El hackeo de la democracia en tiempos electorales

The hacking of democracy in electoral times

Aristeo García González (México)*

Las nuevas tecnologías son una arma de doble filo:
aumentan nuestras capacidades y nuestro poder,
pero también hacen a sus usuarios más vulnerables
a la vigilancia y la manipulación.
Reg Whitaker

Fecha de recepción: 17 de agosto de 2020.
Fecha de aceptación: 18 de diciembre de 2020.

Resumen

La transformación tecnológica en la sociedad actual ha alcanzado un nivel máximo histórico en cuanto a la disponibilidad de la información y la libertad de expresión; no obstante, ello implica una amenaza para la democracia debido a la existencia de organizaciones cibercriminales capaces de manipular el universo digital de manera silenciosa. Los ataques a la privacidad, la recopilación de la información personal y perfilada de individuos, la implementación de granjas de producción de noticias falsas o, incluso, el hackeo de resultados y el boicot electoral son prueba de lo anterior. De ahí proviene la importancia de adentrarse en su estudio.

* Maestro en Derechos Fundamentales y especialista en protección de datos personales y privacidad. Titular de la Unidad de Transparencia del Poder Judicial de Michoacán. argago78@gmail.com.

PALABRAS CLAVE: privacidad, democracia, hackeo, libertad de expresión, decisiones, tecnología.

ABSTRACT

The technological transformation in today's society has reached historical maximum levels in terms of the availability of information and freedom of expression. What a threat to democracy means from cybercriminal organizations capable of silently manipulating the digital universe: attacks on privacy, collection of personal and profiled information from individuals, fake news production farms, or even hacking of results and electoral boycott are proof of this. Hence the importance of entering his study.

KEYWORDS: privacy, democracy, hacking, freedom of expression, decisions, technology.

Introducción

Entender qué piensa cada votante y poder enviarle un mensaje personalizado —por ejemplo, lo que un partido puede ofrecerle— es un sueño que ha comenzado a convertirse en realidad, sobre todo para quienes conocen el alcance y la importancia del uso de los datos que circulan en el internet y las redes sociales.

Lo anterior constituye una nueva guerra política, cuya arma principal es el uso de los mecanismos digitales —es decir, el internet y las redes sociales—, lo cual ha beneficiado a los innovadores y a los nuevos protagonistas en muchos campos, como el político. No obstante, por desgracia, entre los actores se encuentran delincuentes, terroristas, piratas informáticos, traficantes, falsificadores y ciberdelincuentes (Naím 2005, 80); incluso hay expertos contratados, mejor conocidos como los numerati.[1]

Actualmente, los datos obtenidos en el entorno digital son la nueva herramienta; su conocimiento da poder y, por medio de su análisis, se puede llegar a obtener información útil para la toma de decisiones, como en el caso de la política.

El ejemplo más claro es el de Cambridge Analytica, la empresa que contribuyó a la victoria electoral de Donald Trump, al minar la información personal de millones de usuarios de las redes sociales. De ahí que pueda afirmarse que el monopolio de los datos está en manos de unas cuantas empresas o de actores que, a medida que reúnen información, acumulan poder, lo cual, sin duda, aporta al hackeo de la democracia.

En virtud de lo anterior surgió la idea del presente documento. El punto de partida es constituido por las siguientes interrogantes: ¿la tecnología puede contribuir en la toma de decisiones de los votantes?, ¿puede un político ser favorecido en un proceso electoral por el simple hecho de contar con la información personal de los ciudadanos?

---

[1] Se trata de una comunidad integrada por físicos, ingenieros computacionales, psicólogos, economistas, geógrafos y diseñadores, entre otros (Baker 2009).

En principio, la respuesta a ambas interrogantes es "sí". Pero ¿cómo lograrlo sin el consentimiento de los votantes? Dicho planteamiento es justamente lo que se analiza a lo largo de los cinco apartados del presente trabajo.

Para ello, se revisa la nueva forma de hacer política y las diversas relaciones e interacciones suscitadas en el entorno digital. Posteriormente, se hace un análisis acerca de la importancia de la protección de los datos personales en el internet y las redes sociales, a fin de entender cómo puede secuestrarse la democracia mediante el uso de diversos dispositivos tecnológicos. Finalmente, se concluye con algunas reflexiones.

La democracia en tiempos tecnológicos

Uno de los pilares fundamentales, al hablar de movimientos políticos innovadores y cambios en las democracias, es la posibilidad que brindan las herramientas digitales.

Con la desregulación y la comercialización de los sistemas mundiales de radio y televisión, por una parte, y de las telecomunicaciones, por otra parte, los estados han perdido paulatinamente su capacidad de supervisar y controlar las comunicaciones en sus fronteras. Así, los gigantes informativos están erigiendo una red mundial de telecomunicaciones que soslaya a aquellos, cambiando, a la vez, la naturaleza de la política (Rifkin 2013, 209).

En tan solo dos décadas, el internet y las tecnologías digitales se han instalado en el quehacer cotidiano de gran parte de la humanidad y, en torno a estos, se reorganiza un sinfín de ámbitos de la sociedad; su rápida expansión no da oportunidad para apreciar plenamente sus implicaciones en los diversos planos, que van desde la organización de la economía hasta el poder político, pasando por los derechos humanos, el desarrollo cultural y las estructuras sociales.

Si bien el internet fue concebido originalmente como un espacio abierto, descentralizado y no comercial, ha contribuido a democratizar las comunicaciones, puesto que, en los últimos años de comercialización, se ha

producido una concentración y centralización inauditas. Por un lado, está la concentración tecnológica, como sucede, por ejemplo, con los grandes cables internacionales de fibra óptica[2] que interconectan países (Burch 2014, 3).

También se encuentra la concentración de contenidos y datos personales generados en las redes sociales, alojados en los servidores que ofrecen almacenamiento en la nube, que son utilizados por una nueva mafia matemática: los numerati, quienes trabajan sin tregua para empresas, gobiernos y partidos políticos, cuya meta consiste en analizar las actividades de las personas para conocer sus hábitos (Baker 2009, 25), lo cual les permite manipular las conductas, ocasionando una evaporación de la privacidad.

Ese fenómeno de concentración se debe a las características particulares de la economía en la red —denominada *network effect*— que conllevan a la conformación de monopolios, debido a que los usuarios prefieren un servicio más exitoso, en el que se encuentran más personas.

No cabe duda de que internet es dominado por una docena de megacorporaciones, con no más de 15 años de existencia y que van absorbiendo la competencia en el camino; su poder descomunal puede significar una reedición del neocolonialismo con sus secuelas de dominación cultural, extracción de riqueza e injerencia política.

Incluso, que ya no exista privacidad ni seguridad en las comunicaciones es bastante preocupante. Pero aún más peligroso es, justamente, el modo en que se reconfigura el poder y su concentración en manos de quienes controlan las tecnologías y los conocimientos, el cual les permite acumular mayor riqueza, tecnología más sofisticada y, por ende, más poder, en un círculo vicioso que se constituye como una amenaza para el futuro de la democracia.

---

[2] Estos cables han facilitado mucho la tarea de espionaje de la Agencia Nacional de Seguridad de Estados Unidos de América, la cual, con la intervención en apenas 190 centros de datos, puede monitorear casi todos los flujos del mundo de internet y telefonía, entre otras telecomunicaciones.

Respecto a la ciudadanía, no hace mucho la mayoría de las personas empleaba las tecnologías digitales sin preocuparse quién las gestionaba o las controlaba; sin embargo, con las últimas revelaciones comienza a despertarse la conciencia en relación con la importancia del tema, sobre todo con el creciente surgimiento de las granjas de bots u ordenadores zombi, que son los encargados de ampliar la difusión de noticias falsas (*fake news*), las cuales se propagan más rápido que la información verdadera, afectando a todos los ámbitos, especialmente el político (Salas 2018; Nyhan 2018).

Mientras la tecnología digital evoluciona a pasos agigantados, los marcos legales, los derechos y los mecanismos para garantizar su vigencia siguen el ritmo del mundo analógico.

Precisamente, en la medida que avanza el crecimiento del internet, puede que sea necesario que los gobiernos se preocupen cada vez más por las diversas relaciones e interacciones democráticas suscitadas en el entorno digital, en especial cuando represente un riesgo para la democracia de un país. Ello se analiza a continuación.

Relaciones e interacciones democráticas en el entorno digital

La llamada cuarta revolución industrial[3] (Caballero 2018; Schwab 2017) ha traído consigo cambios económicos, sociales y culturales, de proporciones tan grandes que, en ocasiones, resulta imposible prever sus consecuencias. Es el caso de la tecnología, que no solo ha transformado las comunicaciones, los modos de producción y las relaciones humanas, sino también el ejercicio de la democracia.

Así, la identidad digital cobra importancia, aunque se trata de un concepto muy amplio debido a los componentes que la han configurado a lo

[3] La industria 4.0, o cuarta revolución industrial, es el nombre que la comunidad de expertos ha dado al fenómeno de la digitalización en las principales cadenas de producción, fabricación y suministro por medio de la realidad virtual, la inteligencia artificial o el internet de las cosas.

largo del tiempo. A efectos del presente estudio, resulta relevante definirla como el "conjunto de rasgos que hace a una persona ser quien es y lo distingue de los otros, al mismo tiempo que le permite interactuar con su entorno" (Fundación Telefónica 2013, 3).

Lo anterior tiene como consecuencia un cambio suscitado en el acopio y el tratamiento de los datos, por lo que, mediante estos, ahora es posible producir una imagen pormenorizada de una persona en particular, haciéndola identificable a partir de diversa información, como el nombre completo, la fecha de nacimiento, el domicilio, el sexo, el estado civil y el grado de estudios, etcétera.

Como consecuencia de ello, no resulta extraño el estudio de asuntos relacionados con los derechos a la identidad, la libre información, la privacidad, la intimidad, el anonimato o la reputación en la red. Sin embargo, con la tecnología *blockchain*[4] (cadena de bloques) se puede tomar el control de la información y jamás se podrá perder, modificar o eliminar lo que convierte a los individuos en verdaderos dueños de sus datos e identidad digital.

De ahí que el tema esté en auge. Incluso la empresa transnacional International Business Machines (IBM), como parte de sus soluciones en *blockchain*, ha mencionado lo siguiente:

> Transformando la identidad digital en una identidad de confianza. Conozca cómo IBM Blockchain Trusted Identity™ está uniendo fuerzas con otros para construir la capa de entidad descentralizada perdida de Internet (IBM s. f.).

Tal parece que dicha entidad de confianza está basada en un enfoque descentralizado para la gestión de la identidad, toda vez que los individuos o las organizaciones no tienen el control de sus identidades, cuya informa-

[4] Se trata de un registro único, consensuado y distribuido en varios nodos de una red (Pastorini 2018).

ción es tratada sin su consentimiento desde sistemas centralizados. De ahí que surja la propuesta de crear identidades con seguridad y de alta disponibilidad con infraestructura basada en el *blockchain*. El tiempo demostrará su efectividad.

También es verdad que, con la llegada del internet, las personas pueden hacer uso de dispositivos para promover el gobierno electrónico y los instrumentos de democracia, así como ejercer sus derechos fundamentales. Pero eso no es todo. Con la llegada del internet de las cosas, las interacciones con los dispositivos electrónicos son más dinámicas, ya que a partir de estas es posible generar estrategias de tecnología con infraestructura digital para realizar interacciones coordinadas.

Con el internet de las cosas existe una interacción de máquina a máquina, en la que la tecnología permite a los dispositivos o a las máquinas en la red intercambiar información y, principalmente, desempeñar acciones sin la asistencia manual de una persona, lo que cambia toda la realidad. Así, los millones de dispositivos y máquinas conectados al internet pueden comunicarse entre sí y compartir, interactuar y automatizar procesos que podrían ser aburridos o no adecuados humanamente por su constante repetición, convirtiendo hogares, ciudades y naciones inteligentes donde todo esté conectado (Zadaming 2018, 355-96).

Ante ello, cabe preguntarse: ¿cómo afectan a la democracia las conexiones de máquina a máquina? Para responder, es preciso referirse a los bots, un término que ha surgido ante el creciente uso de las tecnologías de la información y la comunicación.

De acuerdo con la Real Academia Española, la palabra *robot* proviene del inglés *robot*, y este, del checo *robot*, cuyo origen es *robota*, que significa "trabajo, prestación personal"; en su definición, es "Máquina o ingenio electrónico programable que es capaz de manipular objetos y realizar diversas operaciones" (RAE 2020). Si a ese concepto se le relaciona con la informática, se convierte en un programa que explora automáticamente la red para encontrar información.

Por lo tanto, surge otra interrogante: ¿los bots son un peligro para la democracia? En un primer momento, debe quedar claro que los bots no son personas, sino máquinas. Por tal motivo, se tendría que identificar y descalificar dichas cuentas antes de que puedan influir en los discursos y en las expresiones políticas en internet (Zadaming 2018, 36).

Lo anterior se puede ejemplificar de la siguiente manera: ¿qué pasaría si los debates en las redes sociales se cayeran en cuestión de segundos? Por citar un ejemplo, el tema de la democracia y la libertad de expresión con la tecnología se convierte en un asunto de la agenda pública y de interés general. En consecuencia, los usuarios viralizan el debate al utilizar y compartir el *hashtag* #DemocraciaTecnológica en Twitter hasta volverlo tendencia y hacerlo aparecer en los destacados de esta red; posteriormente, un ejército de bots, que se hace pasar por humanos, secuestra el debate político al postear la etiqueta #ComeFrutasYVerduras, lo que hace desaparecer el *hashtag* #DemocraciaTecnológica y provoca que el debate llegue a menos personas, al promover que estas dejen de hablar del tema.

Surge entonces una nueva pregunta: ¿los bots destruyen la democracia? La respuesta es "sí". La prohibición de *software* automatizado destinado a suplantar o replicar la actividad humana para la publicidad política en línea es un tema que deberá tratarse y discutirse con exhaustividad. La realidad es que los bots generan contenido y, en consecuencia, manipulan a la sociedad, lo que representa un gran problema para la democracia y para los derechos fundamentales, como en el caso de los datos personales.

Protección necesaria de los datos personales en las redes sociales

En el apartado anterior se dio cuenta de que en el entorno digital es posible mantener una interacción en cuestión de minutos, aunque para lograrlo se requiere un ingrediente: los datos personales, que son el elemento crucial de la información para promover una verdadera democracia participativa y una administración eficiente.

De ahí que los datos personales se han convertido en la nueva herramienta de poder; su conocimiento es poder y, por medio de su análisis, se puede obtener información útil para la toma de decisiones.

Un dato personal es, por ejemplo, el nombre, el número de teléfono celular o el correo electrónico, es decir, la información concerniente a una persona física identificada o identificable; también existen datos sensibles, como el origen racial o étnico; el estado de salud; la información genética; las creencias religiosas, filosóficas y morales; la afiliación sindical; las opiniones políticas, y la preferencia sexual.

Incluso, diversos sitios de internet solicitan dicha información para ofrecer algún servicio, como ocurrió con los test de Facebook: lo que parecía un juego para reír y hacer comentarios entre amigos, en realidad sirvió para procesar información e incidir en la venta de productos, manipular el estado de ánimo y hasta influir en la decisión de los votantes (Wakefield 2015; Romero 2017; Arros 2018; Forbes Staff 2019).

Por lo anterior, se puede afirmar que los datos tienen un gran valor cuando todo alrededor se encuentra automatizado, ya que por sí mismos no son nada; solo es información sin sentido que debe ser organizada. Así, los datos son útiles cuando son procesados y analizados, convirtiéndolos en información y esta, a su vez, en conocimiento, que puede inferir en la toma de decisiones, incluso en los procesos políticos.

Desde una perspectiva digital, toda la información que procesan los sistemas automatizados tiene como base el sistema binario (compuesto solo por dos cifras: 1 y 0), además de ser calculada en bits. Otro aspecto importante tiene que ver con los riesgos potencialmente altos de los sistemas automatizados de tratamiento de datos, unidos a los sistemas de minería de datos e inteligencia artificial.

Precisamente, mediante dichos procesos es posible la gestión de grandes cantidades de información de forma automatizada, cuyo riesgo implica la asociación y la elaboración de perfiles ideológicos a gran escala (Llácer 2011, 67). Lo anterior puede implicar un seguimiento acerca del compor-

tamiento de la persona, no obstante que su aplicación concreta e individual puede ser demasiado discriminatoria.

No cabe duda de que, en la actualidad, el incremento y el uso de los datos personales en los procesos electorales, aunado al desarrollo tecnológico, pueden significar una constante vulneración de la privacidad de los votantes. Por ello, para enfrentar esa problemática debe existir un mínimo de garantías, a fin de que los votantes, al momento en el que emiten su sufragio, tengan la certeza de que su decisión será tomada en cuenta y no usada para otros fines.

Por otro lado, las redes sociales también desempeñan un papel importante, puesto que se han convertido en una herramienta que ha predominado en el cambio de las elecciones políticas, convirtiéndose así en un instrumento de comunicación para los políticos y gobiernos.

A diferencia de otros medios de comunicación tradicionales, como el periódico, el radio y la televisión, las redes sociales otorgan a las personas un elemento esencial para las democracias contemporáneas, el cual consiste en la capacidad de comentar, compartir y publicar ideas, transformándose en un gran altavoz y canal de comunicación entre candidatos y ciudadanos, y gobernantes y gobernados.

Al respecto, el caso más representativo es el de Barack Obama, expresidente de Estados Unidos de América, cuyo mandato duró ocho años y quien resultó victorioso por medio de la elección y la reelección.

En lo que respecta al primer proceso por el que fue electo, cabe destacar que existían pocas redes sociales si se comparan con las que hay en la actualidad; no obstante, Obama representó la diferencia, como lo señaló *The Washington Post*, periódico que lo consideró como el rey de las redes sociales al ser el primero en aprovechar este medio tras crear perfiles en Eons y Myspace para acercarse a la generación de *baby boomers*, así como en blackplanet.com y migente.com, que son comunidades virtuales para personas de origen afroamericano y latino, y en asianave.com para los asiáticos estadounidenses. Por lo anterior, quizá Barack Obama no

haya sido el más popular, pero fue un candidato con demasiada audiencia en todos los sitios virtuales sociales (Vargas 2007).

Fue muy evidente que Obama utilizara las redes sociales tradicionales en esos tiempos y, si bien anunció su candidatura el 10 de febrero de 2007, para el 3 de junio de 2008 se convirtió en el candidato del Partido Demócrata. Posteriormente, triunfó en las elecciones presidenciales del 4 de noviembre del mismo año, frente a John McCain, y tomó posesión del cargo el 20 de enero de 2009.

En ese contexto, Obama usaba su perfil de Twitter desde marzo de 2007, mientras que McCain, su contrincante, desde enero de 2009. Por tal motivo, se puede considerar este proceso como el de un ejercicio democrático y de elecciones en las redes sociales.

Ahora bien, en relación con el segundo proceso electoral, celebrado el 4 de abril de 2011, Obama anunció su reelección presidencial para 2012 y el 6 de noviembre de ese año resultó ganador, al ser reelecto por un periodo más, venciendo a su contrincante Mitt Romney.

Cabe mencionar que, a diferencia del proceso electoral de 2007, en ese momento las redes sociales ya no eran algo novedoso, pues los candidatos ya habían evolucionado como cibernautas, por lo que el pago de publicidad y el procesamiento de datos fueron los elementos principales para triunfar en el mundo inmaterial cibernético e influir en el material. Por lo anterior, se puede decir que dicha elección no solo fue de redes sociales, sino que también tuvo al *big data* (macrodatos) como un elemento adicional.

¿En qué consiste el *big data*? En términos generales, se trata de la administración masiva de datos (Schmarzo 2014); es decir, es el procedimiento mediante el cual se organizan respecto a su volumen, variedad y velocidad.

Esto es, respecto al volumen, tener en cuenta la cantidad de datos que se procesan y se almacenan; luego, por la variedad, qué tipos de datos son, comenzando con sus caracteres, hasta el sector en el que se encuen-

tran, y, por último, la velocidad, para considerar la rapidez con la que son procesados y comunicados.

En definitiva, a partir de los datos la nueva guerra política comienza a estar presente, trayendo como consecuencia el hackeo de la democracia, como se verá a continuación.

El hackeo democrático. Una realidad

En la actualidad, hay una etapa en la que los avances tecnológicos vuelven realidad lo que antes parecía ciencia ficción. En los últimos tres siglos han transcurrido tres grandes revoluciones industriales[5] y, recientemente, ha surgido una cuarta, vinculada con varios fenómenos,[6] en particular con el desarrollo de la inteligencia artificial.

El ámbito electoral, por sus características, es el lugar idóneo para introducir innovaciones tecnológicas debido a la gran cantidad de datos personales y la información con los que se puede contar; incluso es posible la generación de resultados confiables en un corto periodo, a pesar de los riesgos que ello implica.

Con la tecnología, la sociedad ha alcanzado niveles máximos históricos en cuanto a la disponibilidad de la información y la libertad de expresión. Sin embargo, la democracia en la que siempre se ha confiado está siendo amenazada por diversas organizaciones, capaces de manipular el universo digital de manera silenciosa.

El hackeo o la manipulación de la democracia, así como los retos de la tecnología en época de elecciones, como son el voto electrónico, las noticias falsas y la difusión de la información, son una constante en las redes sociales y en el internet, cuyo objetivo no es otro que el de manipular

---

5 La primera, relacionada con el desarrollo del ferrocarril y el motor de vapor para mecanizar la producción; la segunda, vinculada con la energía eléctrica y la cadena de montaje para desarrollar la producción en masa, y, la tercera, ubicada a partir del surgimiento de la electrónica, las computadoras y la tecnología de la información para automatizar la producción.

6 Se habla de la nanotecnología, la biotecnología robótica y el internet de las cosas, entre otros.

a los electores, llegando incluso a impactar en la toma de decisiones políticas debido a la filtración de cables confidenciales robados por piratas informáticos (Sendín 2018).[7]

Un caso emblemático es el de Cambridge Analytica, cuyo trabajo en las elecciones de Estados Unidos de América en 2016 no consistió en que los partidos enviaran propaganda política, identificada como tal, por los medios electrónicos, sino en utilizar los perfiles psicológicos e ideológicos de millones de usuarios de Facebook para dirigirles *fake news* personalizadas que aparecieron en los muros de sus cuentas y fomentaron el discurso de odio.

Como antecedente de dicho caso, es necesario puntualizar acerca del impacto y la trascendencia de los datos personales y su procesamiento. Como se comentó, en las redes sociales, principalmente en Facebook, es común encontrar preguntas del tipo "¿A qué famoso te pareces?", "¿Qué dicen tus ojos sobre tu personalidad?", "¿Cómo se verá tu futura hija?" o "¿Cómo te verás en 50 años?". Sin duda, dichos test permiten la interacción en las redes, pero, al mismo tiempo, recopilan información personal con el objetivo de ser utilizada para otros fines, incluso ilícitos.

Siguiendo con el tema de Cambridge Analytica, empresa dedicada al análisis de datos en procesos electorales mediante su contratación por actores políticos —cuyo trabajo destaca al haber participado en la campaña del *brexit* y en el proceso electoral de Estados Unidos de América con la candidatura de Donald Trump—, la organización protagonizó uno de los mayores escándalos respecto al manejo de datos personales y su procesamiento en las elecciones.

La recopilación de los datos se hizo por medio de la aplicación This Is Your Digital Life, desarrollada por Aleksandro Kogan, mediante un cuestionario de personalidad de Facebook en 2014; posteriormente, los datos pasaron a Cambridge Analytica y se recopilaron con fines académicos. Sin

---

[7] A diferencia de lo ocurrido con WikiLeaks en 2010 o del ataque ruso al Comité Nacional Demócrata en 2016, el motivo se constituye por un espionaje sistemático.

embargo, dicha aplicación también obtuvo información de los amigos de los perfiles en Facebook, red social que también fue utilizada, pese a que en sus políticas se prohíbe la venta de datos (Guimón 2018).

Cabe mencionar que, aunque 270,000 usuarios dieron su permiso, deben tenerse en cuenta los datos de sus amigos. De ahí que se haya previsto que se accedió a los datos de más de 87 millones de personas, la mayoría, perfiles procedentes de Estados Unidos de América, aunque la red social calcula que 2,700,000 cuentas son de la Unión Europea y que más de 780,000 pertenecen a usuarios mexicanos (González 2018).

Por lo anterior, cabría preguntarse cuál fue el rol de Cambridge Analytica en las elecciones de Estados Unidos de América al haber empleado la aplicación de Kogan y la información de Facebook. Según diversos diarios estadounidenses, la tarea principal era inferir perfiles psicológicos de cada usuario, sabiendo cuál debía ser el contenido, el tema y el tono del mensaje, a fin de cambiar la forma de pensar de los votantes, casi de manera individual, además del envío de publicidad personalizada y del desarrollo de noticias falsas que, posteriormente, se replicaron en diversas redes sociales, blogs y otros medios (BBC Mundo 2018). El resultado ya es conocido por todos: Donald Trump obtuvo la presidencia de Estados Unidos de América en 2016.

Con lo anterior, queda claro que hoy en día utilizar la tecnología en los procesos electorales posibilita la obtención de resultados favorables para los políticos que mejor sepan usarla.

Por tal motivo, se dio inicio al presente trabajo al afirmar que entender qué piensa cada votante y poder enviarle un mensaje personalizado con lo que le ofrece un partido es el sueño de cualquier estratega de la comunicación política. Precisamente, segmentar y crear mensajes específicos para cada grupo no tiene nada de malo e, incluso, es de utilidad para que los partidos puedan crear mensajes cercanos a las preocupaciones de la ciudadanía, realidad que materializó Cambridge Analytica por medio del *microtargeting* (personalización del consumidor).

Sin embargo, su uso es peligroso cuando es opaco y no está adecuadamente regulado. Al segmentar de manera alta los mensajes, estos solo son vistos por pequeños grupos de población y evitan el escrutinio y la fiscalización públicos. Lo anterior permite a los partidos políticos caer en la opacidad y sembrar dudas en torno a un proceso electoral o, directamente, incitar al odio mediante la desinformación y las campañas de descrédito.

Incluso es posible que los partidos políticos se escondan detrás de estos mensajes: cuando el *microtargeting* se hace mediante canales encriptados —como el caso de WhatsApp—, la opacidad aumenta al punto de hacer imposible cualquier tipo de monitoreo.

Algo similar ocurrió en el referéndum británico acerca de la salida de la Unión Europea por parte del Reino Unido (conocida como *brexit*) (Sendín 2018) y en las elecciones brasileñas (Bimbi 2018), en los que se viralizaron diversos mensajes por WhatsApp. Incluso, ante la masiva difusión de mensajes por los medios digitales (especialmente en cuentas de Facebook, WhatsApp y Twitter), unas veces cumpliendo las normas y otras no, se tuvo como consecuencia que algunas de esas cuentas se cerraran por difundir información desde perfiles falsos y duplicados (Ollero 2018), como aconteció en la campaña electoral de España del 10 de noviembre de 2019.

Esto no es un fenómeno nuevo. En el proceso federal de México en 2012, las legiones de bots lograron un gran impacto, cuyas estrategias y operaciones digitales con fines de manipulación electoral beneficiaron a Enrique Peña Nieto, al obtener la presidencia. Sin embargo, la intervención en temas de relevancia mediática, como Ayotzinapa, la Casa Blanca y las masacres encubiertas en Apatzingán y Tlatlaya, estuvo marcada por el abuso en la operación digital para intervenir en la conversación e indignación en las redes sociales. Ello generó un mayor conocimiento por parte de los electores acerca de los *trending topics* manipulados y los peñabots.

Tiempo después, en 2018, durante la campaña electoral por la presidencia de la república en México, la manipulación de los electores en el mundo digital ya no fue tan efectiva como en 2012, lo que significó para

el país un avance en el tema. En ese contexto, destaca el trabajo comunitario realizado por #Verificado2018,[8] una página web encargada de desmentir las manipulaciones.

Lo anterior representa algunos ejemplos del hackeo al cual ha estado sometida la democracia en el mundo digital. De ahí que estén comenzando a surgir los *factcheckers* (verificadores de hechos) para desmentir o precisar los acontecimientos, al contrastar las noticias y aportar datos objetivos de fuentes fiables.

En definitiva, las innovaciones tecnológicas hacen necesario debatir qué prácticas sociales y políticas se requieren para el siglo XXI; es decir, qué tipo de democracia se pretende y cuál ciudadanía será la que la protagonice o, en su defecto, si es preciso que se deba contar con un marco normativo que las regule.

Sin embargo, para entenderlo mejor, es preciso analizar la percepción material de la democracia, vista desde la utilización de los dispositivos como objetos.

Tecnología al servicio del hackeo democrático

La tecnología, el internet de las cosas y la inteligencia artificial están ligados al procesamiento de la información y los datos, así como a la implementación de algoritmos inteligentes. Con todo ello, resulta posible identificar las tendencias económicas, predecir el comportamiento digital de la sociedad, diagnosticar alguna enfermedad e, incluso, reconocer determinados problemas y sus posibles soluciones.

La tecnología, vista como un objeto —esto es, mediante el uso de dispositivos electrónicos, como los teléfonos inteligentes—, facilita la comunicación entre las personas; sin embargo, a pesar de sus funcionalidades, sigue siendo objeto. Por otro lado, si se le considera como un medio, es

[8] Se trata de un proyecto integrado por más de 60 organizaciones sociales, universidades y medios de comunicación, cuyo objetivo es detectar las noticias falsas, o *fake news*, y luchar contra ellas de cara a las elecciones presidenciales.

posible incorporarla al cuerpo humano con el fin de superar o mejorar un déficit, lo que puede traducirse en una extensión de la anatomía; es el caso de los cíborgs[9] y el *biohacking*,[10] o bien desde la perspectiva de las corrientes del transhumanismo[11] y poshumanismo.[12]

Por lo tanto, cuando se modifica al ser humano por medio de la tecnología, a fin de mejorar sus capacidades físicas e intelectuales, se deja atrás la percepción de verla como un objeto o una cosa. En ese supuesto, la tecnología se convierte en una extensión del cuerpo, es decir, forma parte del ser humano y de su condición.

Sin embargo, cuando es vista como un fin, se genera una concepción distinta a las anteriores, pues sirve para referirse a actos comisivos, cuyo resultado es un sujeto que ejercita la acción; en ese ámbito entra en juego la inteligencia artificial.

En una revisión breve acerca de los dispositivos tecnológicos, como se comentó, se encuentra el internet de las cosas (en inglés, *internet of things*), término atribuible al británico Kevin Ashton, quien lo ha definido "como una red que no solo conecta a las personas, sino también a los objetos que las rodean" (Ashton 2009).

En el ámbito técnico, la recomendación UIT-T Y.2060 de la Unión Internacional de Telecomunicaciones se refiere al internet de las cosas como la

---

9 "Es un organismo cibernético, un híbrido de máquina y organismo, una criatura de realidad social y también de ficción" (Majfud 2018, 30 y ss.).

10 El término *biohacking* (biología *do it yourself*) nace de la unión de las palabras *biología* y *hacking*; contextualmente, se refiere a la gestión de la propia biología utilizando una serie de técnicas médicas, nutricionales y electrónicas con el objetivo de ampliar las capacidades físicas y mentales del sujeto (Hidalgo 2016).

11 Es un movimiento intelectual y cultural que afirma la posibilidad y la deseabilidad de mejorar fundamentalmente la condición humana mediante la razón aplicada, de manera especial por medio del desarrollo y la puesta a disposición de tecnologías ampliamente disponibles para eliminar el envejecimiento y mejorar, en gran medida, el intelectual humano, el físico y las capacidades psicológicas (Bostrom 2003).

12 Se trata de una corriente que postula a un ser que tiene al menos una capacidad poshumana, esto es, una capacidad central general que excede, en gran medida, el máximo alcanzable por cualquier humano actual sin recurrir a nuevos medios tecnológicos (Bostrom 2003).

> Infraestructura mundial para la sociedad de la información que propicia la prestación de servicios avanzados mediante la interconexión de objetos (físicos y virtuales) gracias a la interoperatividad de tecnologías de la información y la comunicación presentes y futuras (UIT 2012, 6).

Hablar del tema décadas atrás hubiera representado un argumento de ciencia ficción, esto es, dispositivos conectados e inteligentes que toman decisiones por medio de la recopilación, el análisis y el procesamiento de datos para ejecutar acciones. Sin embargo, ya es una realidad.

Para explicar lo anterior, cabe mencionar que el tipo de conectividad y la comunicación tecnológica hacen que las máquinas se comuniquen con otras máquinas, lo que compone la parte fundamental del internet de las cosas. Más aún, con una visión más amplia, va encaminado a sistemas que facilitan la gestión entre personas y máquinas, lo que permite la relación de objetos y cosas con acciones y movimientos.

Sin duda, esa nueva forma de relacionarse abre un gran tema para generar debates y perspectivas, por ejemplo, con la privacidad. En lo que respecta a la vida democrática, se transformará la vida cotidiana y se crearán nuevos modelos de participación mediante dispositivos conectados que hacen uso de los datos, relacionándolos así con los asuntos públicos.

Por otro lado, aunque ya se ha hecho una breve mención del concepto cíborg (en inglés, *cyborg*), aun cuando ha sido usado de manera más constante en la ciencia ficción, la realidad es que este siempre ha ido de la mano de la lucha por la libertad. Por ello, cabe referirlo como una medida material y no tanto formal para llegar a una democratización.

El término *cyborg* fue acuñado en 1960 por Manfred Clynes y Nathan S. Kline y se interpreta como un ser humano mejorado que podría sobrevivir en entornos extraterrestres. La unión entre materia viva —que es el ser humano— y dispositivos electrónicos crea un organismo cibernético denominado cíborg. Por otro lado, para Steven Mann, creador de la computación portátil, es una persona cuyo funcionamiento fisiológico es

ayudado por o depende de un dispositivo mecánico o electrónico (Mann y Niedzviecki 2001).

Ahora bien, respecto al cíborg ciudadano, el problema democrático relacionado con la tecnología radica en que no es confiable por su naturaleza modificable y manipulable. Por lo tanto, el respeto a las instituciones y la participación en estas sería casi nulo.

Es una clara realidad del mundo, en el cual la sociedad vive con avances tecnológicos que ya logran lo que antes parecía ciencia ficción. De ahí que el entorno electoral, por sus características, es el lugar idóneo para introducir innovaciones tecnológicas, debido a la gran cantidad de datos personales e información, por lo que resulta preciso generar resultados confiables en un corto periodo, a pesar de los riesgos que ello implica.

Cada día, como se ha revisado a lo largo de este trabajo, la tecnología y la inteligencia artificial están ligadas al procesamiento de la información y los datos, así como a la implementación de algoritmos inteligentes. Con todo ello, resulta posible identificar las tendencias económicas, predecir el comportamiento digital de la sociedad, diagnosticar alguna enfermedad e, incluso, reconocer determinados problemas y sus posibles soluciones.

De ahí que pueda decirse que, en el ámbito político, la tecnología y la inteligencia artificial han ido encontrando un sitio para su implementación, en el que su uso podrá optimizar el flujo de datos y la información disponible; asimismo, permitirá resolver cuestiones que antes requerían múltiples pasos, procedimientos y fases, o de las que, en algunos casos, no se tenía una respuesta para resolverlas, como en la toma de decisiones políticas.

Al respecto, cabe mencionar el caso del robot Michihito Matsuda, que en mayo de 2018 fue candidato en una elección en un distrito de Tokio, Japón, y fue el tercer aspirante más votado debido a su idea de acabar con la corrupción. En España, hace unos años, se incorporó la iniciativa Ciencia en el Parlamento,[13] cuyo objetivo consiste en utilizar el conocimiento

[13] Una iniciativa ciudadana independiente surgida en España en 2018.

científico en la formulación de propuestas políticas con base no solo en la evidencia científica, sino también en los grandes cambios diversos al entorno tecnológico.

México tampoco ha sido ajeno al uso de la tecnología en los procesos electorales. En la elección presidencial de 2018 apareció EMI (Estándar Mínimo de Inteligencia),[14] el primer chatbot que acompañó a las y los ciudadanos en el ejercicio del voto informado, cuyo objetivo principal fue responder los cuestionamientos referentes al entonces proceso electoral federal.

Ante esas nuevas realidades, cabría preguntarse lo siguiente, con base en la experiencia de la tecnología y la inteligencia artificial: ¿están preparados los estados para la implementación tecnológica en los procesos electorales? ¿Será posible influir en la mente de las y los votantes en el momento de tomar decisiones sin que se vea afectada su privacidad? Más aún, ¿será posible reemplazar parte de las funciones de las y los políticos por algoritmos que les ayuden a hacer su trabajo? ¿Están preparados los gobiernos para la inclusión de la inteligencia artificial en la toma de decisiones?

Con el tiempo se darán las respuestas a las nuevas realidades, las cuales están presentes en el terreno político y conciernen a todas las democracias del mundo.

Conclusiones y reflexiones

1. La tecnología y la inteligencia artificial son una realidad. Cada día que pasa la humanidad se va acostumbrando al modo como las máquinas apoyan en las tareas cotidianas, sin importar la actividad que se trate. La política, por sus características, es el lugar idóneo para introducir innovaciones tecnológicas debido al gran volumen de información disponible con la que se cuenta y que se puede generar.

---

[14] Una inteligencia artificial diseñada y creada en el laboratorio UNAM Mobile. Al respecto, véase DGCS (2018).

2. El uso de macrodatos y algoritmos es, sin duda, una auténtica revolución. Con ellos se hace posible, cada vez más, analizar el exceso de información presente en internet y, por ende, generar resultados favorables en beneficio de la sociedad; su empleo en el ámbito político no será la excepción.

3. En un futuro no muy lejano, para hackear la democracia se utilizarán técnicas más sofisticadas, como una guerra psicológica o la inteligencia artificial; asimismo, se dejará de recurrir a becarios, *millennials* o estudiantes de comunicación para contratar a expertos que tengan la capacidad de crear campañas y manipular los datos, como es el caso de los numerati.

4. Para hacer frente a la radicalización de la democracia mediante las nuevas tecnologías, resulta fundamental una discusión acerca de la neutralidad de la red y la brecha digital, así como su posible regulación en tiempos electorales, a fin de que las nuevas formas de participación y decisión sean lo más democráticas posibles. En caso contrario, se estaría en un plano de desigualdad, en el que las personas con mayores recursos tengan más posibilidades de decidir en torno a asuntos que impacten a la sociedad.

5. La generación de una cultura digital contribuirá, sin lugar a dudas, al entendimiento de la democracia en un mundo cada vez más global y sin fronteras.

Fuentes consultadas

Arros, Fernanda (junio 28 de 2018). *Una famosa aplicación de tests en Facebook expuso la información privada de millones de usuarios*. Mouse, disponible en http://mouse.latercera.com/test-facebook-peligro-informacion-filtracion-seguridad/ (consultada el 13 de marzo de 2020).

Ashton, Kevin (junio 22 de 2009). *That "Internet of Things". In the real world, things matter more than ideas*. RFID Journal, disponible en https://www.rfidjournal.com/articles/view?4986 (consultada el 20 de marzo de 2020).

Baker, Stephen. 2009. *Numerati. Lo saben todo de ti*. Barcelona: Seix Barral.

BBC Mundo. 2018. "5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día". *BBC News*, 20 de marzo, sección Mundo. [Disponible en https://www.bbc.com/mundo/noticias-43472797 (consultada el 19 de abril de 2020)].

Bimbi, Bruno (octubre 20 de 2018). *Elecciones en Brasil: dinero sucio, corrupción y* fake news *en la campaña de Bolsonaro*. Todo Noticias, disponible en https://tn.com.ar/internacional/elecciones-en-brasil-dinero-sucio-corrupcion-y-fake-news-en-la-campana-de-bolsonaro_907624 (consultada el 21 de abril de 2020).

Bostrom, Nick. 2003. *The transhumanist FAQ. A general introduction. Version 2.1 (2003)*. The World Transhumanist Association. Disponible en https://nickbostrom.com/views/transhumanist.pdf (consultada el 10 de enero de 2020).

Burch, Sally (septiembre 9 de 2014). *Poder y democracia en la red*. Sally Burch, disponible en https://www.alainet.org/es/articulo/84705 (consultada el 14 de mayo de 2015).

Caballero, Ana. 2018. "Llega la cuarta revolución industrial". *El Mundo*, abril, sección Economía Digital. [Disponible en http://www.impulsodigital.elmundo.es/economia-digital/llega-la-cuarta-revolucion-industrial (consultada el 15 de febrero de 2020)].

Cadwalladr, Carole y Emma Graham-Harrison (marzo 17 de 2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Cambridge Analytica, disponible en https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (consultada el 19 de junio de 2020).

DGCS. Dirección General de Comunicación Social. 2018. Desarrollan en la UNAM primera inteligencia artificial que responde dudas sobre el proceso electoral. Disponible en https://www.dgcs.unam.mx/boletin/bdboletin/2018_324.html (consultada el 25 de mayo de 2018).

Forbes Staff. 2019. "Netflix estrena 'nada es privado' y abre la puerta a la teoría de la conspiración". *Forbes*, 26 de julio, sección Actualidad. [Disponible en https://www.forbes.com.mx/netflix-estrena-nada-es-privado-y-abre-la-puerta-a-la-teoria-de-la-conspiracion/ (consultada el 19 de marzo de 2020)].

Fundación Telefónica. 2013. *Identidad digital: el nuevo usuario en el mundo digital*. Barcelona: Ariel/Fundación Telefónica.

González, María. 2018. "Qué ha pasado con Facebook: del caso Cambridge Analytica al resto de polémicas más recientes". *Xataka*, 11 de abril, sección Legislación y Derechos. [Disponible en https://www.xataka.com/legislacion-y-derechos/que-ha-pasado-con-facebook-del-caso-cambridge-analytica-al-resto-de-polemicas-mas-recientes (consultada el 14 de mayo de 2020)].

Guimón, Pablo (marzo 27 de 2018). *El* brexit *no habría sucedido sin Cambridge Analytica*. Caso Cambridge Analytica, disponible en https://elpais.com/internacional/2018/03/26/actualidad/1522058765_703094.html (consultada el 15 de junio de 2020).

Hidalgo, María. 2016. "*Biohacking*, el nuevo movimiento que hackea tu cuerpo y hace temblar la industria biotecnológica". *Muhimu*, 4 de octubre, sección Ciencia y Tecnología. [Disponible en https://muhimu.es/ciencia-tecnologia/biohacking/ (consultada el 18 de febrero de 2020)].

IBM. International Business Machines. S. f. *Transforming digital identity into trusted identity*. IBM. Disponible en https://www.ibm.com/blockchain/solutions/identity (consultada el 29 de abril de 2020).

Llácer Matacás, María Rosa. 2011. *Protección de datos personales en la sociedad de la información y la vigilancia*. Madrid: La Ley.

Majfud, Jorge. 2018. *Cyborgs*. España: Izana Editores.

Mann, Steven y Hal Niedzviecki. 2001. *Cyborg: digital destiny and human possibility in the age of the wearable computer*. Canadá: Doubleday.

Naím, Moisés. 2005. *Illicit: how, smugglers, traffickers and copycats are hijacking the global economy*. Nueva York: Doubleday.

——. 2014. *El fin del poder*. México: Random House Mondadori/Debate.

Nyhan, Brenda. 2018. "El verdadero efecto político de las noticias falsas". *The New York Times*, 16 de febrero, sección The Upshot. [Disponible en https://www.nytimes.com/es/2018/02/16/efecto-politico-noticias-falsas/ (consultada el 20 de junio de 2020)].

Ollero, Daniel. 2018. "Facebook contra la derecha radical: cierra decenas de páginas con millones de seguidores". *El Mundo*, 23 de abril, sección Elecciones. [Disponible en https://www.elmundo.es/tecnologia/trucos/2019/04/23/5cbf402c21efa06d5e8b4726.html (consultada el 15 de mayo de 2020)].

Pastorini, Cecilia (septiembre 4 de 2018). Blockchain*: qué es, cómo funciona y cómo se está usando en el mercado*. Welivesecurity, disponible en https://www.welivesecurity.com/la-es/2018/09/04/blockchain-que-es-como-funciona-y-como-se-esta-usando-en-el-mercado/ (consultada el 25 de enero de 2020).

RAE. Real Academia Española. 2020. *Diccionario de la lengua española*. 23.ª ed. Disponible en https://dle.rae.es (consultada el 30 de mayo de 2020).

Rifkin, Jeremy. 2013. *La era del acceso. La revolución de la nueva economía*. Barcelona: Paidós.

Riofrío Martínez Villalba, Juan Carlos. 2014. "La cuarta ola de derechos humanos: los derechos digitales". *Revista Latinoamericana de Derechos Humanos* 25 (enero-junio): 14-45.

Rodotá, Stefano. 2014. *El derecho a tener derechos*. Madrid: Trotta.

Romero, Carolina. 2017. "El inquietante secreto detrás de los tests de Facebook". *Cultura Colectiva*, 29 de marzo, sección Tecnología. [Disponible en https://culturacolectiva.com/tecnologia/tests-de-facebook (consultada el 25 de mayo de 2020)].

Salas, Javier. 2018. "La información falta llegar más lejos, más rápido y a más gente que la verdadera". *El País*, 8 de marzo. [Disponible en https://elpais.com/elpais/2018/03/08/ciencia/1520470465_910496.html (consultada el 22 de mayo de 2020)].

Sam. The world's first virtual politician (2018. All rights reserved). *Sam. Meet your politician of the future*, disponible en http://politiciansam.nz/index.html (consultada el 20 de junio de 2020).

Schmarzo, Bill. 2014. *Big data. El poder de los datos*. España: Anaya Editores.

Schwab, Kalus. 2017. *La cuarta revolución*. México: Debate.

Sendín, Paula. 2018. "Hackeo masivo a la UE". *La Razón*, 20 de diciembre, sección Política. [Disponible en https://www.larazon.es/internacional/hackeo-masivo-a-la-ue-IB21029980 (consultada el 19 de julio de 2020)].

UIT. Unión Internacional de Telecomunicaciones. 2012. Y.2060: Panorámica de internet de las cosas. Recomendación Y.4000/Y.2060 (06/12). Disponible en https://www.itu.int/rec/T-REC-Y.2060-201206-I (consultada el 10 de abril de 2020).

Vargas, José Antonio (octubre 6 de 2007). *Barack Obama, social networking king*. The Trail, disponible en http://voices.washingtonpost.com/44/2007/10/barack-obama-social-networking.html (consultada el 23 de diciembre de 2019).

Wakefield, Jane. 2015. "Los peligros tras los populares 'quiz' de Facebook". *BBC News*, 27 de noviembre. [Disponible en https://www.bbc.com/mundo/noticias/2015/11/151127_tecnologia_quizzes_privacidad_facebook_il (consultada el 5 de junio de 2020)].

Whitaker, Reg. 1999. *El fin de la privacidad*. *Cómo la vigilancia total se está convirtiendo en realidad*. Barcelona: Paidós.

Zadaming Llamas Covarrubias, Jersain e Irving Norehem Llamas Covarrubias. 2018. *Internet ¿arma o herramienta?* México: Universidad de Guadalajara.