Análisis de la correlación ciberespacio-política desde el realismo: El caso de las elecciones presidenciales mexicanas de 2006, 2012 y 2018

Analysis of the cyber-space - policy correlation from realism: The case of the Mexican presidential elections of 2006, 2012 and 2018

Ernesto Ángeles Guerrero*

Fecha de recepción: 22-10-2019
Fecha de aceptación: 27-05-20

RESUMEN: Actualmente el ciberespacio y el internet están en prácticamente todo el mundo, aún en países de mediano y poco desarrollo. Esta acción de penetración ha generado cambios sustanciales en las capacidades y ejercicio de poder por parte de actores estatales y no estatales, así como también dentro de la sociedad. A su vez, el ciberespacio está condicionado por las características espaciales, temporales y sociales. Esta tensión se traduce políticamente en herramientas nuevas usadas en prácticas viejas, o en prácticas nuevas impulsadas por el ciberespacio y adaptadas a un contexto e intereses específicos.

* Internacionalista, maestrando por la Universidad Nacional Autónoma de México en estudios internacionales; especialista en el análisis político e internacional del ciberespacio, el internet y la inteligencia artificial. Experiencia en consultoría y análisis político nacional y seguridad multidimensional. En la actualidad voluntario en el ICANN, la Internet Society Capítulo México y la IA2030MX. Correo electrónico: angelesgnet@hotmail.com.

El caso de las elecciones federales en México a lo largo de tres periodos presidenciales da cuenta de la relación ciberespacio - política, ya que muestra la simbiosis entre las características estructurales del ciberespacio y el sistema político-social, con todas sus limitantes técnicas, sus conflictos de poder y una serie de pautas de ejercicio político propias de México, las cuales coinciden con la limitación de opciones que brinda el ciberespacio.

Por otro lado, el desenlace en la última elección federal (2018), y la conclusión de este escrito, muestran la no correlación lineal de un argumento que simplifique la relación ciberespacio-política a manera de "a mayor capacidad e inversión en el ciberespacio = mejores resultados o mayor capacidad de determinación en los resultados", ya que esta relación no es determinante.

Palabras clave: Ciberespacio, Política Mexicana, Elecciones Federales Mexicanas, Internet, Big Data, Protección de Datos Personales, Democracia y Ciberespacio, Política y Ciberespacio, Vigilancia cibernética, Publicidad política.

SUMMARY: Currently, cyberspace and the Internet are in practically the entire world, even in countries of medium and little development. This capacity of penetration has generated substantial changes in capacities and the exercise of power by states and non-state actors, as well as within society, In turn, cyberspace is conditioned by spatio-temporal and social characteristics. This tension translates politically into new tools used in old practices, or new practices driven by space and adaptations to specific context and interests.

The case of the federal elections in Mexico during three presidential periods put on evidence the political relationship between cyberspace and politics, since it shows the symbiosis between the structural characteristics of the political and social system, with all its technical limitations, its power conflicts and a series of guidelines for Mexico's own political exercise, which coincide with the limitations of options offered by cyberspace.

On the other hand, the outcome in the last federal election (2018), and the conclusion of this paper, shows the non-linear correlation of an

argument that simplifies the cyberspace-politics relationship in a way of "greater capacity and investment in cyberspace = better results or greater capacity for determining results ", but this relationship is not decisive.

Key words: Cyberspace, Mexican Politics, Mexican Federal Elections, Internet, Big Data, Personal Data Protection, Democracy and Cyberspace, Politics and Cyberspace, Cyber Surveillance, Political Advertising.

Introducción

La aparición y consolidación del ciberespacio, entendido como una colección de: instalaciones, datos, usuarios y operaciones interconectadas a manera de red abierta (como el internet) o cerrada (redes privadas), ha propiciado un cambio de paradigma dentro de la historia y devenir de la humanidad. Nunca habían existido tantos datos, información y conocimiento generado, consumido, almacenado, reproducido, transmitido, compartido y comercializado en el mundo.

El ciberespacio ha generado sinergias, reacomodos y nuevas capacidades de poder entre actores estatales y no estatales; con las cuales la vigilancia, el control e influencia pueden ser implementadas de maneras y a escalas nunca vistas previamente, así como también ha ocasionado más transparencia, fortalecido la libertad de expresión y promovido la interacción entre los gobernantes y los gobernados.

Desde cualquier latitud, temporalidad y escenario humano, la generación y posesión de datos, información y conocimiento han sido centrales dentro de las capacidades de poder de todo actor; sin embargo, con el ciberespacio estas fuentes de poder se han potenciado o simplemente cambiado.

La triada datos-información-conocimiento, así como la tecnología y de manera más general, el ciberespacio, presentan características estructurales homologadas, tales como los protocolos y estándares que lo hacen funcionar, así como también la construcción y diseño de dispositivos, lo que genera una sinergia compartida; sin embargo, el funcionamiento

e impacto del ciberespacio es heterogéneo y multivariado, mismos que dependen del contexto.

El ciberespacio, comprendido como un sistema socio-tecnológico, sucede en un contexto y tiempo específicos; por lo tanto, los usuarios y diversos actores implicados se encuentran constreñidos bajo estructuras y prohibiciones de distintos tipos (comunicación, de acceso, difusión, búsqueda, comportamiento, normas morales y de valores, entre otros). De estas estructuras sobresale la estructura institucional que es el Estado como contenedor de la vida en sociedad. (Hughes, 1983).

En este sistema, los actores establecen vínculos y procesos de cooperación y conflicto entre sí, al interior del Estado y también entre Estados, lo cual es determinado por prácticas y sistemas políticos (entre algunos otros elementos) de dichas entidades. En tal interacción, el ciberespacio puede actuar en dos formas: como escenario y como herramienta.

Lo anterior es importante ya que en la relación política-ciberespacio, la política condiciona algunas estructuras, relaciones, comportamiento, procesos y diseño del ciberespacio y, a su vez, el ciberespacio ha comenzado a condicionar, bajo parámetros funcionales y estadísticos, la manera en la cual se vive y ejerce la vida humana y, por ende, la política.

Esta sinergia ha generado nuevas capacidades políticas, tal como el estudio numérico y pormenorizado de la sociedad y sus distintos patrones digitalizados, lo que resulta en capacidades como la inferencia de preferencias, ideologías y posturas, la generación de tácticas de influencia ad hoc (masivas y personalizadas); así como también ha fortalecido y renovado las capacidades y prácticas tradicionales como la vigilancia, el control y la censura.

El presente artículo tiene el objetivo de contribuir a la discusión e investigación del ciberespacio e internet desde una postura realista, la cual se centra en el conflicto por el poder político más que en la cooperación y otras bondades del ciberespacio, tal como lo hacen los idealistas.

La hipótesis de la cual se parte es que al día de hoy, la influencia del ciberespacio depende más del contexto político y social donde sucede, que de la estructura que éste provee como plataforma, herramienta o espacio tecnológico.

Lo anterior contraviene el determinismo ideológico acerca de la capacidad de influencia del ciberespacio en la política y en la democracia; sobre todo la influencia positiva, ya que esta investigación se centra en el conflicto y peligros que genera la dinámica ciberespacio – política.

Esto es importante, ya que en un futuro cercano se piensa que se crearán y diversificarán más los productos y servicios basados en inteligencia artificial y toda una serie de tecnologías interconectadas y centradas en datos, lo que nos hace llegar a la posible conclusión de un incremento en la influencia de este sistema tecnológico en la política.

Lo anterior es algo que debe mantenerse al margen, ya que existen diversos peligros asociados a la dominación de la tecnología sobre el sistema político, lo que puede trastornar a la política y el funcionamiento de la sociedad, sus procesos e instituciones a un nivel nunca visto antes.

El estudio de caso que se piensa analizar es el ejercicio del poder en el ciberespacio de 2006 a 2019 bajo diferentes administraciones federales, caracterizadas en general por un ciberespacio conflictivo y plagado de prácticas políticas que en algunos casos, no estaban y no están reguladas o no pueden ser del todo reguladas sin impactar en los principios del internet y el ciberespacio, aunque eso no impide su ejercicio antidemocrático y nocivo para el sistema político.

Contexto

En el análisis de la relación entre el poder y el ciberespacio cabe resaltar la diferencia del poder *en el* ciberespacio y el poder *del* ciberespacio. En el estudio del poder en el ciberespacio resaltan autores como Stevens (2017), el cual aplica la taxonomía de poder de Bernett y Duvall (2005). Esta taxonomía hace referencia al poder estructural, institucional, simbólico y obligatorio, lo cual se relaciona a la construcción y mantenimiento del ciberespacio como sistema.

Por otro lado, el poder del ciberespacio, o denominado ciberpoder, es definido por autores como Daniel Kuehl: "La habilidad de usar el ciberespacio para crear ventajas e influenciar eventos en otros entornos

operacionales y a través de instrumentos de poder".[1] Otros autores que hablan acerca del ciberpoder son: Joseph S. Nye (2010), Vaishnav y Choucri (2013), entre otros.

El comportamiento del ciberpoder para Nye depende de una serie de recursos relacionados a la creación, control y comunicación de información basada en la infraestructura electrónica y computacional, redes, software, habilidades humanas. Esto incluye el internet de las redes de computadoras, pero también intranets, tecnologías celulares y comunicaciones espaciales (Nye, 2010).

Nye considera que una diferencia en el ejercicio de poder tradicional frente al ciberpoder es que las barreras de entrada en el dominio cibernético son tan bajas que actores no estatales y pequeños Estados pueden producir efectos significativos a niveles bajos de costo.

Según Nye, el ciberpoder depende directamente del ciberespacio y de sus características físicas y virtuales, ya que "el poder depende del contexto y el ciberpoder depende de los recursos que caracterizan el dominio del ciberespacio". (Nye, 2010).

En este sentido, las capacidades de actores que se consideran más relevantes son: la vigilancia y medición (acopio de datos, información y conocimiento por medio de las diferentes tecnologías y funciones del ciberespacio); y la influencia política directa e indirecta por medio de campañas, publicidad, entre otros métodos que impactan el proceso democrático.

El estudio de la vigilancia en internet ha sido analizado desde diferentes disciplinas, lo que ha resultado en conceptos como "la nueva vigilancia, vigilancia de datos, el (súper) panóptico electrónico, vigilancia electrónica o vigilancia digital" (Fuchs, Boersma, Albrechtslund y Sandoval, 2012), todos estos referidos a las capacidades de vigilancia pública y privada que brinda el ciberespacio, ya que muchos sistemas de vigilancia

1 Citado por Klimburg, Alexander y Faesen, Louk (2018). A balance of power in cyberspace. The Hague Center for Strategic Studies, p.3. Disponible en el vínculo: https://www.dropbox.com/s/rb2z5jhq4nuh6kb/A%20balance%20of%20power%20in%20cyberspace.pdf?dl=1

no son abiertos, sino en redes privadas; así como también la vigilancia en el internet y en los dispositivos físicos del ciberespacio.

La capacidad de vigilancia dentro del ciberespacio depende de diferentes elementos, entre estos resaltan: la triada datos, información y conocimiento; así como también la influencia en la construcción y producción de la tecnología, ya que técnicamente es posible la vigilancia por medio de dispositivos y tecnologías físicas, así como el acceso a datos por medio de software.

Esta investigación pertenece a esta segunda visión del poder y el ciberespacio: el ciberpoder, ya que da por sentado las diferentes características de la construcción del ciberespacio y se enfoca en las consecuencias de su uso y funcionamiento dentro de la sociedad en las cuales sucede, tanto a nivel nacional como internacional.

El ciberpoder en México se ha ejercido de manera progresiva e intensiva en los procesos electorales conforme las posibilidades tecnológicas lo han permitido; así como también conforme las adaptaciones del ciberespacio por los usuarios mexicanos.

La vigilancia política y el ciberespacio

La vigilancia ha sido una herramienta política constante dentro de la historia de la humanidad, esto debido a la capacidad de poder que supone su relación con la triada datos, información y conocimiento, los cuales pueden pertenecer a otro actor por sobre quien se ejercerá el poder, a terceros o hasta el entorno y otras variables que influyen a las relaciones de poder.

En el caso de los Estados, el ejercicio de vigilancia ha transitado por diferentes métodos, desde el espionaje de seguimiento físico, hasta métodos masivos facilitados por las capacidades científico- tecnológicas.

El ciberespacio ha originado un aumento en la capacidad de vigilancia por parte de diferentes actores, no sólo por el Estado, así como también ha implicado el crecimiento y expansión de las técnicas de vigilancia en

otras áreas de la vida en sociedad más allá de la política, sobre todo en la economía y otras áreas como la educación, medicina, entre otras.

Estas posibilidades se ven potenciadas debido a las características que brinda el funcionamiento del ciberespacio y el internet a los usuarios:

- Anonimia
- Riqueza e información que las redes sociales proveen
- La omnipresencia del ciberespacio
- La rapidez (transmisión, comunicación, intrusión, entre otros)
- La versatilidad de roles que los usuarios pueden asumir en sus relaciones
- La capacidad de combinar (y analizar) información de manera flexible
- La preeminencia de la subjetividad por sobre la objetividad
- La ausencia parcial o total de mecanismos de regulación. (Auvinen, 2013)

Estas características del ciberespacio generan una serie de capacidades de vigilancia, de entre las cuales resalta la vigilancia específicamente de internet, más allá de redes privadas y otros espectros de transmisión de información.

De acuerdo con Starke-Meyerring y Gurak, es posible diferenciar entre tres tipos de tecnologías de vigilancia por internet: 1) vigilancia de los datos personales capturados del uso general de Internet, 2) vigilancia de datos personales capturados mediante el uso servicios especializados de Internet, 3) tecnologías y prácticas diseñadas para acceder a datos de usuarios de Internet.[2]

2 Citado por Fuchs, Boersma, Albrechtslund y Sandoval (2012: 332).

El espionaje estatal y el uso del ciberespacio en la administración 2006-2012

Pese a que el uso del internet e internet móvil era escaso en México en el año 2006, el desarrollo científico tecnológico de capacidades en el ciberespacio ya permitía la existencia de servicios digitales que explotaban la intercomunicación e interoperatividad de dispositivos, lo que facilitó y aumentó las capacidades de vigilancia del Estado.

Desde el 2007 el gobierno federal adquirió un sistema de vigilancia diseñado por la compañía Verint Systems Inc, Ltd, empresa ligada a Israel y vendido por su filial en México Sogams, SA de CV. La adquisición del sistema fue compartida junto con el gobierno de Estados Unidos dentro del marco de lucha contra el narcotráfico y otras áreas de seguridad exterior. Dicho sistema fue nombrado Sistema de Vigilancia Técnica de México y permitía al gobierno mexicano "interceptar, analizar y usar información interceptada de todo tipo de sistemas de comunicaciones que operan en México" (Beckhusen, 2013).

A la par de la adquisición del Sistema de Vigilancia Técnica de México, en 2013 trascendió, gracias a la investigación de Citizen Lab (SonTusDatos, 2014), que en 2007 el gobierno federal mexicano adquirió otro software de vigilancia de nombre Finfisher. Este era un software de espionaje diseñado por la empresa anglo-alemana Gamma Group International y vendido por la empresa Obses SA de CV en una compra que ascendió a los $109.3 millones de pesos (APC-HIVOS-GISW, 2014).

Una vez que FinFisher se alojaba en el dispositivo, le daba control remoto al atacante, permitiéndole grabar conversaciones; tener acceso a los archivos guardados; descargar listas de contactos, correos electrónicos, mensajes de texto, entre otros contenidos. FinFisher también podía intervenir la cámara web y el micrófono del aparato infectado. Según Digital Rights, hay indicios de que FinFisher fue usado en la Ciudad de México, el Estado de México y en otros estados de la república como en Chiapas, Coahuila, Quintana Roo, Puebla, Tamaulipas y Veracruz. (Flores, 2015).

Debido al hackeo de la empresa italiana Hacking Team en 2015 se supo que en 2010 el gobierno calderonista les compró un software de espionaje llamado Remote Control System, también denominado Da Vinci. (Villaseñor, 2017).

Este era un programa malicioso que una vez instalado permitía extraer todo tipo de información y grabar la actividad en el teclado. El programa malicioso fue desarrollado por una empresa italiana de nombre Hacking Team, la cual ofreció sus servicios a países como Rusia, Uzbequistán, Sudán Chipre o Egipto. Actualmente los contratos (128/13 y 020/15) por los cuales el CISEN adquirió el spyware Galileo a Hacking Team son considerados como reservados hasta el 2027. (Schwartz, 2017).

De acuerdo con Linaloe Flores (2018), el INAI instruyó al órgano de inteligencia modificar la justificación de la reserva. El INAI asesoró para que no se basara en el artículo 14 de la antigua Ley Federal de Transparencia –como lo había hecho–, sino en el 13 de la misma ley, en aras de dejar claro que la revelación de la información de Galileo podría conllevar riesgos.

En esta misma lógica se enmarca el aumento de documentos clasificados en las últimas tres administraciones federales, las cuales son: Vicente Fox Quesada (2000-2006) con 3 millones 839 mil carpetas reservadas, Felipe Calderón Hinojosa (2006-2012) con ocho millones y, por último, Enrique Peña Nieto (2012-2018) con 16 millones 109 mil 762. De acuerdo con las categorías de Starke-Meyerring y Gurak,[3] es posible inferir que las prácticas de vigilancia del gobierno federal mexicano durante la administración de Felipe Calderón cumplen con los diferentes tipos de vigilancia en internet que proponen los autores.

Esto no significa que parte de estas actividades y prácticas pertenezcan al ejercicio legítimo del uso de la fuerza, así como de las capacidades y obligaciones de seguridad del Estado, lo que se traduce en vigilancia legal y legítima; sin embargo, esta capacidad política está en constante tensión entre lo que es legítimo y no.

3 1) vigilancia de los datos personales capturados del uso general de Internet, 2) vigilancia de datos personales capturados mediante el uso servicios especializados de Internet, 3) tecnologías y prácticas diseñadas para acceder a datos de usuarios de Internet.

El espionaje estatal y el uso del ciberespacio en la administración de Peña Nieto

El espionaje durante el gobierno peñanietista se caracterizó por el caso de Pegasus, un software de espionaje muy efectivo que permitía la selección de objetivos individuales y su espionaje profundo. El primer descubrimiento de Pegasus fue en 2016 gracias a la denuncia del activista emiratí Ahmed Mansoor, el cual denunció a Citizen Lab una serie de mensajes sospechosos que lo invitaban a abrir ligas adjuntas.

El análisis mostró que el activista era objetivo de Pegasus, un sofisticado software de vigilancia comercializado a diferentes gobiernos por la empresa NSO. De acuerdo con el análisis inicial del software espía, la mayoría de los dominios de la infraestructura de NSO se encontraban vinculados a México, lo cual significaba que autoridades mexicanas eran clientes de NSO y que personas en México podrían haber sido objetivos de esta forma de vigilancia. (R3D, 2016). No fue sino hasta febrero de 2017 cuando Citizen Lab, junto con otras organizaciones no gubernamentales en México como R3D y SocialTic, documentó cómo los defensores de los consumidores de alimentos, científicos y científicos del gobierno mexicano también recibieron enlaces a la infraestructura que conectaba con NSO Group.

El programa descubierto tenía el nombre Pegasus y fue vendido por la empresa israelí NSO Group por medio de Balam Seguridad Privada SA de CV a la extinta Procuraduría General de la República (PGR) (Asad y Perloth, 2017). Pegasus se distinguió por la capacidad de infiltración en los teléfonos inteligentes y otros aparatos para monitorear cualquier detalle de la vida diaria de una persona por medio de su celular: llamadas, mensajes de texto, correos electrónicos, contactos y calendarios. Incluso podía utilizar el micrófono y la cámara de los teléfonos para realizar vigilancia; el teléfono de la persona vigilada se convertía en un micrófono oculto. (Camarena, 2019).

La compra y uso del programa fue realizado por al menos tres agencias federales por un monto de casi 80 millones de dólares (INFOBAE, 2019); sin embargo. el monto de las operaciones individualmente dependía del número total de objetivos a investigar. Se tiene registro que se enviaron más de 76 mensajes con enlaces al marco de explotación de NSO Group a periodistas mexicanos, abogados y un niño menor. (Scott-Railton, Marczak, Razzak, Crete-Nishihata y Deibert, 2017).

La lista de objetivos de Pegasus abarcó a la periodista Carmen Aristegui y su hijo Emilio; también, Daniel Lizarraga, Salvador Camarena, Rafael Cabrera y Carlos Loret de Mola; los defensores de Derechos Humanos del Centro Miguel Agustín Pro, Mario Patrón Stehanie Brewer y Santiago Aguirre; los políticos panistas Ricardo Anaya y Fernando Rodríguez Doval, así como el entonces senador por este partido, Roberto Gil Zuarth, entre otros (Asad y Perloth, 2017).

Además del uso intensivo de programas diseñados para la vigilancia se han hecho seguimientos por medio de los elementos del ciberespacio, ya sea por medio de las conexiones a internet y sus elementos físicos inmiscuidos, como la geolocalización. El número de escuchas telefónicas legales aprobadas por el Fiscal General de México aumentó en casi un 50 por ciento entre 2013 y 2016, y las autoridades han emitido miles de solicitudes a empresas de Internet durante ese período de tiempo solicitando información del usuario. (Parker, 2017).

El Gobierno de Andrés Manuel López Obrador. *¿El fin de la vigilancia?*

Desde su candidatura de 2018 en el bloque Morena-PT-PES, el ahora presidente de la República, Andrés Manuel López Obrador, se quejaba acerca de la labor de investigación llevada a cabo por el CISEN contra su persona, catalogándola en algunos momentos de persecución política; por tanto, como propuesta política promovió la desaparición del CISEN y el fin de la vigilancia política por medio de las instituciones del Estado. (Excélsior, 2018).

En el proceso electoral no sólo fue AMLO quien se quejó de las actividades del CISEN, sino que también el candidato de la coalición PAN-PRD-MC, Ricardo Anaya, acusó al CISEN de ejercer vigilancia contra él con fines políticos. Tras ambas declaraciones de los candidatos, el Secretario de Gobernación de esa administración, Alfonso Navarrete Prida, reconoció que el CISEN estaba pendiente de las actividades de los aspirantes a la presidencia, aunque negó que lo hiciera con el objetivo de espiarlos, sino que fue con el objetivo de proteger a actores de vital importancia en la vida política de México. (Tirado, 2018).

Después del triunfo de AMLO, éste mencionó su interés en hacer efectiva la desaparición del CISEN y la creación de una nueva agencia de inteligencia (Agencia Nacional de Inteligencia) que no llevara a cabo espionaje telefónico a opositores. Aunque a mediados de 2019, investigadores del Citizen Lab, Whatsapp y organizaciones de la sociedad civil como R3D revelaron que, entre abril y mayo del 2019, se detectaron intentos de infecciones usando este malware en contra de individuos en territorio mexicano. Los ataques buscaban infectar equipos mediante llamadas de voz vía Whatsapp. Los usuarios ni siquiera tenían que contestar la llamada para que, a través del malware, los atacantes pudieran tomar control del dispositivo. La llamada infecciosa podía ser eliminada del historial para no dejar evidencias. (Riquelme, 2019).

Según Luis Fernando García, director de R3D, entre el 29 de abril y el 10 de mayo del 2019 NSO Group infectó aproximadamente a mil 400 personas a través de Whatsapp y justamente se menciona que esos usuarios, o una parte importante de esos usuarios, son abogados, defensores de derechos humanos, periodistas, activistas, diplomáticos y agentes gubernamentales de alto nivel. "Los usuarios atacados tienen números de Whatsapp que tienen un código de país, solo se mencionaron algunos, entre ellos Emiratos Árabes Unidos y México." (Ojeda de la Torre, 2019).

Ante esta situación, el presidente Andrés Manuel López Obrador, negó que se hiciera uso del software de vigilancia y aseguró que se investigaría al respecto (Aristegui Noticias, 2019), aunque al día de hoy no ha habido una investigación concluyente, salvo el nombramiento y remoción de Patricia Rosalinda Trujillo Mariel, excoordinadora nacional operativa de la Guardia Nacional, debido a una investigación en su contra por la adquisición de Pegasus. (Jurado, 2020).

Los procesos electorales de 2006 a 2018

Esta investigación parte del entendido que, tal como lo establece la investigadora Pippa Norris: la red "puede favorecer la participación política pero no transformarla de manera radical" (Norris, 2002). Esta frase nos ayuda a entender cómo es que el funcionamiento del ciberespacio se relaciona íntimamente con las sociedades y contextos en los cuales este existe.

El cambio en la política que significó el advenimiento del ciberespacio no sólo está ligado a la capacidad del Estado de vigilar a sus ciudadanos, sino también en los diferentes modelos económicos basados en la vigilancia de los consumidores, ya que, además del poder coercitivo y directo de la vigilancia estatal en seguridad, la publicidad y diferentes formas de persuasión económica han sido aplicadas a la política.

Como el Centro para la Democracia Digital lo ha hecho notar ampliamente, el funcionamiento del ciberespacio e internet está ligado a diferentes dominios monopólicos, recolección masiva y abuso de datos personales, adicción a dispositivos, explosiones en propaganda marcada por una nueva presencia y amplia distribución de noticias falsas, memes racistas y de derecha, y una marginación de medios y voces progresistas. (Chester y Rosenfeld, 2019).

Hay dos desarrollos generales que tienen un enorme impacto en las elecciones, que dependen de la base modelo de recolección de datos de economía de vigilancia. El primer problema es que la tecnología avanzada hace posible para las campañas la ampliación de la interacción con los votantes individuales. Nuevas herramientas permiten a las compañías de datos alcanzar, comprometerse y generar micro-objetivos de votantes con precisión exacta. Detrás de este escrutinio hay un poderoso sector corporativo que incluye corredores de datos, identidad de plataformas de gestión, nubes de marketing, medición de empresas, redes sociales y la industria publicitaria (Chester y Rosenfeld, 2019). El segundo gran problema es el estallido de noticias basura y desinformación.

La desinformación y otras formas de comunicación manipuladora y antidemocrática se han convertido en un problema para la política de Internet. Si bien tales operaciones no se limitan a la política electoral, los esfuerzos para influir y perturbar las elecciones han creado preocupaciones importantes.

La publicidad digital basada en datos ha jugado un papel clave en facilitar las campañas de manipulación política. En lugar de incidentes independientes, las operaciones de manipulación reflejan problemas sistémicos dentro de los mercados y las infraestructuras de publicidad digital. Las respuestas políticas deben incluir enfoques que consideren las plataformas de publicidad digital y las capacidades estratégicas de comunicación que permiten. En su raíz, estos sistemas están diseñados para facilitar relaciones asimétricas de influencia. (Chester y Rosenfeld, 2019).

Un hallazgo central de este estudio es que los sistemas de anuncios digitales se han construido con capacidades que pueden ser fácilmente armadas. Cuando los operativos políticos arman la tecnología publicitaria, la usan para identificar puntos débiles donde los grupos y las personas son más vulnerables a la influencia estratégica. En tales casos, los datos de las personas se vuelven contra ellos y se utilizan para ayudar a los anunciantes políticos a influir más eficazmente en sus objetivos.

El uso de tecnología en la política ha sido acorde a las posibilidades del ciberespacio en su momento, lo que se ilustra claramente en los procesos políticos, en donde es clara la transición de una estrategia simple de envío de publicidad por medio de correos, al estudio segmentado de poblaciones y la creación de contenido ad hoc.

El ciberespacio en las elecciones federales de 2006

El uso del ciberespacio en elecciones federales a nivel mundial tiene su origen en 2004 en Estados Unidos, cuando Al Gore y George W. Bush utilizaron el correo electrónico como plataforma de difusión de mensajes y propuestas en sus campañas políticas; esto sólo fue el preámbulo

de lo que se avecinaría en los años sucesivos, ya que en ese momento el ciberespacio sólo sirvió como una herramienta de marketing muy básica que digitalizaba estrategias como el envío de publicidad por correo.

La utilización del ciberespacio en una elección federal en México fue a partir de las elecciones presidenciales de 2006, cuando la contienda se dio principalmente entre el candidato panista Felipe Calderón, el candidato de la Alianza por el Bien de Todos (APBT), Andrés Manuel López Obrador, y el candidato priísta, Roberto Madrazo.

Al 2007 existían alrededor de 23.7 millones de internautas, de los cuales el 79% oscilaba en una edad de entre 18 y 34 años; de éstos, la mayoría (el 34%) se conectaba en un promedio de 1 a 2 horas diarias. Y, de sus actividades sociales usuales en internet, se destacó el uso de correo electrónico (83%), seguido del envío de mensajes instantáneos (74%) y de visitar una sala de chat (64%). De ese número de usuarios, la mayoría (56.1%) tenía una situación económica holgada. (Asociación de Internet , 2007).

Bajo este universo digital, las estrategias electorales se distinguieron por el uso del correo electrónico como medio de publicitar al candidato con el electorado; sin embargo, y a diferencia de las elecciones estadounidenses, el uso de ataques a la imagen de otros candidatos fue una norma dentro y fuera de internet, lo que refleja directamente la relación entre cultura política y la instrumentación de tecnologías y procesos que sirvan a diversos fines, más allá de ideales democráticos y utópicos de cooperación y fortalecimiento democrático.

En esa elección el 8% de la población total afirmó que recibió correos por parte de partidos, la mayoría (45.2%) aseveró haber recibido un mensaje favorable en favor del candidato del PAN, Felipe Calderón, frente a un 5.3% de menciones en su contra; el candidato priísta, Roberto Madrazo, reportó un total de 24.2% de menciones positivas y un total de 13.7% de menciones negativas; mientras que AMLO, contrariamente a estos dos, presentó un 11.6% de menciones positivas y un total de 32.2% de mensajes con información negativa. (Meneses Rocha y Bañuelos Capistrán, 2009).

Lo anterior se desprende también del tipo de campañas que se decidieron hacer, ya que la campaña elaborada por el PAN apostó fuertemente por los medios masivos, y sobre todo la televisión, mientras que el candidato de la APBT optó por una campaña directa con los electores por medio de presentaciones en eventos públicos.

De acuerdo con Meneses Rocha y Bañuelos Capistrán, las elecciones federales de 2006: "en el plano político no crearon una agenda paralela ni aportaron información que los medios tradicionales a través de los spots no hayan dicho. Se limitaron a reproducir el eje del discurso negativo de los candidatos diseñado por sus estrategas".

Esto se puede entender debido a que en ese período la exposición a medios como la televisión y el radio alcanzaban cifras del 98% y del 70%, respectivamente, frente al 31% de exposición hacia el internet. (Asociación de Internet, 2007). Esto pone en evidencia la inmadurez y capacidad de alcance de la red y el ciberespacio en general en ese momento.

En ese proceso electoral el gasto total destinado a radio y tv ascendió a 2 580 mdp. (Animal Político, 2011). De este gasto, la campaña de Calderón se destacó por ser la más costosa, ya que a los dos días de comenzada la contienda ya había hecho un gasto de 7 millones 343 mil 852 pesos. (El Universal, 2006).

El proceso electoral para la elección de presidente en 2006 es muestra clara de las características del ciberespacio en ese momento, así como del mercado en general, en donde el análisis de datos y el big data aún tenían que esperar algunos años para su aparición y fortalecimiento en el ciberespacio y el mercado internacional.

El ciberespacio en las elecciones federales de 2012

Mientras que las elecciones presidenciales estadounidenses de 2004 marcaron el camino que seguirían los procesos electorales en otras latitudes, las elecciones federales estadounidenses de 2008 representaron

un viraje en la forma de cómo se llevarían a cabo no sólo los procesos electorales, sino la política y sus capacidades cuantificables.

Este cambio se debió en gran parte a la mejora de las capacidades tecnológicas y a la constante evolución del ecosistema que es el ciberespacio, así como también al fortalecimiento e instalación de infraestructuras de comunicación.

Con esto se marcó el inicio de una compleja relación que apunta no sólo a la profundización de la digitalización de servicios políticos, sino también al uso masivo de datos (la mayor parte de ellos personales) de múltiples formas y aplicaciones: la cuantificación emocional y conductual de los votantes y la generación de estrategias y contenido acorde a estas variables.

La campaña presidencial de Barack Obama en 2008 se caracterizó primeramente por ser llevada a cabo en un país con una penetración de internet del 75%; además, el uso del ciberespacio fue intensivo, participativo y flexible (Meneses Rocha y Capistrán Bañuelos, 2009). Dicha campaña no sólo se limitó a distribuir propuestas y la imagen del candidato, sino que llevó a cabo una estrategia que combinó el análisis de bases de datos, la conformación de comunidades en línea, la estructuración de una red de apoyos y donativos coordinados en la red, la comunicación bidireccional entre el equipo de Obama y los votantes, la estructuración de voluntarios y activistas autónomos, el uso combinado de sitios web y redes sociales, entre otras.

Las elecciones presidenciales de México en 2012 tuvieron lugar con estas lecciones dejadas por la campaña de Obama, bajo una experiencia como la de 2006, en un ciberespacio más maduro, con una específica cultura política como la mexicana y, sobre todo, tras dos sexenios panistas que no habían cumplido con las expectativas sociales.

Para 2012, la penetración de internet había aumentado a 45.1 millones de usuarios nacionales con una población votante mayoritariamente compuesta por internautas de una edad que oscilaba de entre los 25 a 44 años. (Asociación de Internet, 2013).

En este año el tiempo de conexión promedio había aumentado a 4 horas diarias. De entre las principales actividades que llevaban a cabo, la pri-

mera fue uso de correo electrónico (80%); a diferencia de 2006, el uso de redes sociales apareció y se situó en la segunda actividad más realizada (77%), seguida de la búsqueda de información (71%). (Asociación de Internet, 2013).

En este contexto y en comparación con las elecciones de 2006, las redes sociales se posicionaron en un 92% de uso de los internautas, con un promedio de uso de 4 redes y con Facebook como la red social más utilizada (90% de los internautas inscritos); del total de usuarios de redes sociales, el 51% accedió a publicidad política. (Asociación de Internet, 2013).

En las elecciones de 2012 participaron el PAN, con su candidata Josefina Vázquez Mota; la Coalición Compromiso por México (PRI y PVEM) que postuló a Enrique Peña Nieto; por último, la coalición Movimiento Progresista (PRD, PT y MC) nominó a Andrés Manuel López Obrador, el cual se presentó en su segunda elección a la presidencia. Las elecciones de 2012 fueron para México lo que las elecciones presidenciales estadounidenses en 2008 fueron para el mundo.

A diferencia de las elecciones estadounidenses de 2008, las elecciones de México en 2012 sucedieron en un entorno político donde los bots y trolls ya existían como herramienta política en el ciberespacio, tal fue el caso de la elección gubernamental de Estado de México un año antes, en 2011. (Islas y Pimienta, 2016). Tras las lecciones que dejó 2006, el PRI, de entre los otros partidos, se distinguió por una preparación no sólo en la publicidad de medios (radio, tv y medios impresos), sino que desde 2007 implementó una estrategia web con un enfoque basado en las redes sociales (en ese momento la red utilizada fue Hi5).

En 2009 el diario británico The Guardian dio a conocer un documento en donde se hablaba de la colaboración de Televisa con el PRI en un proyecto para promover videos a favor de la campaña del PRI vía correos electrónicos masivos o en sitios como YouTube. El nombre de la colaboración era "proyecto Handcock", y en este no sólo estaban inmiscuidos el PRI y Televisa, sino que fueron asesorados por la empresa Blue State Digital, la cual trabajó con los demócratas en la icónica elección presidencial de Obama en 2008. (Aristegui Noticias, 2012).

En ese momento la penetración de la televisión se mantenía muy por delante por sobre el internet, lo que añade importancia a la alianza PRI-Televisa. Además, quien fue la coordinadora de la estrategia de la campaña de Peña Nieto en 2012, Alejandra Lagunes, fue asesorada por Blue State Digital, por lo que, al igual que la campaña de Obama, incorporó varias plataformas digitales como apoyo en la campaña, tales como Facebook, Twitter, YouTube, Google Plus (Google+), Instagram y Foursquare.

La participación de jóvenes fue un elemento medular en la estrategia de campaña del PRI, ya que éstos fungieron como un elemento de posicionamiento y manipulación de la percepción en redes sociales. La relación entre los jóvenes y su apoyo a Peña puede resumirse en dos casos: el movimiento "ectivista" y la creación de "PRIbook". El movimiento ectivista comenzó en diciembre de 2009 cuando un simpatizante priísta creó en Facebook una página de apoyo a Peña Nieto. Tres años después, este movimiento aglutinó a jóvenes que apoyaban a Peña y se organizaban para impulsar temas en Internet por medio de temas de tendencia en Twitter. (Laurant, 2018).

Por otro lado, en 2012 se creó "PRIbook", un sitio que concentró a las juventudes del PRI para apoyar en Internet a su candidato presidencial. En esa red social sólo los miembros del partido tenían acceso y se usaba para coordinar las acciones de apoyo a Peña Nieto en Facebook, impulsar un hashtag en Twitter o reaccionar a los ataques de los opositores. El registro en Pribook requería de una serie de datos personales básicos de los priístas, tales como nombre, dirección de correo electrónico y el sector del PRI al que estaban afiliados. (ADN Político, 2012).

A su vez, López Obrador, pese a pertenecer a la coalición Movimiento Progresista, creó una red social en torno a su Movimiento de Regeneración Nacional, MORENA (aún no reconocido como partido). En este sitio no era necesario el crear una cuenta, aunque existía esa posibilidad, ya fuera directamente o por medio de alguna red social. Aquí la interacción no estaba ligada a la autentificación por parte de una jerarquía de partido; características del sitio permitían la interacción directa entre usuarios.

En este proceso, los partidos con más presencia en las redes sociales eran el PRI (21,666 usuarios de Facebook y 2,662 usuarios de Twitter), el PAN (1,341 usuarios en Facebook y 23,663 en Twitter), seguido del PRD (5,213 usuarios de Facebook y 7,900 usuarios de Twitter. (ADN Político, 2012). Los candidatos con más seguidores estaban divididos, tanto por partidos, como por red social: Enrique Peña Nieto con 1,008,018 seguidores en Facebook y Andrés Manuel López Obrador con 97,274 seguidores en Twitter.

Las redes sociales no sólo generaron fenómenos y sinergias dentro de los partidos, sino que también impactaron en la actividad de los votantes; tal fue el caso del movimiento #YoSoy132. Éste se coordinó, articuló y difundió en parte gracias al ciberespacio, ya que el movimiento se originó como una protesta estudiantil que buscaba la democratización de los medios de comunicación, la creación de un tercer debate entre los candidatos presidenciales y el rechazo a lo que a su parecer fue la imposición mediática del candidato priísta. (Martínez, 2012). La interacción de este movimiento con los simpatizantes del PRI generó una serie de sinergias que se vieron enmarcadas por lo que el periodista Héctor De Mauleón señala:

"La novedad de las elecciones de 2012 fue que los candidatos crearon ejércitos digitales encargados de abrir frentes electorales en la red. Tuiteros a sueldo, cuentas falsas, militantes en línea, robots controlados por programas informáticos (con el fin de) crear temas de moda y mejorar la imagen del uno mediante el deterioro de desprestigio de otro" (De Mauleón, 2012).

En esta tónica, en marzo de 2012 se calculaba un total de 4,103,200 cuentas de seguidores de Peña Nieto en Twitter, de las cuales 2,480,000, es decir, 60.44 %, estaban activas. Para algunos expertos, entre el 20 y 30 % de los seguidores de Peña en Twitter eran bots. (Islas y Pimienta, 2016). Un actor clave en la campaña negra digital del PRI fue el estratega político J.J. Rendón, el cual trabajó en la campaña por un período que fue de 2011 a 2013.

La importancia de este estratega recae en la guerra sucia que desató en las redes por medio de la contratación del hacker Andrés Sepúlveda. Esta persona es un hacker colombiano que en 2012 se dedicó, de acuerdo

con su testimonio, a "hacer acciones de guerra sucia y operaciones psicológicas, propaganda negra, rumores, en fin, toda la parte oscura de la política que nadie sabe que existe pero que todos ven". El costo de sus servicios para la campaña de Peña Nieto fue de 600,000 dólares durante tres años. Entre los costos que ofrecía, había un paquete por 12,000 dólares al mes. Con este paquete, un cliente contrataba a un equipo que podía hackear teléfonos inteligentes, falsificar y clonar sitios web y enviar correos electrónicos y mensajes de texto masivos. (Robertson, et. al. 2016).

La campaña presidencial de Peña Nieto es una clara muestra de cómo el ciberespacio y su uso con fines políticos había cambiado drásticamente en apenas seis años; sin embargo, dicho cambio estuvo enmarcado en una cultura política que refleja no sólo valores democráticos y participativos dentro de los electores, sino también la tendencia al uso de la guerra sucia en las campañas políticas y el recurrir a descalificaciones personales, contextuales, funcionales o de cualquier tipo.

El caso de la campaña electoral de 2012 fue acorde a las capacidades que brindaba el ciberespacio en ese momento. Es por esto que el uso masivo de datos no tuvo tanto impacto, ya que aún no se desarrollaba del todo el potencial del big data y otras capacidades del ciberespacio, tal como se observó en las elecciones de 2018.

El ciberespacio en las elecciones federales de 2018

El proceso de las elecciones federales de 2018 siguió con la tendencia de uso intensivo del ciberespacio en las campañas, sobre todo con el caso de las elecciones estadounidenses como referente, ya que al igual que las elecciones federales estadounidenses de 2016, el uso de datos, información y servicios del ciberespacio (como la publicidad de redes sociales) fue un elemento clave, aunque poco trasparente.

Las elecciones presidenciales mexicanas de 2018 marcaron un hito dentro de la historia política nacional, ya que no sólo se caracterizaron por

ser el proceso electoral más grande de la historia moderna de México, sino también por realizarse en un contexto de hartazgo político y rechazo a lo que el votante consideraba como "el sistema", un elemento presente en otros procesos electorales como en las elecciones presidenciales de Estados Unidos en 2016. Además, a diferencia de 2012, el mercado digital y el ciberespacio presentaban opciones novedosas como la etno y la psico segmentación, ofrecidas por empresas, nacionales e internacionales, dedicadas a la recopilación y análisis masivo de datos, más allá de una estrategia de mailing (2006) o el uso masivo de redes sociales (2012). (Laurant, 2018).

El rasgo característico de estas elecciones, en comparación a las de 2012, es que la implementación de noticias falsas en las campañas electorales fue más ampliamente usada que los bots, sobre todo los bots digitales, así como el aumento de comunidades, discusiones y comunicación orgánica. En esta tónica, de acuerdo con el reportero español Fernando Peinado: "Los partidos han descubierto tácticas más efectivas como la generación de noticias falsas y publirreportajes en portales supuestamente informativos que se venden al mejor postor". No extraña esta deriva, ya que las noticias falsas se expanden "significativamente más lejos, más rápido, más profunda y ampliamente" que las verdaderas. (Peinado, 2018).

Para 2018, la penetración de internet en México ascendió a 82.7 millones de usuarios, casi el doble de internautas que en 2012 y cuatro veces más que en 2006. De este número de internautas, la mayoría (el 40%) está conformado por individuos de una edad entre 18 y 34 años. El nivel socioeconómico mayoritariamente expresado es el medio bajo (36%), seguido del medio alto (32%). El tiempo promedio de conexión ascendió a 8 horas y 12 minutos; aunque de acuerdo con el 64% de los internautas, se percibió que la conexión a internet constaba de 24 horas del día. El dispositivo favorito de conexión fueron los smartphones con un 89% de preferencia y el acceso a redes sociales se posicionó en el primer lugar de las actividades online de los usuarios (89%), seguido de enviar y recibir mails (84%) y participar en chats (83%). (Asociación de Internet, 2018).

En este momento el acceso a redes sociales estaba dominado por Facebook (98%), Whatsapp (91%) y Youtube (82%). Estos datos son de vital importancia, ya que las opciones que brindan las redes sociales a los diferentes actores dentro del proceso electoral permiten un nivel de penetración más intensivo y profundo en los votantes, lo que puede afectar el proceso democrático y la libertad de elección.

El proceso electoral presidencial de 2018 se dio entre el candidato de la coalición Juntos Haremos Historia (Morena, PT y PES), Andrés Manuel López Obrador; Ricardo Anaya, candidato de la coalición Por México al Frente (PAN, MC y PRD); el candidato de la coalición Todos por México (PRI, PVEM y Nueva Alianza) José Antonio Meade; y los candidatos independientes, Jaime Rodríguez Calderón, mejor conocido como "El Bronco" y Margarita Zavala, esposa del expresidente Felipe Calderón, aunque esta última se retiró de la contienda después de haberse realizado el primer debate presidencial.

Un elemento de continuidad lo representó el candidato de MORENA, Andrés Manuel López Obrador, el cual se presentó por tercera vez consecutiva en las elecciones, lo que le permitió tener una sólida base de apoyo y campaña acumulada, aunque también esto representó la reactivación de estrategias y un discurso ya existente, dentro y fuera del ciberespacio y que, de acuerdo a la visión de la oposición, había sido fundamental para cooptar el ascenso a la presidencia de AMLO los dos sexenios anteriores.

La presencia de los medios de comunicación tradicionales se mostró costosa y, si sólo nos guiamos por el resultado electoral, podríamos decir que poco efectiva, ya que de acuerdo a las cifras del Instituto Nacional Electoral (INE), la coalición Juntos Haremos Historia, que resultó vencedora, recibió casi la mitad de tiempo en spots publicitarios (4,591,836) frente a los 9,003,234 de la coalición Todos por México y los 8,673,468 de la coalición del candidato panista, Ricardo Anaya. (Ávila, 2018).

En lo que respecta al ciberespacio, la contienda presidencial de 2018 se distinguió por una serie de irregularidades en los afiliados a los partidos, un fenómeno recurrente en el mal manejo de bases de datos de las

instituciones; la presencia constante de noticias falsas en redes sociales y apps de mensajería instantánea, alimentadas y diseminadas por bots (orgánicos y digitales); la participación de empresas de servicios políticos novedosos; y, al igual que en las elecciones de 2006 y 2012, una constante opacidad en la determinación de gastos publicitarios en internet, sobre todo debido a la flexibilidad y versatilidad de creación y distribución de contenido en la red y a la dificultad de auditar.

Durante el proceso de campaña los candidatos habían realizado inversiones considerables en publicidad en medios digitales. Al sumar 141.9 millones de pesos, Meade se situó en el primer lugar con un gasto de 65.6 millones de pesos), seguido de Anaya, 63.8 millones, 'El Bronco', 5.5 millones de pesos y Margarita Zavala, con 7 millones en redes sociales, antes de abandonar la contienda. (Rodríguez, 2018). El único contendiente que afirmó no haber realizado ningún gasto en redes sociales fue AMLO.

Este dato resulta complejo si se tiene en cuenta que, de acuerdo con los datos del INE, hasta el 25 de mayo los candidatos presidenciales habrían pagado por difundir 575 "anuncios" en páginas de internet y redes sociales: 292 de Ricardo Anaya, 171 de José Antonio Meade, 73 de López Obrador, 22 de Margarita Zavala y 17 de Jaime Rodríguez Calderón. (Nicolai, Aldo. et. al. 2018).

La explicación ante tales irregularidades corre en dos vías: una general y la otra de estrategia de campaña de la coalición Juntos Haremos Historia. La primera es la complejidad de fiscalización que brinda el ciberespacio, no sólo en los actores sino en las actividades, ya que un contrato de una empresa de publicidad política bien podría denominar actividades de análisis masivo de datos, segmentación y personalización como publicidad política. Lo anterior genera estimaciones tales como de cada peso declarado por los partidos políticos en gasto de campaña, en realidad el gasto asciende a 15 o más. (Nicolai, Aldo. et. al. 2018). Además de esto, es necesario considerar que la contratación de servicios de internet se da por terceros y no por contratación directa, tal como lo dejó

en claro Google ante el proceso electoral. [4] Por esta razón, tampoco se encontró a Twitter ni Facebook en el Registro Nacional de Proveedores.

La segunda explicación viene de la estrategia que adoptó la coalición liderada por AMLO y coordinada digitalmente por la actual senadora de Morena, Tatiana Clouthier. Dicha estrategia se valió de la flexibilidad, espontaneidad y difusión de las redes para crear contenidos simples (memes, comentarios) y complejos (manuales, infografías), todo esto bajo la coordinación de la cuenta "Abre más los ojos". (Esteinou, 2019). En dicha campaña no sólo fueron los jóvenes los que llevaron las riendas del proyecto, sino que también miembros y partidarios importantes de Morena contribuyeron a la discusión y difusión digital, como en el caso de la propia Tatiana, John M. Ackerman y Epigemio Ibarra, lo que implicó la formación de redes orgánicas de comunicación.

Pese a esto, una investigación realizada por el periódico Reforma reveló que Andrés Manuel López Obrador registró en Twitter la mayor cantidad de 'bots' (cuentas fantasmas o fraudulentas) con un millón 467 mil 500 cuentas falsas (Recillas, 2018), lo que equivale a un 67.6% de bots, seguido de Meade Kuribreña con 59.8%; Anaya Cortés, 49% y Rodríguez Calderón, con 45.8%. (Aristegui Noticias, 2018).

Al igual que en 2006 y 2012, en las elecciones de 2018 el PRI y el PAN optaron por una estrategia basada en un discurso de descalificación y ataques personales, principalmente dirigidos a AMLO, lo que a todas luces ayudó a que la cuenta "Abre más los ojos" recibiera un total de 98 millones de impactos sólo en Facebook (Navarro, 2019), con el fin de servir como contrapeso a la campaña sucia contra AMLO. Un resultado claro de esta apuesta es lo que menciona la investigadora Carmen Fernández: "La clase política mexicana le apostó al miedo a AMLO como

4 Google no puede establecer relaciones contractuales con partidos políticos ni entidades que tengan alguna obligación legal según lo estipulado en la normativa de auditorías del Instituto Nacional Electoral de México. Tampoco puede aceptar pagos de dichos partidos ni entidades. Si tu entidad debe cumplir con alguna obligación conforme a dicha normativa, debes usar un intermediario para realizar las compras (por ejemplo, una agencia publicitaria). (Blanco, 2018).

mensaje único, pero en un entorno de tal desprestigio del sistema, el mayor miedo del electorado era a la continuidad" (Fernández, 2018).

Así como en las elecciones presidenciales estadounidenses en 2016 y en el referéndum del Brexit, en México algunos partidos intentaron hacer uso de la tecnología de punta y servicios especializados en campaña y comunicación política, lo que orilló al PRI y el PAN acercarse a gente clave en Cambridge Analytica, empresa especializada en el análisis de datos y estrategia política. Aunque las negociaciones entre los partidos nacionales con Cambridge Analytica comenzaron desde 2017, la información no saldría a la luz hasta abril de 2018, tras conocerse el incidente de la empresa y el uso indiscriminado y no consensuado de bases de datos de usuarios en Facebook; con el fin de generar contenido a la medida e impactar los resultados electorales, tal como lo presumían en el Brexit y en las elecciones presidenciales estadounidenses de 2016. (Asad y Hakim, 2018).

La noticia resultó estremecedora para algunos investigadores, académicos y público en general, no sólo por la violación a la privacidad, sino por las capacidades que estaban desarrollándose y que podían cambiar radicalmente la forma en la que unas elecciones tuvieran lugar; sin embargo, y tras un breve análisis de la oferta nacional, se puede concluir que esta clase de servicios ya está desarrollándose y operando dentro del mercado nacional, aunque constreñidos bajo el marco legal nacional en materia de protección de datos personales.[5]

En México existen pocas empresas dedicadas al análisis de datos para partidos políticos, a diferencia de los servicios de comunicación y publicidad política. Las principales empresas mexicanas del sector ofrecen servicios de análisis histórico de datos electorales (tendencias de voto) y de datos estadísticos poblacionales (datos socioeconómicos, educativos y de carácter político), ambos con el fin de hacer un perfilamiento cruzado entre características sociales y decisiones electorales. (Laurant, 2018).

5 Estas son: la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) y la Ley Federal de Protección de Datos Personales en Posesión de Particulares (LFPDPPP)

Algunas de estas empresas también crean noticias y usuarios falsos para apoyar a un candidato; miden y rastrean la movilidad y la interacción de personas en eventos políticos (para conocer el comportamiento social y realizar eventos más efectivos); y analizan variables socioeconómicas con el fin de tener una idea a nivel regional de qué características comparten los votantes y cómo captar sus necesidades. Dentro de las primeras empresas figuran Descifra (fusionada con Telus, otra empresa de análisis de datos), Klustera, y entre las segundas, Victory Lab (la cual, de acuerdo a su presidente, Carlos Merlo, se especializa en bots y noticias falsas); ésta tuvo su aparición en la escena electoral desde 2012. (Chávez, 2017).

Pese a que en este proceso electoral no se suscitó un movimiento como YoSoy132, la iniciativa VerificadoMx fungió como un contrapeso ciudadano al uso indiscriminado de las redes sociales y de internet por parte de partidos políticos y servicios adyacentes. Dicha iniciativa surgió con el fin de desmentir información y noticias falsas, además de que coadyuvó la participación de la iniciativa privada, medios de comunicación internacionales y a la ciudadanía organizada.

Pese a las estrategias, dinero, actividades y material invertido, los resultados electorales de 2018, no sólo presidenciales, le dieron una apabullante victoria a AMLO y a su partido. Si el análisis partiera únicamente de la inversión e impacto tecnológico, no se podrían interpretar los resultados correctamente, ya que en este proceso la cultura política, el descontento social, la corrupción y diversos indicadores económicos fungieron un papel primordial que impactaría en los resultados finales más allá del peso de la tecnología.

El caso de las elecciones presidenciales de 2018 es muestra clara de las limitaciones en la influencia del ciberespacio en la política. Dichas limitantes están asociadas a factores legales e institucionales (las leyes de protección de datos personales), sociales, económicos y sobre todo, a las características políticas estructurales que inciden en la capacidad de influencia del ciberespacio entre los usuarios y votantes.

Aunque esto no resta evidencia a algo que podría considerarse como una "nueva normalidad", en la cual las noticias falsas, el uso constante de datos personales y una serie de actores e intermediarios del ciberespacio

(orgánicos o digitales) son parte inherente del ciberespacio, así como la vida y cultura política de la sociedad y que pueden incidir en corto, mediano o largo plazo en la política y las instituciones nacionales.

Conclusión

El ciberespacio genera sinergias novedosas en la vida de las personas gracias a la inmediatez, anonimia y otros elementos, los cuales han impactado en diversas áreas, una de ellas las fuentes, ejercicio y capacidad de poder en la sociedad, lo que obliga a reevaluar a las ciencias existentes y el análisis de la realidad.

Lo anterior es muy importante, ya que esta tendencia influida por el ciberespacio está en constante expansión y consolidación, lo que aumentará su simbiosis dentro de la sociedad. La progresión del uso de mail a la creación de publicidad segmentada e híper-segmentada son una muestra de este camino, el cual tiene a la Inteligencia Artificial como objetivo y herramienta central.

Por esto es que el estudio del ciberespacio en su papel e influencia social es necesario, sobre todo si éste puede hacer peligrar a las instituciones y tradiciones democráticas, lo que inevitablemente también está ligado a la propia estructura y seguridad nacional y hasta internacional. La relación mutua entre política y el ciberespacio es más clara a la hora de analizar las elecciones, ya que en ellas es posible rastrear fenómenos políticos como la generación de grupos y comunidades políticas; los controles y accesos permitidos en el ciberespacio implementados por el gobierno, las discusiones políticas y sus vicios característicos –como el uso de noticias falsas o bots-, entre otros, propios del espacio-temporalidad en donde exista el ciberespacio.

También es posible analizar la relación del ciberespacio en la política, sobre todo en la transformación de métodos, estrategias y prácticas como la creación de bases de datos de votantes (pormenorizadas y segmentadas a partir de rasgos no sólo socioeconómicos, sino psicológicos y conductuales); el espionaje a otros candidatos. Los peligros asociados a la manipulación política por medio de publicidad, mensajes y material

personalizado (alimentado no sólo de las demandas sociales, sino de los miedos, aspiraciones y otros elementos psicológicos), son algunos de los ejemplos que muestran una lógica vigilancia de mercado adecuada a la política.

México es muestra de cómo la utilización del ciberespacio puede tener un impacto negativo en los actores y procesos políticos, a la vez de que también es muestra de la adaptación tecnológica en una cultura política particular. El análisis de las elecciones mexicanas puede dar cuenta de la importancia de la cultura política sobre el ciberespacio y la configuración de opciones disponibles, así como también de indicadores culturales y socioeconómicos. Además, en éste se puede notar la progresión y madurez del ciberespacio a través del tiempo y los riesgos asociados que pueden significar un retroceso sustancial en la cultura y sistema político de los Estados.

No sólo los gobiernos, partidos políticos y otros actores poderosos han hecho uso de los beneficios del ciberespacio para sus propios fines, sino que la ciudadanía, así como ciertos actores e iniciativas privadas, dan muestra del potencial de resistencia que puede tener el ciberespacio para la ciudadanía y la democracia en general. Ejercicios ciudadanos como el movimiento YoSoy132 y VerificadoMx deberían de fomentarse día a día, ya que tras el final de las elecciones, las estrategias políticas usualmente llegan para quedarse, como el caso de los bots, las noticias falsas y el uso masivo de datos personales.

Es importante tener en cuenta y alimentar la discusión acerca de la relación entre la política, la sociedad y el ciberespacio, ya que esta discusión no sólo es pertinente, sino necesaria en un futuro que presenta a la Inteligencia Artificial como un objetivo, el cual en sí mismo plantea más dudas y miedos que respuestas, ya que es necesario solucionar cuestiones estructurales tales como la construcción y uso del ciberespacio para poder cimentar el diálogo entre un ciberespacio orientado a la Inteligencia Artificial, el ejercicio y los conflictos de poder, además de la regulación de la vida en sociedad como entes políticos y afectados por la política.

Además del diálogo y crítica constante, es necesario el replanteamiento y fortalecimiento de valores e instituciones democráticas para evitar que las libertades y beneficios del ciberespacio y la tecnología en general

socaven los valores fundamentales de Occidente. El análisis realista del ciberespacio es útil a la hora de generar críticas hacia el discurso idealista que gira en torno al ciberespacio como el sinónimo de una sociedad con mayor libertad de expresión y fortalecimiento de la democracia, ya que esta noción puede oscurecer el papel y los peligros del ciberespacio en procesos institucionales vitales para la democracia, el Estado y las relaciones internacionales.

Fuentes consultadas

a) Bibliografía y hemerografía

Auvinen, Ari Matti. (2013), *Social media - The new power of political influence. Version 1.0*. Centre for European Studies. https://www.martenscentre.eu/sites/default/files/publication-files/social-media-and-politics-power-political-influence.pdf

Asad, Ahmed y Perloth, Nicole (2017), 'Somos los nuevos enemigos del Estado': el espionaje a activistas y periodistas en México'. *The New York Times* (19 junio). https://www.nytimes.com/es/2017/06/19/mexico-pegasus-nso-group-espionaje/

Asad, Ahmed y Hakim, Danny (2018), "Los recursos del PRI en las presidenciales: de Cambridge Analytica a la politización de la justicia". *The New York Times*, (24 junio): https://www.nytimes.com/es/2018/06/24/pri-mexico-elecciones-pgr-trife/

Ángel, Arturo (2015), "México, el principal cliente de una empresa que vende software para espiar". *Animal Político* (7 julio). https://www.animalpolitico.com/2015/07/empresa-de-hackers-exhibida-por-venta-de-software-espia-a-paises-represores-y-mexico-resulta-su-principal-cliente/

Ávila, Yuriria (2018). "Así asigna el INE el número de spots a los que cada partido y candidato tienen derecho", *Animal Político*. https://www.animalpolitico.com/2018/04/asi-asigna-el-ine-el-numero-de-spots-a-los-que-cada-partido-y-candidato-tienen-derecho/

Barnett, Michael y Duvall, Raymond (2005), "Power in International Politic". *International Organization*, Vol. 59, No. 1 (Winter), 39-75.

Blanco, Ricardo (2018). "La publicidad digital wink ;) wink ;) wink ;)...". *Forbes México*. https://www.forbes.com.mx/publicidad-digital-wink-wink/

Beckhusen, Robert (2013). "U.S. Looks to Re-Up Its Mexican Surveillance System." *Revista Wired*. (5 enero). https://www.wired.com/2013/05/mexico-surveillance-system/

Camarena, Salvador (2019), "Cisen, Pegasus y un peligroso fetichismo". *El Financiero*. https://www.elfinanciero.com.mx/opinion/salvador-camarena/cisen-pegasus-y-un-peligroso-fetichismo

Chávez Gabriela, (2017). "Las mentiras políticas son un negocio". *Expansión*. https://expansion.mx/tecnologia/2017/11/03/las-mentiraspoliticas-son-un-negocio.

Chester, Jeff y Rosenfeld, Steven (2019), "Enough Already! Protect Yourself from Online Political Manipulation and False News in Election 2018. (Reporte)". Centro para la Democracia Digital.

Fuchs, Christian, Boersma, Kees, Albrechtslund, Anders y Sandoval, Marisol (2012), "Internet and Surveillance The Challenges of Web 2.0 and Social Media". Londres: Routledge.

De Mauleón, Héctor, (2012). "YoSoy132 y el uso político de las redes sociales", Revista Nexos, n. 417. https://www.nexos.com.mx/?p=14967.

Deibert Ronald J, (2013). *Black Code, Inside the Battle for Cyberspace*. Toronto: McClelland & Stewart.

Esteinou, Javier (2019). "Las 'benditas redes sociales' y la victoria de AMLO/Morena". *Siempre*. http://www.siempre.mx/2019/04/las-benditas-redes-sociales-y-la-victoria-de-amlo-morena/

Fernández, Carmen Beatriz (2018), "Ciberpolítica 2018: Tendencias en Latinoamérica", en "Las campañas políticas electorales en América Latina". Konrad-Adenauer-Stiftung. https://dialogopolitico.org/wp-con-

tent/uploads/2018/11/Campa%C3%B1as-electorales-en-Am%C3%A9rica-Latina_WEB.pdf

Flores, Pepe (2015), "FinFisher en México: Sonríe, te siguen espiando", *Digital Rights LAC* (Junio) https://www.digitalrightslac.net/es/finfisher-en-mexico-sonrie-te-siguen-espiando/

Hughes, Thomas (1983), "Networks of Power Electrification in Western Society, 1880-1930". Baltimore: The Johns Hopkins Unibersity Press.

Islas, Octavio y Pimienta, Xóchitl (2016). "El empleo de redes sociales en las campañas presidenciales en México, 2012". *Cuadernos Artesanos de Comunicación/100*, https://dialnet.unirioja.es/servlet/libro?codigo=581633.

Islas, Octavio (2018). "De bots, trolls y elecciones". *El Universal*. https://www.eluniversal.com.mx/columna/octavio-islas/techbit/de-bots-trolls-y-elecciones

Jurado, Karen (2020), "Destituyen a coordinadora de la GN por presunta corrupción". *Periodismo Hoy* (29 febrero). http://periodismohoy.com/destituyen-coordinadora-guardia-nacional/

Klimburg, Alexander y Faesen, Louk (2018). *A balance of power in cyberspace*. The Hague Center for Strategic Studies.

Laurant, Cedric (2018), *Datos personales e influencia política: Investigación sobre las estrategias digitales del Partido Revolucionario Institucional en 4 de sus campañas electorales recientes en México*. México: SonTusDatos, Artículo 12, A.C. https://sontusdatos.org/2018/06/29/partidos_politicos_datos_influenciar_voto/

Lawrence, Lessig, (2006). *Code*. New York: Basic Books.

Linaloe Flores, R. (2018), "Los expedientes secretos de Enrique Peña Nieto". *Vice.com* (27 Noviembre) https://www.vice.com/es_latam/article/439a8n/los-expedientes-secretos-de-enrique-pena-nieto

Meneses Rocha, María Elena y Bañuelos Capistrán, Jacob (2009), *Internet y campañas electorales en México. La oportunidad postergada*. Toluca: IEEM / Breviarios de Cultura Política.

Martínez, Pario (2012), "No se aceptará la imposición de Peña Nieto: #YoSoy132". *Animal Político*. https://www.animalpolitico.com/2012/07/no-se-aceptara-la-imposicion-de-pena-nieto-yosoy132/

Morozov, Evgeny (2011). *The Net Delusion: The Dark Side of Internet Freedom*. Nueva York: Public Affairs

Navarro, María Fernanda (2019), "Ellos son los creativos que dieron un vuelco a la campaña de AMLO", *Forbes México*. https://www.forbes.com.mx/ellos-son-los-creativos-que-dieron-un-vuelco-a-la-campana-de-amlo/

Nicolai, Aldo, et. al. (2018), "Verificado.mx: Candidatos gastan más de 106 mdp en propaganda en internet, pero no declaran todos los anuncios". *Animal Político*. https://www.animalpolitico.com/2018/06/verificado-candidatos-anuncios-internet/

Norris, Pippa (2002). *La participación ciudadana: México desde una perspectiva comparativa*. Harvard University / IFE.

Nye, Joseph S. (2010). *Cyber Power*. Harvard Kennedy School, Belfer Center for Science and International Affairs.

Ojeda de la Torre, Ivonne (2019), "Se espió con Pegasus en México en 2019; el Gobierno de AMLO debe explicar, exigen organizaciones". *SinEmbargo* (octubre 29). https://www.sinembargo.mx/29-10-2019/3669914

Parker, Asmann (2017), "Mexico Authorities Misusing Surveillance Tech to Spy on Political Opponents: Reports Brief". *Insight Crime* (junio 19) https://www.insightcrime.org/news/brief/mexican-authorities-misusing-surveillance-technology-spy-political-opponents/

Peinado, Fernando (2018). "Las redes rotas de la campaña electoral en México". *El País.* https://elpais.com/internacional/2018/03/21/actualidad/1521628738_165398.html.

Rebolledo, Ruy Alonso (2017), "Los 5 casos de espionaje del gobierno mexicano". *El Economista* (20 junio) https://www.eleconomista.com.mx/politica/Los-5-casos-de-espionaje-del-gobierno-mexicano-20170620-0101.html

Recillas, Angélica (2018). La acción y reacción de los bots de Morena", *Etcétera*. https://www.etcetera.com.mx/opinion/accion-reaccion-bots-trolls-morena/

Red en Defensa de los Derechos Digitales (R3D) (2016), "El estado de la Vigilancia: Fuera de control". https://r3d.mx/wp-content/uploads/R3D-edovigilancia2016.pdf

Riquelme, Rodrigo (2019), "Pegasus reaparece durante el gobierno de AMLO". *El Economista*. (29 octubre), https://www.eleconomista.com.mx/tecnologia/Pegasus-reaparece-durante-el-gobierno-de-AMLO-20191029-0084.html

Robertson, Jordan, et. al. (2016), "¿Cómo hackear una elección?". *Bloomberg Businessweek.* https://www.bloomberg.com/features/2016-comomanipular-una-eleccion/.

Rodríguez, Adriana (2018), "AMLO, el rey de las redes sociales durante el proceso electoral 2018", *Economía Hoy*. https://www.economiahoy.mx/elecciones-mexico-2018/noticias/9231206/06/18/AMLO-el-rey-de-las-redes-sociales-durante-el-proceso-electoral-2018.html

Ronfeldt, David (1991). *Cyberocracy, Cyberspace and Cyberology: Political effects of the Information Revolution.* Los Angeles: RAND.

Sánchez Onofre, Julio (2017), "Sospechan mayor espionaje del gobierno mexicano". *El Economista*, (13 febrero). https://www.eleconomista.com.mx/politica/Sospechan-mayor-espionaje-del-gobierno-mexicano-20170213-0039.html

Schwartz, Maathatias (2017). "Cyberwar for Sale". *The New York Times Magazine*. https://www.nytimes.com/2017/01/04/magazine/cyberwar-for-sale.html?smid=tw-share&_r=1&ref=nyt-es&mcid=nyt-es&subid=article

Scott-Railton, John, Marczak, Bill, Abdul Razzak, Bahr, Crete-Nishihata, Masashi y Diebert, Ron (2017), "Reckless Exploit Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware". *CitizenLab*, (19 junio), https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/

Stevens, Tim (2017). *Cyberweapons: power and the governance of the invisible*. International Politics, (october), DOI:10.1057/s41311-017-0088-y

Tirado, Erubiel (2018). "El Cisen: Inteligencia de Estado... que no fue". *Proceso* (30 julio) https://www.proceso.com.mx/544943/el-cisen-inteligencia-de-estado-que-no-fue

Torres Soriano, Manuel (2013). "Internet as a Driver of Political Change: Cyber- Pessimist and Cyber-Optimists". *Revista del Instituto Español de Estudios Estratégicos*. Núm. 1. http://www.ugr.es/~gesi/internet-political-change.pdf

Villaseñor, Yara (2017), "Antes de Pegasus existió Galileo: todo será confidencial hasta el 2027". *La Izquierda Diario*, (28 junio) http://www.laizquierdadiario.mx/Antes-de-Pegasus-existio-Galileo-todo-sera-confidencial-hasta-el-2027

Vaishnav, Chintan, Choucri, Nazli y Clark, David (2013), Cyber international relations as an integrated system. *Environment Systems and Decisions*, 33 (4): 561–576. https://dspace.mit.edu/bitstream/handle/1721.1/103775/10669_2013_9480_ReferencePDF.pdf?sequence=1&isAllowed=y

b) Cibergrafía periodística

ADN Político (2012), "¿Quieres amigos políticos? Da 'like' a Pribook o FaceMorena". (6 octubre). http://static.adnpolitico.com/2012/2012/10/03/quieres-amigos-politicos-dale-like-a-pribook-o-facemorena

Animal Político (2018), "¿Cambridge Analytica en México? AMLO y Anaya piden investigar presunta intervención en electores" (21 marzo) https://www.animalpolitico.com/2018/03/cambridge-analytica-mexico-amlo-anaya/

Animal Político (2013), "¿Cuánto costaron las elecciones de 2012?", (8 febrero). https://www.animalpolitico.com/2013/02/cuanto-costaron-las-elecciones-de-2012/

Animal Político, (2011), "PRI y PAN, los partidos con más presencia en redes sociales: AMIPCI", (20 septiembre). https://www.animalpolitico.com/2011/09/pri-y-pan-los-partidos-con-mayor-presencia-en-la-redes-sociales-amipci/

Aristegui Noticias (2019), "No estamos metidos en eso", dice AMLO ante cuestionamientos sobre Pegasus. (6 noviembre), https://aristeguinoticias.com/0611/mexico/no-estamos-metidos-en-eso-dice-amlo-ante-cuestionamientos-sobre-pegasus-enterate/

Aristegui Noticias, (2018), "Los bots y su influencia en la elección presidencial mexicana: Albert-László Barabási", (20 junio). https://aristeguinoticias.com/2006/mexico/los-bots-y-su-influencia-en-la-eleccion-presidencial-mexicana-albert-laszlo-barabasi/

Aristegui Noticias (2012), "The Guardian revela unidad secreta de Televisa para la campaña de EPN". (26 junio). https://aristeguinoticias.com/2606/lomasdestacado/theguardian-revela-unidad-secreta-de-televisa-para-la-campana-de-epn/

Asociación de Internet. (2018), "Estudio sobre los hábitos de los usuarios de internet en México 2018", https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/14-Estudio-sobre-los-Habitos-de-los-usuarios-de-Internet-en-Mexico-2018/lang,es-es/?Itemid=

Asociación de Internet (2013), "Estudio sobre los hábitos de los usuarios de internet en México 2012", https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/Estudio-sobre-los-habitos-de-los-usuarios-de-internet-en-Mexico-2012/lang,es-es/?Itemid=

Asociación de Internet (2007), "Estudio sobre los hábitos de los usuarios de internet en México 2007", https://www.asociaciondeinternet.mx/es/component/remository/Habitos-de-Internet/Estudio-sobre-los-habitos-de-los-usuarios-de-internet-en-Mexico-2007/lang,es-es/?Itemid=

Association for Progressive Communications (APC), Humanist Institute for Cooperation with Developing Countries (HIVOS) y Global Information Society Watch (GISW) (2014), *Communications surveillance in the digital age.* https://www.giswatch.org/sites/default/files/gisw2014_communications_surveillance.pdf

El Economista (2019), "Desde Cantinflas y Frida Kahlo hasta John F. Kennedy, así espiaba el gobierno de México". (12 abril) https://www.

eleconomista.com.mx/politica/Desde-Cantinflas-y-Frida-Kahlo-hasta-John-F.-Kennedy-asi-espiaba-el-gobierno-de-Mexico-20190412-0024.html

Excélsior (2018), "Con el fin del Cisen, se acabará el espionaje telefónico: López Obrador". (14 septiembre), https://www.excelsior.com.mx/nacional/con-el-fin-del-cisen-se-acabara-el-espionaje-telefonico-lopez-obrador/1252335

Expansión (2018), "La sombra del Cisen se mete a la contienda de las #Elecciones2018". (febrero), https://politica.expansion.mx/politica/2018/02/13/la-sombra-del-cisen-se-mete-a-la-contienda-de-las-elecciones2018

El Sol de México (2019) "En México no hay regulación del espionaje: especialistas". (mayo), https://www.elsoldemexico.com.mx/mexico/justicia/en-mexico-no-hay-regulacion-del-espionaje-especialistas-3644842.html

El Universal (2006), "Felipe Calderón, el candidato que más spots transmitió el fin de semana", (23 enero), http://archivo.eluniversal.com.mx/nacion/134371.html

INFOBAE (2019), "Caso Pegasus: Hacienda perdonó a la empresa que vendió el equipo de espionaje; también vigilaron a la viuda de Javier Valdéz". (20 marzo), https://www.infobae.com/america/mexico/2019/03/20/caso-pegasus-hacienda-perdono-a-la-empresa-que-vendio-el-equipo-de-espionaje-tambien-vigilaron-a-la-viuda-de-javier-valdez/

HispanTv (2016),"Informe: México pagó $15 millones a una empresa de ciberespionaje". (4 septiembre) https://www.hispantv.com/noticias/mexico/286935/mexico-paga-espionaje-millones-nso-group

HispanTv (2018), "Hallan en México edificio oficial con equipo de espionaje". (10 diciembre), https://www.hispantv.com/noticias/mexico/395683/espionaje-edificio-estatal-pena-nieto

RT (2019), "México espió para la CIA a diplomáticos y ciudadanos de Rusia, China y otros países", (20 agosto), https://actualidad.rt.com/actualidad/324539-mexico-espionaje-cia-china-rusia

SonTusDatos (2014), "El caso 'FinFisher': una historia de espionaje en México, (9 septiembre) https://sontusdatos.org/2014/09/09/el_caso_finfisher_historia_de_espionaje_en_mexico/

Verificado MX (2018), "Qué es Verificado". https://verificado.mx/que-es-verificado-2018/