituta y diciendo que yo no rebuznaba porque no podía ser más burra cuando jamás, jamás, en mi quehacer periodístico tuve una descalificación hacia su persona".[32]

En abril de 2018, se hizo famoso el caso de un aficionado del equipo de futbol Chivas de Guadalajara, que agredió sexualmente a una reportera deportiva del canal Fox Sports que trasmitía en vivo. El tocamiento lascivo a María Fernanda Mora, además de visibilizar las formas diferentes de violencia que enfrentan las mujeres dentro del periodismo, ha permitido constatar la clase de comentarios agresivos y descalificatorios que las periodistas suelen recibir al denunciar públicamente estas formas de violencia, como el usuario que desde una cuenta anónima opinó: "Te viste súper pendeja, el aficionado solo estaba celebrando, si no quieres rosarte con ellos vete a un programa de cocina a donde perteneces" (*sic*). Las agresiones pueden producirse sin mayor razón que la de insultar a mujeres que ocupan el espacio público representando roles tradicionalmente considerados masculinos, como ha sido denunciado por periodistas deportivas en México y en Estados Unidos.[33]

2. A MANERA DE CONCLUSIÓN

Los casos de espionaje y ataques DDOS, además de ser actos inaceptables, afectan la confianza de los actores en riesgo y de terceros, pues, como expusimos en este texto, con frecuencia no hay certeza sino únicamente sospechas, acerca de la perpetración de ataques. Aunque

32. Planter, Karla. "Entrevista a Cecilia Márquez y el caso de 'La Antena'", en *UDG Noticias*, 25 de marzo de 2011. Recuperado el 31 de octubre de 2015, de http://medios.udg.mx/node/7724

33. Corona, Sonia. "Las periodistas de deportes de México quieren detener el acoso en redes", en *El País*, 27 de febrero de 2017. Recuperado el 1 de diciembre de 2018, de https://verne.elpais.com/verne/2017/02/27/mexico/1488150620_563816.html

el acoso y hostigamiento digitales pueden pasar desapercibidos para el público en general por la falta de visibilización del tema, se trata de prácticas violentas que producen frustración, incomodidad y ansiedad en quienes son blancos de estas.

En ambos tipos de riesgos, hablamos de afectaciones a los derechos de actores con un importante rol democrático que no son menores ni intrascendentes. Y además de lo anterior, los casos relatados de vigilancia tienen en común el uso escandaloso de recursos públicos en tareas ilegítimas que tienen exclusivamente propósitos políticos.

Hasta el momento, el nuevo presidente de la república, Andrés Manuel López Obrador, ha prometido transparentar todo lo relativo a la adquisición del *software* Pegasus, al tiempo que un amparo promovido por R3D ha frenado la clasificación realizada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) de la información relacionada con Pegasus.[34] La incertidumbre permanece respecto a las acciones que tomen los nuevos gobiernos (y sus efectos) hacia el tema del espionaje y la vigilancia tecnológica.

34. Rodríguez García, Arturo. "Espionaje político mediante Pegasus será transparentado: López Obrador", en *Proceso,* 19 de diciembre de 2018. Recuperado el 1 de enero de 2019, de https://www.proceso.com.mx/564519/espionaje-politico-mediante-pegasus-sera-transparentado-lopez-obrador