

¿QUIÉN VIGILA AL VIGILANTE?

JESÚS MARÍA AGUIRRE

El texto nos analiza cómo, a partir del desarrollo de los sistemas informáticos, el auge de las telecomunicaciones satelitales e Internet, y todo el arsenal derivado de las llamadas nuevas tecnologías se usan para el campo de la vigilancia de todo orden. Nos ofrece una relación entre la vigilancia-espionaje y el periodismo de investigación que en muchos casos es el resultado de la filtración de documentos con datos sensibles para gobiernos, empresas e incluso ciudadanos. El articulista concluye con la siguiente afirmación ética: el periodista de investigación se confronta con el dilema ético de escoger a qué amo sirve o, en otros términos, a quién vigila y por quién prefiere ser vigilado.

SE ENCIENDEN LAS ALARMAS

Hace ya dos años el documental de Netflix, *El dilema social*, mostraba el lado más oscuro de las redes sociales, avivando el debate sobre el peligro de estas plataformas para la privacidad y la democracia. Pero, su enfoque no se centraba tanto en la producción e intrusión en los procesos informativos, sino en su potencial de manipulación, ya que están programadas para generar adicción y explotar la vulnerabilidad humana.

En ese clima de *agenda setting* mediático una investigación realizada por *The Washington Post*¹ y dieciséis medios asociados revelaba que el *spyware* Pegasus de NSO Group, vendido a gobiernos de todo el mundo, podía infectar teléfonos sin un solo clic y relataba cómo hackearon teléfonos de informadores, entre ellos 37 teléfonos que pertenecían a periodistas, activistas de derechos humanos, ejecutivos de empresas y dos mujeres cercanas al periodista saudí asesinado Jamal Khashoggi.

Efectivamente, en enero Amnistía Internacional informaba que una investigación conjunta de Access Now y Citizen Lab² había identificado el uso a gran escala del programa espía Pegasus, de la israelí NSO Group, contra periodistas y miembros de organizaciones de la sociedad civil en El Salvador.

El gobierno, fácticamente militarizado de Venezuela, bajo el eufemismo de cívicomilitar, en su carrera alocada hacia el control de la sociedad civil se suma a esta carrera de la vigilancia cuando ni siquiera las telecomunicaciones públicas ofrecen unos servicios básicos eficientes y su *ranking* está en los últimos puestos latinoamericanos.

En un foro celebrado el 16 de febrero de 2022, bajo el marco de las actividades de reflexión organizadas por el Observatorio Venezolano de Fake News, como un proyecto que adelanta la Asociación Civil Medianálisis, se presentó al especialista en seguridad digital y director ejecutivo de Venezuela Inteligente, Andrés Azpúrua. En el conversatorio aludió a

DOSSIER

una información atribuida al presidente de la República sobre la intención de adoptar el programa PEGASUS de tecnología israelí por parte del gobierno de Venezuela³.

El gobierno, fácticamente militarizado de Venezuela, bajo el eufemismo de cívicomilitar, en su carrera alocada hacia el control de la sociedad civil se suma a esta carrera de la vigilancia cuando ni siquiera las telecomunicaciones públicas ofrecen unos servicios básicos eficientes y su *ranking* está en los últimos puestos latinoamericanos.

Entre los anuncios previos al caso venezolano se mencionó la situación de El Salvador, ya de dominio común, cuando el gobierno estadounidense sancionó a la firma israelí que produce Pegasus, el programa espía que ha sido empleado para vigilar periodistas.

EL PAPEL DE ISRAEL EN LA EXPANSIÓN DE LOS PROGRAMAS

Estas noticias alarmantes no son tan nuevas, si tenemos en cuenta los *affaires* del hacker William Assange y Edward Snowden, exagente del aparato de inteligencia de los Estados Unidos, condenado y perseguido por demostrar que la “National Security Agency, NSA, espía a ciudadanos comunes y autoridades a partir del uso y consumo de las redes sociales, e incluso de los servidores de las empresas Microsoft y Google entre otras. Mientras el caso del primero quedó judicialmente empantanado, las denuncias de Snowden no pasaron de provocar una indignación pasajera.

Lo novedoso de la intervención israelí en un espacio que se considera reservado a los militares, y con propósitos de seguridad y ciber guerra, es que a través de sus centros de investigación se hayan traspasado unas barreras sensibles, desde el ámbito del espionaje, al terreno comercial, vendiendo el *software* a gobiernos y empresas.

Sin embargo, hay que dejar el asombro, cuando ya estudios realizados en el siglo pasado por Herbert Shiller y André Mattelart, mostraban la articulación entre las industrias militares y civiles en los Estados Unidos y la mutua retroalimentación. No es de esperar menos con Estados autoritarios como Rusia o totalitarios como China.

El desarrollo de los sistemas informáticos, el auge de las telecomunicaciones satelitales y hasta la misma Arpanet, matriz de Internet, surgieron con esa doble lógica controlada por las grandes potencias.

Con la consigna de que lo que es igual no es trampa, los israelíes se han anticipado en un negocio que en un plazo corto se considera tan lucrativo como el de la venta de armas, pero tal estrategia desfavorece los intereses regionales norteamericanos que aducen razones de seguridad, sobre todo cuando se trata de ventas a gobiernos hostiles o autoritarios, como en el caso de El Salvador o Venezuela.

Lo que han revelado las investigaciones periodísticas de *The Washington Post* en Estados Unidos o *The Guardian* en Europa, basándose en las mismas fuentes, es que O-NSO Group, empresa israelí de seguridad y ciber guerra, ha desarrollado un *software* intrusivo, llamado Pegaso, para uso de gobiernos y empresas que pueden obtener datos sea de los ciudadanos o de los consumidores. Derivadamente, en último término, los flujos pueden ser monitoreados y controlados por la inteligencia israelí.

Y, aunque en estos escenarios que desbordan los planteamientos jurídicos internacionales, e incluso los umbrales críticos de la convivencia social, es común que los expertos pidan ralentizar la marcha de adopción de estas tecnologías invasivas y solicitar a los gobiernos la aplicación de una moratoria mundial sobre la venta, la transferencia y el uso de programas espías, los procesos de aceleración se mantienen por la actual dinámica geopolítica. Hasta que se establezcan salvaguardias y garantías de derechos humanos, sabemos por experiencia en este nuevo milenio, que los ritmos de la incorporación técnica marchan por delante, acicateados por la competencia, mientras los acuerdos de concertación se mueven lentamente y trabados por

una carrera de obstáculos entre países e instituciones de concertación mundial (UIT, OMC, OIT, Unesco, etcétera).

Pero los casos noticiosos utilizados en la palestra política para descalificar al gobierno oponente, sobre todo si es autoritario, no nos deben hacer perder la perspectiva de fondo y el horizonte al que se enfrentan los periodistas en su ejercicio profesional, pues en las actuales telecomunicaciones globalizadas las fronteras no existen, son grises o pueden ser traspasadas.

NUEVAS CLAVES DE COMPRENSIÓN DE LA VIGILANCIA

A mi entender, para la comprensión del fenómeno, sometido a las diatribas políticas de coyuntura, es necesario levantar el vuelo para analizar el horizonte en el que se inscriben estas tecnologías sociales, derivadas del mundo militar (ciberguerra) o del espionaje industrial, y adoptadas por las nuevas empresas, primero bajo el señuelo de la supervisión, después de la seguridad, y últimamente del mercadeo digital.

Los antecedentes de esta corriente, como ocurre en varios campos de la ciencia, los encontramos en las distopías en un grupo de novelistas cuyos intereses se mantenían próximos al análisis político a las ficciones conductistas. Desde el imaginario distópico *1984* de Orwell y *Un Mundo Feliz* de Huxley, pasando por la novela *Walden Two* del psicólogo conductista Skinner, en este milenio estamos asistiendo a una industrialización de las tecnologías de control social y de manipulación de la conducta humana, nunca antes vistas. El ensayo *Vigilar y castigar* de Foucault, le dará un vuelo más intelectual al vértigo moderno de la pérdida de subjetividad a partir de los micropoderes, que, como chips, operan en el subconsciente humano.

El ensayo de Shoshana Zuboff, *La era del capitalismo de la vigilancia*, lleva por subtítulo “La lucha por un mundo humano, detrás de las fronteras del poder”. Es decir, formula la intencionalidad clara del libro. *The Guardian*, periódico cuyo nombre evoca también la vigilancia, le considera como uno de los cien mejores libros; mejor dicho, *bestsellers* del siglo XXI

y, aunque no sea más que por su hiperbolismo mercantil, que afecta la opinión de grandes mayorías, merece nuestra atención.

Como toda publicación con un propósito ético tiende a cargar las tintas negras de la invasión de las nuevas tecnologías y argumentar desde una posición crítica que advierte sobre las consecuencias negativas de los procesos de su adopción ingenua. En ese sentido los datos y las pruebas se ven contagiados por ciertas insuficiencias probatorias, en que lo normativo se impone a la falsación.

Zuboff tiene el mérito, sobre todo en la primera parte del libro, de describir pormenorizadamente los mecanismos y el potencial de estas nuevas herramientas de intrusión, que parten de los gobiernos y de las transnacionales, asociadas a los núcleos del poder mundial, para manejar los hilos conductores de las tomas de decisión personales y sociales.

A pesar de esta limitación posee el gran mérito de situarnos en el horizonte más apropiado para analizar el impacto de las nuevas tendencias del desarrollo de los infomedia, que están en la base del mundo digital, porque para Zuboff la operación de “automatizar” (en inglés *automate*) necesitaba complementarse con el de “informar”, para lo que ella acuñó un nuevo verbo en inglés, *informate*. No es nada gratuito que la parte más amplia del libro esté dedicada a la “información” en el sentido más estricto del término.

Hace seis años, al analizar los nuevos dinámicos en los procesos de producción informacional en el libro *Comprender la Sociedad Red* (Aguirre, 2016: 33) señalaba que bajo los fenómenos superficiales de los cambios espectaculares de las NTIC, o INFOMEDIA, se iban imponiendo las características transversales de la sobreinformación, hipercomplejización, rapidización y supervigilancia.

A este último respecto ya entonces, entre los estudios realizados en el marco de la Unesco, citábamos el artículo de Stephane Callens, “La

DOSSIER

Société de l'Information: Une société de surveillance", que mostraba uno de los aspectos sombríos de la sociedad de la información, en medio de los mitos y realidades del mundo actual (Mathien 2005).

Los *Panama papers* y los *Pandora papers*, que aparecen como los grandes hitos del periodismo investigativo del siglo XXI se caracterizan tanto por el número de partícipes internacionales, como por la masa de datos manejada, en gran parte filtrados.

Zuboff tiene el mérito, sobre todo en la primera parte del libro, de describir pormenorizadamente los mecanismos y el potencial de estas nuevas herramientas de intrusión, que parten de los gobiernos y de las transnacionales, asociadas a los núcleos del poder mundial, para manejar los hilos conductores de las tomas de decisión personales y sociales.

Sin agotar otras dimensiones desgranadas en un libro de más de novecientas páginas, dejo esta consideración última sobre la deriva del periodismo investigativo.

DEL PERIODISMO INVESTIGATIVO DE PRECISIÓN A LA MINERÍA DE DATOS Y A LA VIGILANCIA PROGRAMADA

En la tradición sociológica de los medios de comunicación, Merton, Lazarsfeld, Whright y otros, recalaban la función de vigilancia del entorno que satisfacen los medios para la reducción de la incertidumbre y la homeostasis social. Incluso agregaban la función de moralización bajo ciertas circunstancias y regímenes. En una visión responsabilista de los medios, considerados como un cuarto poder moderador en las democracias, el papel del periodismo, fuera noticioso o investigativo, cumplía ese rol.

En el juego de poderes, presuntamente diferenciados, las críticas contra los periodistas provenían sobre todo por extralimitarse hacia la judicialización pública, por encima de los tribunales, o por supeditarse a otras instancias de dominación.

Desde que se democratizaron las redes sociales y los grandes conglomerados propagan que todo teléfono inteligente es un medio y todo ciudadano es comunicador, las fronteras del ejercicio periodístico, las condiciones de profesionalización y las normas éticas, se han disuelto.

Nunca el campo de las comunicaciones estuvo tan abierto para la invasión de todo tipo de prácticas legales e ilegales, invasoras e intrusivas, donde campean la astucia, los simulacros, la suplantación, la mentira y, en fin, la ley del más fuerte en el dominio de los infomedia.

En el campo periodístico lo novedoso es que las técnicas de intrusión, consideradas antes excepcionales, se están implementando velozmente por rapidización en dos dimensiones de la profesión periodística: el teletrabajo y la vigilancia.

Detengámonos en el aspecto de la vigilancia periodística, que ha motivado esta reflexión.

Las famosas investigaciones periodísticas del siglo pasado sobre el caso Vietnam, Watergate y *New York Times*, pusieron de moda no solamente los sistemas de espionaje utilizados por los gobiernos y los partidos políticos, sino también las astucias y herramientas de los periodistas para filtrarse en ámbitos grises, supuestamente protegidos bajo privacidad o confidencialidad.

Ha quedado también aclarado que gran parte de la llamada investigación periodística es resultado de la filtración de documentos con datos sensibles para gobiernos, empresas e incluso ciudadanos.

Los *Panama papers* y los *Pandora papers*, que aparecen como los grandes hitos del periodismo investigativo del siglo XXI se caracterizan tanto por el número de partícipes internacionales, como por la masa de datos manejada, en gran parte filtrados.

Baste este último caso para hacerse idea del volumen operativo manejado por el Consorcio Internacional de Periodistas de Investigación (ICIJ), por sus siglas en inglés: Los 'Pandora Papers' ('papeles de Pandora') fueron publicados el 4-10-2021 tras una larga investigación centrada en la mayor filtración de la historia de este tipo. Se trata de 11,9 millones de archivos,

por 600 reporteros de 150 medios de comunicación de más de 100 países, todos ellos coordinados por el Consorcio Internacional de Periodistas de Investigación.

La obsesión por el periodismo de precisión, ahora es suplantada por la minería de datos o los *big data*, y también por el espionaje programado de los gobiernos, cuyo tratamiento exponencial, basado ya en algoritmos, y alimentado por herramientas intrusivas, pone al periodista en el dilema ético de escoger a qué amo sirve, o en otros términos a quién vigila y por quién prefiere ser vigilado.

JESÚS MARÍA AGUIRRE

Profesor titular de la Universidad Católica Andrés Bello (UCAB). Profesor de pregrado y posgrado de la UCAB. Miembro del Consejo de Redacción de la revista *Comunicación* desde su fundación (1975).

Referencias:

- AGUIRRE, Jesús María (2015): *Comprender la Sociedad Red*. Educación y Comunicación. Caracas: Centro Gumilla.
- ____ (2020): “El régimen de la mentira: anotaciones pragmáticas y semánticas sobre las FakeNews”. En: Torrealba, Mariela y otros. *Las FakeNews en Venezuela: la mentira en la censura*. Caracas: Medianálisis, abediciones.
- ____ (2021): “Los resortes de la Fake News y su dinámica comunicacional: viralización vs. verificación”. En: Torrealba, Mariela y otros. *Desmontando la mentira: dos*

años bajo la lupa del OVFN. Caracas: Medianálisis, abediciones.

- BAMFORD, James. (2016): “The espionage economy. U.S. firms are making billions selling spyware to dictators”. En: *Foreign Policy*, January 22, 2016. Disponible: <https://foreignpolicy.com/2016/01/22/the-espionage-economy/>
- CALLENS, Stephane (2005): “La société de l’information: une société de surveillance”. En: MATHIEN, Michel. *La ‘société de l’information’. Entre mythes et réalités*. Bruxelles: Ed. Bruylant.
- MARCZAK, Bill y otros (julio 18, 2021): “Independent Peer Review of Amnesty International’s Forensic Methods for Identifying Pegasus Spyware”. *Citizen Lab*. Link: <https://citizenlab.ca/2021/07/amnesty-peer-review/>
- MAYER SCHÖNBERGER, Víctor y CUKIER, Kenneth (2013): *Big Data. La revolución de los datos masivos*. Madrid: Turner.
- NUEVA SOCIEDAD. *Capitalismo de vigilancia*. Recuperado: <https://nuso.org/articulo/capitalismo-de-vigilancia/>. NUSO N° 290 / noviembre - diciembre 2020.
- PANAMA PAPERS https://www.icij.org/investigations/panama-papers/power-players/?gclid=CjwKCAiApfeQ-BhAUEiwA7K_UH59UY-L95Z2zHvCNAHsOxdqxWN-Vk9e9qqgPX-YdUOZBJDm_6r4O7RoCOcQQAvD_BwE
- PANDORA PAPERS https://www.icij.org/investigations/panama-papers/power-players/?gclid=CjwKCAiApfeQ-BhAUEiwA7K_UH99vcYic-aOdZ8qo-YepdDqk6BZg-jZ21U-FFZcd4LKWTNQFYinSdGxoCAVYQAvD_BwE
- ZUBOFF, Shoshana (2020): *La era del capitalismo de la vigilancia*. Edic. Paidós.

Notas

- <https://www.washingtonpost.com/es/world/2021/07/21/proyecto-pegasus-malware-espia-periodistas-activistas-mexico-spyware/>
- <https://periodistas-es.com/amnistia-internacional-sutoridades-de-el-salvador-utilizan-el-programa-espia-pegasus-para-vigilar-a-periodistas-156688>.
- Canal de YouTube de Medianálisis.