LA POLÍTICA DIGITAL EN MÉXICO

DERECHOS, CIUDADANÍA Y GOBIERNO

SENADO DE LA REPÚBLICA
ESTADOS UNIDOS MEXICANOS
LXV LEGISLATURA

Instituto Belisario Domínguez
Senado de la República

LA POLÍTICA DIGITAL EN MÉXICO

DERECHOS, CIUDADANÍA Y GOBIERNO

Ricardo Monreal Ávila, Miguel Ángel Osorio Chong,
Rodrigo Ávila Barreiro, Itzkuauhtli Zamora Saenz,
Judith Mariscal Avilés, César Rentería Marín,
Juan Pablo Aguirre Quezada, Jimena Moreno González,
Francisco Adrián García García, Ismene Ithaí Bras Ruíz,
Alejandro Pisanty Baruch, Carolina Aguerre,
Perla Carolina Gris Legorreta, Fernando Rocha Rosario,
Aram Barra Ramírez, Pablo Collada Chávez,
Jaime Arturo del Río Monges, José Luis Clavellina Miller,
María Fernanda Viecens, Lina Ornelas Núñez

SENADO DE LA REPÚBLICA
ESTADOS UNIDOS MEXICANOS
LXV LEGISLATURA

Instituto
Belisario Domínguez
Senado de la República

LA POLÍTICA DIGITAL EN MÉXICO

DERECHOS, CIUDADANÍA Y GOBIERNO

Primera edición: Abril 2022

D.R. © 2022 INSTITUTO BELISARIO DOMÍNGUEZ,
SENADO DE LA REPÚBLICA

Miguel Ángel Osorio Chong
Presidente

Donceles 14, colonia Centro,
Alcaldía Cuauhtémoc,
06020, Ciudad de México.

ISBN: 978-607-8620-46-3

Coordinación: Rodrigo Ávila Barreiro
Itzkuauhtli Benedicto Zamora Saenz

Edición: Lorena Hernández

Lectura de pruebas: Raúl Duque Luciano y Gamaliel Valentín

Diseño editorial: Edgar A. Reyes

Autorías: Ricardo Monreal Ávila, Miguel Ángel Osorio Chong, Rodrigo Ávila Barreiro, Itzkuauhtli Zamora Saenz, Judith Mariscal Avilés, César Rentería Marín, Juan Pablo Aguirre Quezada, Jimena Moreno González, Francisco Adrián García García, Ismene Ithaí Bras Ruíz, Alejandro Pisanty Baruch, Carolina Aguerre, Perla Carolina Gris Legorreta, Fernando Rocha Rosario, Aram Barra Ramírez, Pablo Collada Chávez, Jaime Arturo del Río Monges, José Luis Clavellina Miller, María Fernanda Viecens, Lina Ornelas Núñez.

DISTRIBUCIÓN GRATUITA

Las opiniones expresadas por las y los autores no necesariamente reflejan la postura de los editores de esta obra o del Instituto Belisario Domínguez del Senado de la República.

http://www.ibd.senado.gob.mx/ Facebook: IBDSenado Twitter: @IBDSenado

LA POLÍTICA DIGITAL EN MÉXICO

DERECHOS, CIUDADANÍA Y GOBIERNO

SENADO DE LA REPÚBLICA
ESTADOS UNIDOS MEXICANOS
LXV LEGISLATURA

Instituto Belisario Domínguez
Senado de la República

ÍNDICE

013 PRESENTACIÓN
Senador Ricardo Monreal Ávila

019 PRÓLOGO
Senador Miguel Ángel Osorio Chong

023 INTRODUCCIÓN
Rodrigo Ávila Barreiro e Itzkuauhtli Zamora Saenz
INSTITUTO BELISARIO DOMÍNGUEZ

053 CAPÍTULO 1
La política digital en México: siguiendo a la innovación tecnológica
Judith Mariscal Avilés y César Rentería Marín
CIDE - CENTRO LATAM DIGITAL

083 CAPÍTULO 2
Derechos digitales en México y otros países: regulación en constante transformación
Juan Pablo Aguirre Quezada
INSTITUTO BELISARIO DOMÍNGUEZ

111 CAPÍTULO 3
Ciudadanía digital, privacidad y protección de datos personales
Jimena Moreno González y Francisco Adrián García García
CIDE – CENTRO LATAM DIGITAL

CAPÍTULO 4
Ciudadanía digital, datos personales e inteligencia artificial: retos socioéticos para el T-MEC
Ismene Ithaí Bras Ruíz
FCPYS - UNAM
139

CAPÍTULO 5
Ciudadanía digital en México: derechos de acceso, habilidades y participación política
Itzkuauhtli Zamora Saenz
INSTITUTO BELISARIO DOMÍNGUEZ
179

CAPÍTULO 6
Estrategias nacionales de ciberseguridad en Latinoamérica y el Caribe
Alejandro Pisanty Baruch
UNAM – CENTRO LATAM DIGITAL
209

CAPÍTULO 7
Estrategias nacionales de ciberseguridad desde un enfoque de economía política
Carolina Aguerre
CIDE – CENTRO LATAM DIGITAL
241

CAPÍTULO 8
La transición hacia la e-democracia: lecciones para México
Perla Carolina Gris Legorreta
y Fernando Rocha Rosario
INSTITUTO BELISARIO DOMÍNGUEZ
269

309
CAPÍTULO 9
Participación ciudadana en México y reflexiones para su innovación
Aram Barra Ramírez y Pablo Collada Chávez
OPEN SOCIETY LATIN AMERICA

339
CAPÍTULO 10
Tres áreas de oportunidad que ofrece la economía digital para contribuir al desarrollo en México
Jaime Arturo del Río Monges
y José Luis Clavellina Miller
INSTITUTO BELISARIO DOMÍNGUEZ

383
CAPÍTULO 11
Acceso a Internet e inclusión financiera: teoría y evidencia acerca del rol de la innovación tecnológica
María Fernanda Viecens
CONICET – ARGENTINA

411
CAPÍTULO 12
La innovación basada en datos: hoja de ruta para lograrla
Lina Ornelas Núñez
GOOGLE

PRESENTACIÓN

SENADOR RICARDO MONREAL ÁVILA*

* Presidente de la Junta de Coordinación Política.

El libro que tiene en sus manos es el resultado de un esfuerzo editorial del Senado de la República, a través del Instituto Belisario Domínguez, por abordar un fenómeno de la mayor pertinencia en nuestros tiempos. Hablar de política digital implica ir directamente al centro del debate en torno a la justicia social en una época de profundos cambios en todos los ámbitos de la vida social, motivados por las innovaciones tecnológicas.

Particularmente, el contexto de la emergencia sanitaria provocada por la pandemia de Covid-19 propició, como se señala en esta obra, una aceleración en el proceso de transición hacia una sociedad digital, en el marco de la Cuarta Revolución Industrial (también llamada revolución digital). Esta aceleración, a su vez, expuso el lado más crudo de la desigualdad social que aún existe en nuestro país. Como resultado de la exclusión del acceso al uso de Internet, amplios sectores de la población, especialmente fuera de los grandes centros urbanos, quedaron al margen de las modalidades de teletrabajo y educación a distancia, y tuvieron que seguir el curso de la pandemia en condiciones de vulnerabilidad.

Por lo tanto, la presente obra nace en un momento pertinente para abordar el estado que guarda la política digital en nuestro país a efecto de poder proyectar las decisiones necesarias para hacer frente a los retos y desafíos en esta materia. No sólo se trata de ampliar la cobertura o el acceso a la infraestructura de las tecnologías de la información y la comunicación (TIC) ya que, si bien es condición necesaria superar esta asimetría, el simple acceso a dichas herramientas no garantiza el desarrollo de la sociedad. El objetivo de la política digital nacional debe ser calibrar el uso de las nuevas tecnologías mencionadas con un sentido social que permita diseñar políticas públicas para atender los diversos temas que enfrentan las sociedades de nuestros tiempos.

Dicho de otra forma, el debate al que esta obra busca contribuir tiene que ver no sólo con el acceso a dispositivos, plataformas, señales (el *qué*), antes bien es necesario acompañar este proceso de cambio tecnológico con el *cómo* incidir de manera efectiva en la realidad social. La transición digital implica el desarrollo de capacidades cognitivas e intelectuales en las personas, por lo que su proceso está altamente asociado con la función de la educación

como factor de desarrollo social. El papel de la educación permite, por lo tanto, trascender de una sociedad de la información a una sociedad del conocimiento. Una diferencia que, como se verá más adelante, no es menor.

Fijar como meta de desarrollo que la política nacional en materia digital permita la democratización, tanto de infraestructura, como de capacidades, en relación con el acceso a Internet y a las TIC, abre la posibilidad de hacer del México digital una sociedad del conocimiento. Sin embargo, esto obliga a los poderes públicos a deliberar en torno a una realidad en constante cambio. Pero esta debe ser una deliberación responsable, porque la política digital es un ámbito que tiene un amplio impacto en prácticamente todas las esferas de la vida individual y colectiva.

Las esferas política, social, económica y cultural se han convertido en espacios digitales en la medida en que las innovaciones tecnológicas van ampliando sus áreas de aplicación. Si en los albores de la revolución digital una de las premisas fundamentales del nuevo mundo era la libertad absoluta en el flujo de información a escala planetaria, su evolución ha atraído la atención de las agendas públicas para revivir debates en torno a la intervención del Estado en un ámbito de nueva generación.

La construcción de una vida democrática para nuestro país pasa entonces por definir los alcances de esta nueva realidad tecnológica y social. Entenderla como una cuestión de justicia social permitirá diseñar instrumentos de política pública que aporten a la superación de las desigualdades sociales que se acentúan en un contexto de exclusión digital. La edificación de una sociedad del conocimiento implica la ampliación de derechos para satisfacer necesidades emergentes, así como garantizar otros vigentes en contextos novedosos. La dimensión social de la política digital debe atender derechos civiles (libertad de expresión), políticos (derecho a la participación) y sociales (acceso a la educación), así como satisfacer nuevos derechos para salvaguardar otras esferas de la vida individual y colectiva, como es el derecho a la privacidad y a la protección de datos personales.

La propuesta de análisis que se ofrece en este libro considera que, en contextos democráticos, la política digital se traduce en esquemas de regulación pública de los espacios digitales con res-

peto a los derechos humanos fundamentales. Teniendo en cuenta el desarrollo histórico de las TIC, los espacios digitales (las redes sociales, por ejemplo) son lugares en manos de la iniciativa privada. Esto crea ambigüedades jurídicas respecto a la salvaguarda de derechos fundamentales que no permiten establecer con claridad la responsabilidad de las entidades privadas sobre la vulneración de tales garantías. Por esta razón, el Estado se convierte en la entidad con la autoridad suficiente para garantizar que las políticas de uso de los espacios digitales privados estén en armonía con el marco constitucional y los tratados internacionales de los que México es parte en materia de protección de los derechos humanos.

Sin embargo, como señalan nuestros autores, no existen las recetas mágicas para formular políticas perfectas en materia digital. Tal como ocurre en otros aspectos de la vida pública, la formulación de nueva legislación y el diseño de políticas públicas deben obedecer a las particularidades del contexto en el que tienen lugar. Las características políticas, éticas, sociales, económicas, culturales e históricas de cada sociedad determinarán las necesidades del debate público.

En México no podemos permanecer al margen de transformaciones de escala global como la que representa la revolución digital. Las aportaciones que nutren esta obra, provenientes de distintos enfoques y disciplinas, constituyen la materia prima de un debate necesario dentro de la agenda pública nacional. Un debate que reclama por igual la creatividad y la voluntad política para encontrar las formas que permitan convertir las tecnologías de la información y la comunicación en instrumentos de desarrollo social al potenciar sus alcances, al mismo tiempo que se respetan y garantizan los derechos humanos de las personas usuarias.

Por ahora, sirva esta presentación como una atenta invitación al amable lector para que encuentre, en las páginas que siguen, un conjunto de reflexiones e interrogantes sobre un futuro que ya nos alcanzó. Esta obra demuestra el compromiso del Senado de la República con el análisis de la realidad social para mejorar la toma de decisiones y, con ello, alcanzar un México digital para todas y todos.

PRÓLOGO

SENADOR MIGUEL ÁNGEL OSORIO CHONG*

* Presidente del Instituto Belisario Domínguez.

La discusión actual sobre la creciente necesidad de implementar políticas digitales es una invitación no sólo a reflexionar colectivamente sobre las implicaciones y efectos que los cambios tecnológicos traen consigo a nivel global, sino también constituye una oportunidad para enriquecer el intercambio de ideas sobre la ruta que un país como México debería tomar en esta materia.

El ámbito digital no debe ser considerado únicamente un tema técnico, también es un elemento estratégico y transformador que se incorpora a la vida cotidiana e incluye todos los procesos de política pública; desde los temas de seguridad nacional, hasta la participación política, pasando por la salud, la educación y el combate a las desigualdades. Este enfoque transversal contribuirá a que la transición digital no beneficie sólo a ciertos sectores de la población, sino a que mejore la vida de todas y todos, permitiendo disminuir las brechas sociales existentes.

Sin lugar a duda, la pandemia ha acelerado la llamada revolución digital. Ante el cierre de espacios físicos y los periodos de confinamiento, muchas actividades se trasladaron al ámbito digital. Para no ir más lejos, nuestras sesiones en el Senado de la República fueron en línea, las comparecencias se realizaron mediante videollamadas, las votaciones se implementaron en formatos híbridos para prevenir la saturación de espacios y cumplir el llamado a guardar una sana distancia. No obstante, al mismo tiempo, en los últimos meses se han hecho evidentes (y en algunos casos profundizado) las brechas que existían.

Atento a lo anterior, es necesario repensar qué tipo de transición digital necesita el país. Para ello es importante plantear cuestionamientos como: ¿qué lugar tiene el Estado en el ecosistema digital?, ¿cómo erradicar las brechas existentes en materia de acceso a las tecnologías de la información (TIC)? y ¿cómo poner las TIC al servicio de la población y de los grandes retos nacionales? Son preguntas que hacen eco en todos los sectores de la vida pública y que obligan a la búsqueda permanente de respuestas.

Parte de estas soluciones tienen que surgir del Poder Legislativo. En ese sentido, durante la LXIV Legislatura, en el Senado de la República se presentaron iniciativas que buscan garantizar el acceso a la justicia mediante el uso de las TIC, reconocer el derecho a la protección de toda actividad realizada en línea, regular la violencia en medios digitales, asegurar la rendición de cuentas y la transparencia o la protección de datos personales, por mencionar algunas. Todas ellas buscan responder a los retos que plantea la llamada Cuarta Revolución Industrial, así como construir un marco legal flexible que se ajuste a las dinámicas particulares de las TIC, proponga soluciones a los problemas tanto emergentes, como en constante evolución y, al mismo tiempo, favorezca la innovación.

Para lograrlo, como en cualquier política de Estado, se requiere de un horizonte de largo plazo con acciones basadas en evidencia que permitan alcanzar las metas que nos proponemos como sociedad. Esta agenda debe construirse de manera multisectorial y considerarse en los grandes tópicos por resolver para una vida social más justa, equitativa e incluyente. El reto es bastante grande, por ello la coordinación y colaboración entre el sector público, la sociedad civil, el empresariado, las universidades y los centros de investigación resultan esenciales para avanzar y profundizar en la comprensión de estos desafíos.

De eso trata *La política digital en México*, una publicación coordinada por el Instituto Belisario Domínguez que reúne escritos relacionados con dichos temas. En sus diferentes secciones se abordan diversos asuntos prioritarios relacionados con el mundo digital y se presentan propuestas de políticas públicas y reformas legales para exponer soluciones que nos permitan superar la brecha digital, construir capacidades digitales y anticiparnos también a las amenazas que emergen en este nuevo ámbito de la realidad humana.

El contenido de esta publicación es una interesante contribución para construir modelos que permitan a México desarrollar sus capacidades y adaptarse de la mejor manera al actual ecosistema digital. Ahora bien, cualquier política digital debe estar orientada a resolver los problemas del pasado, entender el presente y prepararnos para los desafíos del futuro.

Es difícil imaginar un mundo en el que la presencialidad sea suplida por medios digitales, pero es igualmente difícil imaginar un presente y un porvenir sin la evolución digital. Por ello, desde el Instituto Belisario Domínguez seguiremos abriendo espacios de discusión y reflexión para aportar, desde nuestra esfera de actuación, elementos que colaboren en el diseño de una política digital incluyente y sostenible.

INTRODUCCIÓN

RODRIGO ÁVILA BARREIRO
E ITZKUAUHTLI ZAMORA SAENZ*

* Instituto Belisario Domínguez.

El año 2020 ha sido clave en la expansión del entorno digital en cada una de las esferas de la experiencia social. Por un lado, el confinamiento global que se realizó a partir de la pandemia de Covid-19 aumentó el comercio electrónico y favoreció el teletrabajo y la educación a distancia; por otro, la coyuntura política de la elección presidencial en Estados Unidos que derivó en la cancelación de las cuentas en redes sociodigitales del entonces presidente Donald Trump generó un intenso debate sobre los derechos digitales y la libertad de expresión. Aunado a estos procesos, estamos presenciando el paso de la red 4G a la 5G, con todas las implicaciones que esto tiene para el desarrollo digital en distintas áreas como la Internet de las cosas, la inteligencia artificial, el *blockchain* y la ciberseguridad, por mencionar unos ejemplos.

¿En dónde se encuentra nuestro país en esta denominada Cuarta Revolución Industrial (la revolución digital)? ¿Qué necesita implementar para incorporarse de manera exitosa en este cambio? ¿Cómo puede hacerlo sin ignorar la importancia de la inclusión social, el respeto al marco de derechos humanos y el desarrollo sostenible? En este libro se abordan estas y otras cuestiones que esperamos el lector encuentre relevantes para entender el momento histórico en el que nos encontramos. De esta manera, el libro tiene el objetivo general de revisar la situación actual, los desafíos y los pendientes que tiene el Estado mexicano en su política digital. El abordaje que proponemos da por sentado la necesidad de construir y ampliar la infraestructura de la red digital y subraya otros aspectos como el campo de derechos que ha emergido con la revolución digital, la inserción de nuestro país en la nueva economía digital, las tareas pendientes que tienen las diferentes entidades gubernamentales para mejorar y ampliar sus servicios, los retos crecientes que implican los ataques digitales a la seguridad nacional, así como oportunidades de innovación digital en el ámbito de las políticas públicas, entre otros aspectos.

Independientemente del futuro del entorno digital cuando concluya la pandemia, es un hecho que hoy ocupa un papel cada vez más central en la economía, la educación, el entretenimiento y en las propias tareas del gobierno. Por esta razón, México requiere diseñar e implementar políticas que favorezcan el desarrollo de la ciencia y la tecnología, garanticen el acceso a las tecnologías de la información y la comunicación (TIC) y fortalezcan las capacidades digitales de la población. Lo anterior se tiene que realizar en armonía con la diversidad cultural que caracteriza a nuestro país, de manera que se permitan cerrar las brechas digitales existentes que amplifican los diferentes fenómenos de desigualdad socioeconómica. Para no perder esta orientación normativa, consideramos útil enmarcar la presente discusión en un paraguas conceptual más amplio conocido como es la sociedad del conocimiento. En la presente introducción definiremos con mayor detalle a qué nos referimos con la sociedad del conocimiento y destacaremos otros aspectos que consideramos básicos para reflexionar sobre el presente y el futuro de la política digital en México.

¿DE QUIÉN ES LA RED? UNA APROXIMACIÓN A LA ECONOMÍA POLÍTICA DE INTERNET

El miércoles 6 de enero de 2021 la red sociodigital de Twitter decidió suspender la cuenta del entonces presidente de Estados Unidos de América, Donald Trump. Hasta ese momento, Twitter era la red favorita de Trump para dirigirse a sus simpatizantes y contrarrestar la información contraria a su persona, la cual definió sistemáticamente como noticia falsa. Mediante mensajes en esa red anunció durante todo su periodo de gobierno medidas para la política interior y algunas con implicaciones internacionales, principalmente para amenazar a otros países para obtener ventajas en sus relaciones bilaterales.[1]

Twitter decidió suspender temporalmente la cuenta de Trump tras un video en el cual parecía incitar a sus simpatizantes para que tomaran la sede del capitolio tras haber perdido las elecciones presidenciales del año 2020. Desde que los resultados preliminares le

1 Al respecto, véanse los resultados de la mesa de discusión organizada por el Instituto Belisario Domínguez sobre el tema "Aranceles y conflictos políticos en la relación México-Estados Unidos". Disponible en: http://bibliodigitalibd.senado.gob.mx/handle/123456789/4571

fueron adversos, Trump comenzó a enviar mensajes que atribuían su derrota a un fraude electoral. La comunicación fue subiendo de tono hasta la emisión de dicho video, justo el día en que el Senado ratificaría los resultados validados por el Colegio electoral de aquel país. La toma del Capitolio, sede del Congreso de Estados Unidos, representó para muchos analistas la antesala de un golpe de Estado o, al menos, de una crisis política con fuertes repercusiones para el régimen democrático. Dos días después, el viernes 8 de enero, Twitter decidió suspender de manera permanente la cuenta antes señalada "debido al riesgo de mayor incitación a la violencia" y "tras una revisión atenta de los tuits recientes de la cuenta @realDonaldTrump y del contexto alrededor" (BBC, 2021). Facebook e Instagram, que también le habían suspendido sus cuentas a Trump el día de la toma del Capitolio, decidieron mantener esta medida al menos hasta que se concretara el cambio de poder con Joe Biden.

La decisión de las redes sociodigitales dividió la opinión de la clase política, por un lado, estaban aquellos que la aplaudieron por considerar que estos mensajes propagaban información falsa e incitaban a la confrontación política con base en mentiras: "había que callar al tirano", señalaron estas voces: por otro, hubo personalidades de la política, tanto en la Unión Americana como en otros países, que identificaron la medida como un riesgo: "la cancelación de las cuentas fue una acción de empresas transnacionales y privadas que administran las redes bajo los propios términos y condiciones que han elaborado para regular las plataformas, sin que éstas hayan pasado por una revisión jurídica y legal por parte del Estado" (Watson, 2021). Por lo tanto, ¿quién regula estas acciones de las empresas, que inciden en definir quién tiene acceso a una audiencia masiva en línea? ¿Podemos confiar en que la censura de las empresas siempre se hará en aras del interés público? Sin lugar a dudas, estas interrogantes son centrales para abrir a una discusión colectiva sobre quién, qué y cuándo se puede bloquear o establecer filtros a la información que circula no sólo en las redes sociodigitales, sino en todo Internet.

La discusión es de una gran relevancia para el futuro de la sociedad digital. Principalmente, porque Internet ha ocupado un lugar central en las nuevas formas de comunicación política, las cuales han derivado en acciones colectivas de gran repercusión en el nivel internacional, como fue en su momento la denominada "Primavera

árabe" y la lucha feminista de nuestros días. También, de especial relevancia, como plataforma para personajes políticos que han visto en las redes sociodigitales una invaluable posibilidad de estar en permanente comunicación con sus simpatizantes y para contrarrestar los medios tradicionales de información masivos, como la prensa y la televisión. En ese sentido, dichas redes han modificado la manera de crear narrativas en las campañas políticas, establecer vínculos entre representantes y representados, así como en el procesamiento de conflictos en la arena política. Por esta razón, los Estados han visto con particular interés la necesidad de regular estos espacios. Los Estados de corte autoritario se refieren más a un control y monopolio de la red, mientras que aquellos de corte democrático hablan de una regulación que pueda salvaguardar el ejercicio de derechos civiles fundamentales como la libertad de expresión. Alcanzar una regulación dentro de un marco democrático no es una tarea sencilla y revela una tensión esencial: por un lado está la promesa inicial de Internet que consistía en plantear el flujo libre de información en todo el mundo, mientras que los Estados democráticos buscan la manera de respetar dicha promesa sin que su puesta en práctica constituya una amenaza al orden social, debido a la proliferación de noticias falsas y discursos de odio, por mencionar algunos ejemplos. Probablemente, la salida intermedia que decante dicha discusión tendrá que ver con un equilibrio entre la autorregulación corporativa y la regulación gubernamental, de manera que los términos y usos de las empresas sean transparentes para las personas usuarias y el Estado garantice que el marco jurídico en la materia esté en armonía con los criterios internacionales de derechos humanos. Al respecto, es importante advertir que no hay un consenso internacional sobre cómo alcanzar un punto intermedio entre el derecho a la información y el derecho a la libertad de expresión, los cuales suelen ser los que se encuentran en disputa cuando se busca regular las redes sociodigitales, de manera que cada Estado establecerá una alternativa, resultado de su contexto histórico y cultural.[2]

2 Al respecto, se puede consultar la síntesis que realizó el Instituto Belisario Domínguez sobre un evento organizado por el Senado de la República y el Instituto de Investigaciones Jurídicas de la UNAM, titulada "La regulación de las redes sociodigitales a debate". Disponible en: http://bibliodigitalibd.senado.gob.mx/handle/123456789/3809

Por otro lado, está la información, el insumo más valioso que circula por Internet. El valor que tiene para la toma de decisiones individuales y colectivas ha promovido un debate sobre el derecho al acceso y a la participación, pero también sobre los derechos de propiedad (robo, acceso desautorizado, violaciones, etcétera) y la libertad, aspectos que no siempre resultan fáciles de conciliar en los marcos regulatorios de la red. En ese sentido, la economía política de Internet requiere identificar a los principales actores que compiten por concentrar la mayor cantidad de información posible, así como los recursos estratégicos que utilizan para lograr tal fin, dentro de los cuales destaca, precisamente, su capacidad para incidir en la definición de derechos de acceso, propiedad y participación (Gandy y Neil Farrall, 2009).

Para comprender los orígenes e implicaciones de este debate es importante remitirse a dos hitos en el desarrollo de Internet (Bolaño y Viera, 2014). El primero se remonta a 1995, cuando la *National Science Foundation* de Estados Unidos cedió a la iniciativa privada el control y el desarrollo de la red. Esta transición se consideró exitosa en la medida en que logró mantenerse el principio de acceso gratuito a la red, aunque el modelo de gestión y desarrollo se mudó a los principios establecidos por una lógica económica de mercado. El segundo momento histórico corresponde a la especulación financiera que aconteció en el sector digital a comienzos del siglo XXI, el cual derivó en el crecimiento, las quiebras y las fusiones de empresas que resultaron en el escenario de oligopolios y gigantes corporativos que controlan el mercado digital en la actualidad. Justamente esta posibilidad de procesar y distribuir información es lo que permite que estas empresas obtengan ganancias económicas considerables a partir de dos actividades principales: la venta de espacios publicitarios en la red (forma de financiamiento ampliamente conocida por la industria cultural en el siglo pasado) y la obtención de información personal de usuarios de la red, la cual, una vez que es procesada por empresas especializadas en datos, es ofrecida a terceros para que puedan realizar una estrategia de mercadotecnia que pueda resultar atractiva a diferentes sectores poblacionales (Bolaño y Vieira, 2014). El acceso gratuito a los servicios de la red implica que las

personas otorgan libremente datos personales, lo que permite que se pueda conocer no solamente su perfil sociodemográfico, sino que, a partir de los propios rastros que deja la navegación, también sea posible tener acceso a las preferencias y gustos del internauta. Este aspecto es muy importante, ya que el valor económico de los datos personales no es algo intrínseco en los rastros que va dejando la navegación en Internet, sino que se requiere el procesamiento mediante empresas especializadas para ser ofrecidos como un servicio a otras compañías.

Al ser la información el principal recurso económico y estratégico que circula en la red, se ha configurado un nuevo escenario en donde diferentes organizaciones, tanto del sector público, como del privado, buscan la manera de establecer formas de concentración y control. En términos de la discusión que esto ha generado en el ámbito económico, se ha enfatizado que esta nueva arena de competencia de la sociedad digital ha transitado de considerar la información como un bien público a una mercancía. Esta es una discusión diferente a la del comercio electrónico que vende mercancías digitales o físicas mediante la ayuda de Internet; antes bien, se refiere a la nueva lógica de acumulación económica que se desarrolló en la Web 2.0, cuyo libre acceso y servicios gratuitos es posible a partir de vender espacios publicitarios y datos personales a otras empresas para que puedan afinar y dirigir sus estrategias de mercadotecnia de manera más específica (Fuchs, 2009: 81). Para ello se requiere rastrear, almacenar y analizar las actividades de las personas usuarias de la red. La recolección de toda esta información personal y la posibilidad de ponerla a disposición de terceros, sean estos actores privados o incluso gobiernos, ha generado un fuerte debate sobre la nueva dimensión de la vigilancia en la era de Internet (Hintz, Dencik y Wahl-Jorgensen, 2017).[3]

[3] El uso de datos personales con fines políticos en una elección fue un tema bastante señalado en Estados Unidos y en la Gran Bretaña a partir de la intervención de Cambridge Analytica, empresa que recolectó y sistematizó datos personales en las redes sociodigitales a partir de convenios con las empresas, con la finalidad de desarrollar una estrategia de comunicación política a solicitud de ciertos candidatos.

Estamos presenciando un momento muy importante en la construcción de la gobernanza digital, en donde el tema del control o filtro de información será un tema crucial. Resulta comprensible que los Estados tengan cierta incidencia en la información de la red para evitar la propagación de actividades criminales, como la pornografía infantil o la distribución de material que lesione social y culturalmente a un grupo en particular (mensajes de discriminación y racismo), por mencionar algunos casos. No obstante, para evitar que la regulación devenga en censura que afecte derechos civiles y políticos (práctica ampliamente utilizada en países de corte autoritario), las reglas para filtrar información deberían estar completamente especificadas en leyes que hayan resultado de una amplia participación de la sociedad civil; de lo contrario, persistirá un margen de discrecionalidad y opacidad en filtrar información para que predomine el interés de ciertos actores políticos o privados (Deibert, 2009). En este punto vuelve a ser relevante la rendición de cuentas y la transparencia sobre los controles que se ejercen para regular el libre flujo de información en la red.

En síntesis, durante los últimos 20 años, Internet se ha consolidado como un nuevo ambiente relacional con profundo impacto en todos los campos de la experiencia social. Se ha caracterizado por generar nuevas formas de realizar transacciones de manera más inmediata y global. En gran medida, este rol preponderante de la red para las interacciones contemporáneas descansa en la posibilidad de producir, almacenar y analizar una gran cantidad de datos; capacidades que se han concentrado en grandes actores corporativos. La importancia de regularlos radica en que tienen en sus manos información de carácter privada con un valor económico y político que va más allá de la intención original de los usuarios que originalmente confiaron dicha información a las empresas. Sin lugar a dudas, Internet ha representado una nueva área de política pública que busca resolver expresiones contemporáneas de problemas clásicos para los Estados liberales y democráticos, como la propiedad, la libertad y la participación política (Chadwick y Howard, 2009).

COVID-19: LA ACELERACIÓN DEL TRÁNSITO A UNA SOCIEDAD DIGITAL

La discusión general que plantea este libro sobre la importancia de tener una política digital robusta y actualizada para México parte de una premisa muy básica, la cual consiste en afirmar que el tránsito hacia una sociedad digital, que hemos presenciado desde la expansión global de las TIC a finales del siglo pasado, se aceleró notablemente a partir de la pandemia sanitaria de Covid-19. Dicho con otras palabras, la pandemia emergió en un momento histórico caracterizado por dos procesos: la globalización y el desarrollo de un entorno digital en el que las TIC tienen una función importante en todos los ámbitos de la vida cotidiana.[4] La globalización tuvo un papel fundamental en la propagación acelerada de la enfermedad, ya que la cantidad de viajes internacionales por avión, con fines comerciales y turísticos, no tiene comparación con ninguna etapa previa en la historia de la humanidad. Además, las TIC han sido una herramienta muy importante para mitigar los efectos que ha tenido el confinamiento exigido por autoridades de gobierno en prácticamente todos los países del mundo con el objetivo de ralentizar el contagio, pero también se han utilizado para diseñar políticas públicas que permitan superar la contingencia sanitaria con base en los avances tecnológicos. Por ejemplo, varios países han recurrido al uso de aplicaciones móviles, la analítica de datos masivos, robots, drones y la emergente red 5G como medidas para tener información que permita rastrear el comportamiento expansivo del virus SARS-CoV-2 mediante un monitoreo en tiempo real de estadísticas sobre personas enfermas, disponibilidad hospitalaria y análisis de la movilidad poblacional en centros urbanos, por mencionar algunos ejemplos (Agudelo *et al.*, 2020).

[4] El entorno digital consiste en el conjunto de infraestructura y dispositivos tecnológicos que han permitido generar, almacenar y procesar una gran cantidad de información. La portabilidad de esta información es cada vez mayor y se ha vinculado estrechamente con nuevas posibilidades de comunicación. Al incidir en los procesos comunicativos de la sociedad, el entorno digital se ha constituido como un nuevo espacio relacional para las interacciones y transacciones sociales en la esfera cultural, política y económica. El entorno digital también se caracteriza por una nueva configuración espacio-temporal que favorece las interacciones inmediatas y globales.

De esta emergencia sanitaria se pueden destacar tres aspectos relacionados con el entorno digital de la sociedad contemporánea. En primer lugar, la capacidad de resiliencia que permite la infraestructura digital. Aquellos países o sectores de la sociedad con mayor uso y conocimiento de las TIC, tuvieron la posibilidad de transferir más exitosamente sus actividades laborales, comerciales, educativas y de entretenimiento al espacio en el que realizaron su confinamiento. Esta población tuvo las condiciones óptimas para llevar a cabo el teletrabajo a partir de videollamadas, la búsqueda y el envío de la información; la posibilidad de completar el ciclo escolar mediante el uso de las diferentes plataformas en la que se gestiona la educación en línea e incluso la posibilidad de realizar la compra de víveres para evitar la exposición de los miembros de la familia en la adquisición de insumos básicos para su manutención. Sin lugar a dudas, los hogares equipados y conectados con las TIC tuvieron mejores condiciones para ajustarse a los desafíos que ha representado el confinamiento durante la pandemia. Ahora bien, en segundo lugar, si un hogar conectado tuvo mejores condiciones para enfrentar el confinamiento, también es cierto que la población que carece de Internet en casa, y no está suficientemente equipada, enfrentó el encierro desde la adversidad. Por ejemplo, las y los niños no pudieron realizar los trabajos que requerían recursos en línea, lo que impactó negativamente en su proceso de aprendizaje con respecto a sus compañeros que sí pudieron hacerlo. Una persona jefa de familia con una micro o pequeña empresa pudo explorar la comercialización de sus servicios en ventas electrónicas, mientras que un hogar desconectado tuvo que afrontar con mayor fuerza el paro económico y la subsecuente contracción del ingreso. En suma, la exclusión del entorno digital, amplificó en muchos casos la desigualdad socioeconómica prevaleciente, de manera que un hogar desconectado recrudeció su estado de marginación. Sobre este aspecto, volveremos más adelante.

En tercer lugar, se encuentra la incertidumbre que representa el futuro del entorno digital, particularmente en un país como el nuestro. Durante 2020, como un efecto secundario de la pandemia, se pudo apreciar el auge financiero de varias empresas que se dedican a comercializar servicios y plataformas digitales, como son aquellas dedicadas al comercio electrónico, a los servicios de almacenamiento en la nube, el entretenimiento en línea y los servicios de videconferencia, las cuales lograron una alza notoria en los mercados financieros.[5] La reconversión de los hogares a espacios multifuncionales para albergar el teletrabajo, la educación en línea y el entretenimiento, representó el incremento exponencial del número de suscriptores a este tipo de empresas que algunos analistas han definido como representantes de una nueva economía en el nivel planetario, como es el capitalismo digital (Ramonet, 2020). Independientemente de que se esté o no de acuerdo con el término, es un hecho que la configuración del mercado en las TIC se transformó por el auge de ciertas empresas digitales durante la emergencia sanitaria. ¿Este crecimiento seguirá después de que concluya la pandemia o será una burbuja que hará eclosión como parte de una crisis generalizada? Esta pregunta plantea una interrogante más amplia sobre el futuro del entorno digital. Algunas voces proponen que la digitalización de nuestra vida cotidiana era una tendencia manifiesta e irreversible antes de la pandemia, pero que recibió un impulso exponencial a raíz de la emergencia sanitaria. Desde otro ángulo, opiniones más moderadas consideran que cuando termine esta emergencia, algunos sectores regresarán a sus actividades presenciales con las mismas rutinas y prácticas previas a la pandemia. Resulta imposible hacer un pronóstico certero sobre qué escenario se cumplirá en el futuro; sin embargo, como parte del análisis se destaca la importancia de que los Estados retomen su agenda digital para crear políticas públicas que democraticen el acceso a Internet y al resto de las TIC, sin olvidar la necesidad de impulsar la construcción de capacidades digitales (Noreña, 2020).

[5] Las empresas que tuvieron un mayor crecimiento financiero durante la pandemia se pueden agrupar en aquellas que se dedican al comercio electrónico minoritario (Amazon, Paypal, Shopify y Mercado Libre), a la información tecnológica (Microsoft, Apple, Zoom y Adobe) y de servicios comunicativos o entretenimiento (Tencent, Facebook, Nvidia, Alphabet y Netflix) (Braithwaite, 2020a). Otras empresas "ganadoras" en esta pandemia están relacionadas con la industria farmacéutica, no sólo por la posibilidad de patentar una vacuna contra la Covid-19, sino también por todos los insumos médicos relacionados con su prevención y la atención hospitalaria (Braithwaite, 2020b).

EL PROBLEMA ESTRUCTURAL DE LA BRECHA DIGITAL

Desde la difusión masiva de Internet a finales del siglo pasado, se advirtieron los peligros que representa excluir a sectores de la sociedad de su acceso. Internet modificó la configuración espacio-temporal de la sociedad contemporánea, de manera que grandes cantidades de información circulan por esta red a una gran velocidad sin importar las distancias geográficas. La red de redes ha modificado la manera en que se llevan a cabo las interacciones sociales en las diferentes esferas de nuestra vida cotidiana, de modo que representa oportunidades para el conocimiento, la acción y las transacciones en procesos políticos, económicos, jurídicos, sociales y culturales (Castells, 2001). Por ejemplo, Internet constituye una herramienta que brinda oportunidades para la competitividad de cualquier empresa no solamente por la posibilidad de comercializar sus productos o servicios en línea, sino por la de vincularse a escala global con nuevos socios para innovar sus procesos productivos. En el caso de la administración pública, ha sido determinante para mejorar la comunicación con la ciudadanía y facilitar los trámites y servicios que se encuentran en el marco de sus atribuciones. En síntesis, Internet ha sido clave para detonar nuevas formas de interacción y organización en diferentes ámbitos de la sociedad a partir de favorecer el flujo inmediato de grandes cantidades de información sin importar las distancias geográficas. Esto ha dado la oportunidad de configurar redes relacionales que inciden poderosamente en actividades políticas, mercados económicos, iniciativas culturales y rutinas organizacionales en el gobierno, por mencionar algunos ejemplos. Dicho con otras palabras, si el acceso a fuentes de información y la posibilidad de generar conocimiento mediante el uso de dispositivos electrónicos conectados a Internet favorece la participación en el nuevo espacio que ha configurado el entorno digital, la falta de accesibilidad y de herramientas para utilizar dichas herramientas se convertirá en un nuevo factor de desigualdad con notorias implicaciones en la estructura socioeconómica.

La exclusión social al uso de Internet se ha definido como brecha digital, es decir, una asimetría de oportunidades en el acceso a las TIC y en el desarrollo de capacidades digitales para generar

conocimiento con estas herramientas. La brecha digital sigue constituyendo un reto para varios Estados que han carecido de una política digital robusta e inclusiva. Los efectos pueden observarse a escala internacional (diferencias entre países) y nacional (diferencias entre sectores poblacionales). En el primer caso se ha insistido en que la brecha digital global ha sido un factor determinante para que países o regiones geográficas no tengan la posibilidad de articularse a nuevas redes que son indispensables para generar conocimiento, innovación tecnológica y nuevas redes productivas. Al respecto, señaló Castells en el despunte de Internet en el nivel global que:

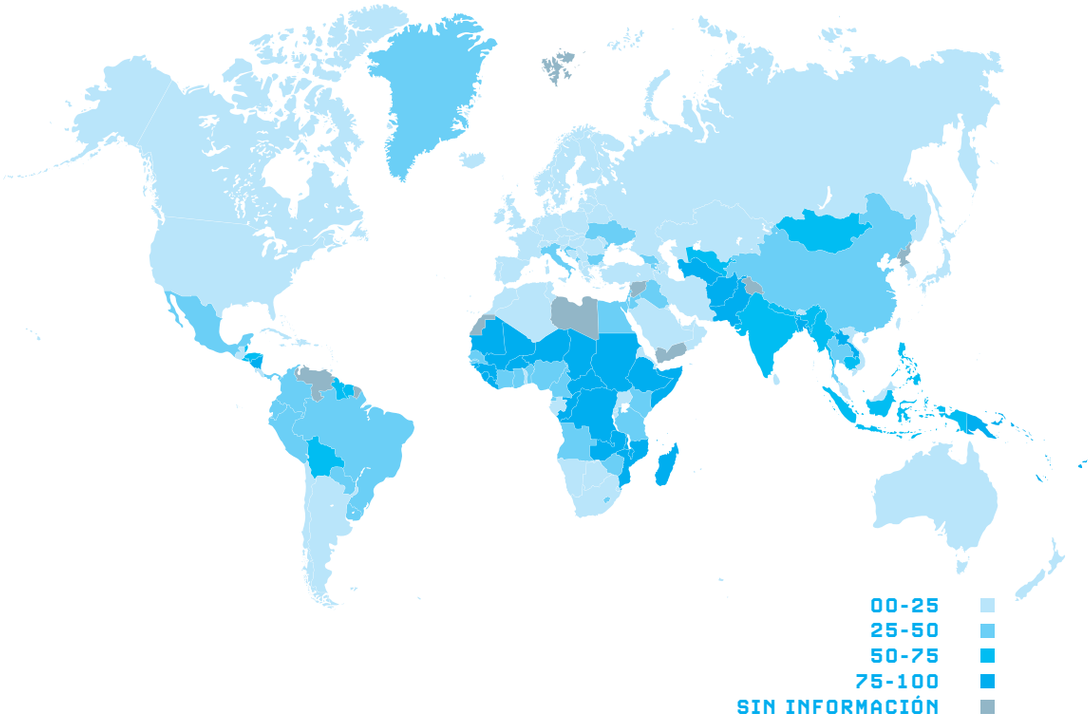
> Sin una economía y buen sistema de gestión basados en Internet, es prácticamente imposible que un país sea capaz de generar los recursos necesarios para cubrir sus necesidades de desarrollo, sobre una base sostenible, o sea, económica, social y ecológicamente sostenibles, como demuestra el informe de desarrollo humano de Naciones Unidades de 2001 (Castells, 2001: 298).

Veinte años después de esta afirmación, siguen resultando vigentes las consecuencias globales de estar desconectado. De acuerdo con cifras de la Unión Internacional de Telecomunicaciones (UIT), 53.6% de la población mundial era usuaria de Internet en el año 2019. Sin embargo, este promedio no muestra las importantes diferencias regionales. Los mismos indicadores de la UIT precisan que 86.6% de la población en el conjunto de los países desarrollados es usuaria de Internet, mientras que para los países en desarrollo el valor es inferior a la mitad de la población (47%). Una aproximación continental estima que en Europa 17.5% de la población no era usuaria de Internet, mientras que en América el indicador era de 22.8%; los países que conforman la Comunidad de Estados Independientes (CEI)[6] tenían el valor de 27.8%, los países árabes de 48.4%, Asia-Pacífico de 48.4%, y los países de África 71.8%. El siguiente mapa muestra estas tendencias mundiales.

6 Este conjunto de países está integrado por Armenia, Azerbaiyán, Bielorrusia, Kazajistán, Kirguistán, Rusia, Tayikistán, Turkmenistán y Uzbekistán. Para conocer la manera en que la itu integra el resto de las regiones, véase: https://www.itu.int/en/ITU-D/Statistics/Pages/definitions/regions.aspx

MAPA 01.

PORCENTAJE DE POBLACIÓN QUE NO ES USUARIA DE INTERNET, 2019



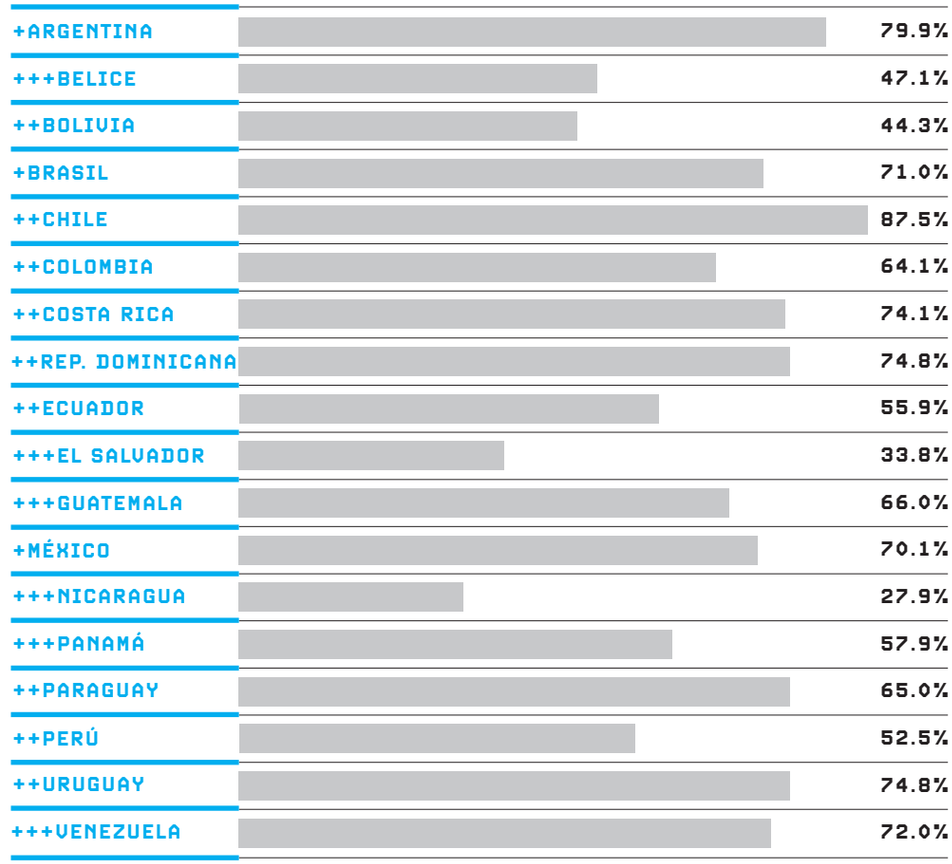
El porcentaje para la región latinoamericana se encuentra muy lejano del dato proporcionado por la UIT para el continente americano, debido a que el valor se eleva por los casos de Estados Unidos y Canadá. Una estimación realizada por CAF y el Banco de Desarrollo para América Latina, indica que aproximadamente 38% de la población latinoamericana no tienen acceso a Internet, esto es, cerca de 244 millones de personas en nuestra región (Noreña 2020). Si se exploran los datos con mayor nivel de detalle, se muestra nuevamente cómo al interior de América Latina hay diferencias importantes. En la gráfica 1 se aprecia que los países con la mayor cantidad de personas usuarias de Internet son Chile, Argentina y Uruguay. Aunque en Centroamérica se encuentran los valores más bajos para este indicador, destaca Costa Rica que tiene valores superiores a México, misma situación que acontece en el caso de la República Dominicana.

FUENTE:

estimaciones de la UIT, 2019. Disponible en: https://itu.foleon.com/itu/measuring-digital-development/offline-population/

GRÁFICA 01.

POBLACIÓN USUARIA DE INTERNET EN PAÍSES DE AMÉRICA LATINA, 2017, 2018 Y 2019



FUENTE:

elaboración propia, con base en datos de la UIT. *2019 / **2018 / ***2017

Guerra y Jordán (2010) afirman que la agenda digital de América Latina se caracterizó en una primera etapa por priorizar el avance en la construcción de infraestructura, la enseñanza de las TIC en la educación formal y en la gestión gubernamental. Posteriormente, se ha avanzado en definir una agenda más integral que no descuide los tres aspectos anteriormente señalados, pero también trata de incluir otras áreas, como la economía, la salud, la cultura y la gestión territorial, por mencionar algunas. En el caso mexicano, se ha tenido que discutir nuevamente el tema de su agenda digital, a raíz del inicio formal del nuevo tratado comercial con Estados Unidos y Canadá,

denominado T-MEC, el cual entró en vigor a partir de julio de 2020. El acuerdo comercial consolida una de las regiones con el mercado digital más grande del mundo y en él se incorporaron tres nuevos capítulos que son relevantes para la agenda digital de nuestro país: telecomunicaciones, comercio digital y propiedad intelectual.

En otro caso, la brecha digital que interesa destacar en la escala nacional es la existente entre los asentamientos rurales y los urbanos, debido a que suele ser la más fuerte. Normalmente la alta cobertura de Internet se encuentra en las ciudades, de manera que estos espacios han visto con mayor nitidez la transformación del nuevo espacio relacional favorecido por el entorno digital. De ese modo, son las urbes en donde se realiza la innovación tecnológica de las TIC y se produce la gran mayoría del contenido que circula en Internet. Este hecho ha favorecido que las ciudades amplíen sus ventajas comparativas en términos laborales, educativos y en prestación de servicios con respecto a las zonas rurales, las cuales han quedado desconectadas y a la retaguardia. Recordemos que los lugares con un déficit en infraestructura y capacidades digitales, se encuentran en una fuerte desventaja para difundir y vincularse a redes de conocimiento que les permita resolver sus problemáticas. Es verdad que el avance de otros dispositivos para conectarse a Internet, particularmente los teléfonos inteligentes o Smartphones, han incrementado el número de usuarios en las zonas rurales, pero no se ha avanzado con la misma velocidad en las capacidades digitales para procesar la información de Internet con ayuda de otras herramientas más sofisticadas como las computadoras.

La brecha digital entre ciudades y zonas rurales se incrementa en la medida en que las TIC se van transformando y van presentando nuevas innovaciones para procesar información. A las personas que no han tenido acceso les resulta mucho más complicado familiarizarse con un entorno digital, ya que las nociones básicas que puedan tener, son rápidamente superadas por los cambios que tienen los programas y los dispositivos electrónicos. Este desfase provoca que la persona no se pueda adaptar al entorno digital. Por esta razón, resultan indispensables las acciones que realizan los gobiernos para disminuir la brecha digital existente al interior de cada país, ya que sus esfuerzos tendrán consecuencias no solamente en la escala nacional, sino también en el escenario internacional.

HACIA UNA GUÍA NORMATIVA PARA LA POLÍTICA DIGITAL: LA SOCIEDAD DEL CONOCIMIENTO

El diseño e implementación de una política digital requiere identificar y promover consensos entre los múltiples intereses de actores económicos, políticos y sociales con respecto a la innovación, difusión y uso de las TIC. En principio, la articulación y obtención de estos consensos es lo que suele denominarse como gobernanza digital. Su logro es un proceso complejo por la cantidad de intereses y visiones antagónicas que se puede tener sobre el sentido del entorno digital. Desde nuestra perspectiva, un primer paso que puede favorecer la gobernanza es compartir una guía normativa que establezca un piso básico de valores para discutir el tema. En ese sentido, se propone recuperar los avances que se han hecho en el campo de la sociedad del conocimiento. Recapitulemos de manera sucinta el origen del concepto y sus postulados básicos.

Con el surgimiento y uso masivo de las TIC a finales de la década de 1990, diferentes analistas consideraron necesario definir el nombre de esta etapa histórica para diferenciarla del pasado y para establecer sus contornos analíticos. De esta manera, surgieron las propuestas de "sociedad red", "sociedad de la información" y "sociedad del conocimiento". De las tres acepciones, la que tuvo una mayor difusión inicialmente fue la de "sociedad de la información" (Tobón *et al.*, 2015; Krüger, 2006), por lo que inicialmente fue adoptada por organismos internacionales como parte de los estudios que diagnosticaban el avance de las TIC en el nivel mundial. No obstante, en el año 2005, la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO), prefirió referirse a este momento histórico como sociedad de conocimiento.[7] El cambio no fue únicamente

[7] Las primeras propuestas referentes a una sociedad del conocimiento como modelo de desarrollo se remontan a la década de 1960. Desde aquella época, diferentes científicos sociales como Peter Drucker (1969) y Daniel Bell (1973) señalaron que el conocimiento era una palanca de crecimiento y desarrollo económico, particularmente en los países postindustriales que se enfocaban en las actividades terciarias. Desde esta perspectiva, se propusieron diferentes alternativas para favorecer la ciencia y la tecnología a partir del aumento de la inversión en la educación superior, ya que se consideraba que el trabajo conceptual tenía mayor relevancia en la organización

de etiqueta, ya que este concepto tiene implicaciones más amplias que la importancia de mejorar la infraestructura tecnológica para subrayar las nuevas oportunidades y retos en el aprendizaje, el fortalecimiento de los derechos humanos y la sostenibilidad relacionados con el nuevo entorno digital (Mansell y Tremblay, 2015).

Mientras que el enfoque de la sociedad de la información se restringe a la rápida difusión de la tecnología y al aumento de la cantidad de datos que circula por las TIC, la sociedad del conocimiento retoma este proceso básico de innovación y propagación tecnológica en todos los aspectos de la vida social, pero lo vincula significativamente con las consecuencias y oportunidades que representa para el desarrollo humano y la capacidad de una comunidad para resolver problemas públicos. Información y conocimiento no constituyen sinónimos, forman parte de un proceso de aprendizaje en el cual la información (señales medidas en bits) constituye la primera etapa, la cual se interpreta para establecer relaciones y combinaciones posibles de manera organizada a partir de las habilidades cognitivas de las personas, proceso que deriva en la generación de conocimiento que le permite a una colectividad definir y resolver problemas para mejorar las condiciones de vida, tanto individuales como sociales, de acuerdo con los valores que predominan en un momento histórico determinado (Mansell y Tremblay, 2015; Balderas, 2009). Dicho con otras palabras, la acumulación de información no deviene automáticamente en conocimiento, la transformación es posible mediante el desarrollo de habilidades cognitivas que forman parte de un proceso de aprendizaje que permite darle sentido y significado a la información, así como orientarla para que cumpla cierta utilidad en un ámbito específico de la vida social, la cual puede ser incluso de carácter meramente estético y artístico.

laboral y era indispensable para resolver los problemas públicos mediante políticas basadas en mejor información. Desde aquellos primeros modelos de la sociedad del conocimiento se percibió una mayor amplitud en la desigualdad entre los países, ya que los desarrollados tuvieron mejores condiciones para concentrar a las mejores instituciones académicas y de investigación, lo que generalmente ha representado un polo de atracción a la mano de obra calificada como científicos y tecnólogos de países del Sur, como los de la región latinoamericana, que emigran para buscar mejores condiciones laborales y de vida (Marrero, 2007).

Con las premisas anteriores, resalta que para la sociedad del conocimiento las TIC no son un fin en sí mismo, sino que constituyen nuevas herramientas que pueden ser utilizadas para mejorar la calidad de vida de las personas. Las TIC permiten generar, almacenar, procesar y compartir una gran cantidad de información como nunca antes en la historia de la humanidad; sin embargo, para que se conviertan en un medio que contribuya a elaborar respuestas efectivas a las problemáticas complejas que afronta la sociedad contemporánea como son el cambio climático, la desigualdad o el crimen organizado, por mencionar algunas, se requiere de una perspectiva más amplia por parte de los Estados para que le den un sentido social a este tipo de tecnologías mediante políticas públicas que fortalezcan las capacidades cognitivas e intelectuales de las personas, así como la posibilidad de trabajar en red (Barroso, 2013; Pineda, 2009). Por esta razón, se ha enfatizado que las sociedades del conocimiento deben promover la educación de alta calidad en todos los niveles, no sólo por la importancia que tienen para el desarrollo de capacidades digitales, sino porque su puesta en práctica se incrusta en un marco de valores más amplios como pueden ser la diversidad cultural, la sostenibilidad y una cultura de paz. La sociedad del conocimiento involucra dimensiones políticas, éticas, sociales, económicas y culturales, ya que todas ellas tienen un papel importante en el desarrollo humano y en la calidad de vida de una colectividad.

La sociedad del conocimiento como aproximación conceptual para entender los efectos que ha tenido la revolución del entorno digital en diferentes prácticas sociales tiene dos vertientes, la primera más descriptiva que pretende identificar las transformaciones sociales, económicas y culturales de las TIC y otra de carácter prescriptiva que precisamente constituye una guía normativa para políticas públicas que incidan favorablemente en las capacidades cognitivas y pragmáticas de la población en la era digital. En ambos casos, se trata de un proceso en marcha, no de un estadio de la humanidad que se ha alcanzado plenamente, de manera que este proyecto en construcción está abierto a una revisión crítica sobre sus alcances y contornos.

El abordaje que se propone para entender el avance de la sociedad del conocimiento en el presente libro tiene un especial

énfasis en que su implementación se ancle en un marco de derechos humanos. Al respecto, se destacan algunos derechos civiles como la libertad de expresión; derechos políticos, como la participación en la vida cultural y social de una comunidad; así como derechos sociales, como el acceso a una educación que permita gozar de los beneficios del progreso científico (UNESCO, 2005). Con esta vasta base de derechos humanos –ampliamente discutidos y compartidos en marcos jurídicos internacionales y nacionales– la dinámica y las características particulares del entorno digital han incidido en la emergencia de derechos particulares, entre los cuales destaca el derecho a la privacidad, debido a la recopilación opaca de datos personales en la red, que suelen comercializarse a terceros para fines distintos a los originales o incluso para prácticas fraudulentas. Como señalamos anteriormente, la generación de datos masivos (*Big Data*) y de datos abiertos (*Open Data*) han generado un debate interesante sobre la manera en la cual debe regularse este tipo de información para salvaguardar la integridad de las personas. Este tipo de derechos específicos relacionados con el entorno digital se discutirán ampliamente en varios capítulos de este libro.

Nosotros queremos destacar tres principios normativos que consideramos relevantes cuando se trata de construir e impulsar una sociedad de conocimiento, a saber, el principio de inclusión, el de participación y el de protección de la diversidad cultural. Los tres están estrechamente relacionados, de manera que no se puede mencionar uno sin hacer referencia a los demás. El aspecto inclusivo se refiere a que ninguna persona o grupo social puede quedar marginada de los beneficios que ofrecen las TIC; por esta razón, se tienen que desarrollar programas que permitan la generación de capacidades digitales en todos los sectores de la población para que cada persona esté en condiciones de mejorar su calidad de vida con estas herramientas, de la manera que considere más conveniente, sin que esto ponga en riesgo la integridad y la seguridad de terceros. El derecho a la participación se vincula con los aspectos regulatorios de las TIC, esto es, con las condiciones de posibilidad para hacer uso apropiado de las mismas, que se contemplen en leyes y reglamentos, aspectos que deben estar abiertos a la opinión de todos los sectores (estatales, privados y sociales) que quieran expresar su voz y manifestar sus intereses. En este proceso deliberativo es que se

va construyendo un esquema de gobernanza que regula el entorno digital. Los problemas que puedan surgir con la propia evolución de las TIC, así como aquellos que se intentan resolver con ayuda de estas herramientas digitales que tendrían que resolverse de forma colaborativa, definiendo conjuntamente el diagnóstico y las estrategias para resolver las problemáticas detectadas.

El principio de pleno respeto y reconocimiento a la diversidad cultural es muy importante para un Estado como México. Con anterioridad señalamos que en la sociedad del conocimiento es muy importante fortalecer todos los niveles escolares en los que está organizado un sistema educativo. La construcción de capacidades mediante la educación formal favorece un contexto social que reconoce el valor público que tiene la ciencia y la innovación tecnológica para resolver problemas ambientales, económicos y sociales. Sin embargo, este planteamiento puede conducir a la conclusión errónea de que solamente el conocimiento científico resulta valioso. La sociedad del conocimiento tiene especial interés en incluir en los procesos de aprendizaje los saberes tradicionales que se encuentran en los diferentes grupos indígenas que hay en nuestro país. El filósofo León Olivé, quien tuvo un papel relevante en incorporar la discusión de la sociedad del conocimiento en México, fue enfático en este punto y señaló que el saber tradicional de los grupos indígenas es un conocimiento valioso que ha sido muy importante para resolver los problemas de sus comunidades (Olivé, 2007). Esta diversidad lingüística y cultural debe ser tomada en cuenta como una riqueza de la que abreva nuestro país para estimular el intercambio de saberes y construir conjuntamente diversos caminos de desarrollo que se amolden a las necesidades de cada grupo cultural.

> Promover la diversidad equivale a promover la creatividad de las sociedades del conocimiento emergentes. Esta perspectiva no obedece exclusivamente a un imperativo abstracto de carácter ético, sino que apunta principalmente a suscitar en cada sociedad una toma de consciencia de la riqueza de los conocimientos y capacidades de que es depositaria a fin de que los valore y aproveche mejor (UNESCO, 2005: 18).

El conocimiento tradicional de los grupos indígenas de México es parte del patrimonio cultural de nuestro país, el cual debe ser suficientemente valorado si queremos alcanzar una sociedad del conocimiento que, con el apoyo de las TIC, encuentre de manera colaborativa soluciones de los problemas complejos a los cuales nos enfrentamos. Estas alternativas se pueden construir y ser más ampliamente aceptadas si son resultado de esfuerzos colectivos elaborados de manera incluyente, participativa y basados en el reconocimiento de la diversidad cultural. Desde luego que implementar estos principios en leyes y políticas públicas concretas es un desafío; pero, en la medida que se utilicen como guía, estaremos más cerca de diseñarlas y de vigilar su cumplimiento. Como se desprende de esta idea, impulsar el desarrollo de una sociedad del conocimiento no está al margen de lo que sucede en la esfera política; por el contrario, los resortes para su concreción descansan en la existencia de un Estado democrático y de su correlato ciudadano caracterizado por una cultura política correspondiente con esta forma de gobierno. Desde una perspectiva sistémica es posible afirmar que, para lograr una sociedad del conocimiento, se requiere de un acoplamiento estructural entre los diferentes sistemas (político, social y cultural) que favorezca el empleo concreto del entorno digital para favorecer el desarrollo humano incluyente, participativo y respetuoso de la diversidad cultural.

PLAN DE LA OBRA

En el capítulo 1, Judith Mariscal Avilés y César Rentería Marín analizan de manera detallada la transformación que tuvo el sector de telecomunicaciones a partir de la década de los noventa, así como las políticas regulatorias y reformas en la materia que se han impulsado a partir de la introducción de la telefonía móvil, la Internet y las nuevas tecnologías. La revisión abarca cuatro distintos momentos en la evolución de la política digital del país: *1)* El *boom* de las telecomunicaciones, *2)* La introducción del Internet y la telefonía celular, *3)* Internet móvil y convergencia tecnológica y *4)* Tecnologías disruptivas emergentes. Para cada uno de estos momentos, los autores analizan el contexto nacional, las políticas que fueron introducidas y los efectos de éstas en la conectividad y la disminución de la brecha digital. El capítulo concluye con una revisión muy interesante sobre los resultados, las lecciones y la evolución de las políticas y reformas de telecomunicaciones que han sido introducidas en cada etapa.

El capítulo 2, escrito por el doctor Juan Pablo Aguirre Quezada, afirma que el rápido crecimiento en el número de personas que usan Internet en pocos años motivó la necesidad de crear leyes en diferentes países, a fin de regular el uso de las tecnologías de la información. En su escrito menciona que la *Declaración Universal de Derechos Humanos* de 1948, y la *Declaración y Programa de Acción de Viena* de 1993 son los fundamentos comunes en dicha regulación, pero además existen particularidades en las normatividades nacionales que delimitan la política digital. En su contribución el autor describe ciertas características de este tipo de ordenanzas en un conjunto de casos de estudio, como son Alemania, Brasil, Canadá, Colombia, Chile, España, Estados Unidos y México; a fin de generar una idea de los alcances y limitaciones existentes.

De los capítulos 3 al 5, la ciudadanía digital constituye el principal concepto de reflexión. Primeramente, Jimena Moreno González y Francisco Adrián García García proponen, en el capítulo 3, que hay suficiente evidencia sustantiva para afirmar que la ciudadanía digital tiene un gran potencial para el involucramiento en los asuntos públicos. No obstante, remarcan que es muy importante no pasar por alto las condicionantes en la estructura social que la hacen inaccesible a toda la población, y que están asociados a la brecha digital. Por tanto, el capítulo analiza qué es la ciudadanía digital y cuáles son las dimensiones desde donde se le analiza. Se estudia el alcance de la ciudadanía digital en la vida pública a partir de dos enfoques: desde un nivel de régimen, donde se identifican los principales elementos por los cuales la ciudadanía digital mejora la vida en democracia; y desde el nivel de gobierno, acotado a cómo el gobierno electrónico contribuye a la gestión eficiente de recursos públicos y algunas de sus principales implicaciones en materia de cumplimiento de derechos. En el capítulo 4, Ismene Ithaí Bras Ruiz analiza desde un enfoque complejo, ético y sociotecnológico, la relación entre la ciudadanía digital y la recopilación de información de plataformas digitales en tanto que pueden menoscabar la seguridad y los derechos fundamentales, principalmente de asociación, organización y libertad de expresión al usar los datos de uso y otro tipo de informaciones con finalidades

distintas, además de las de mercadotecnia. Bras Ruiz subraya que los Estados requieren garantizar la ciberseguridad de los ciudadanos de manera general, para lo cual considera de mucha utilidad revisar las conceptualizaciones y regulaciones de otros países o regiones en la materia, así como examinar las reglas éticas digitales que se establecen en el marco regional de América del Norte a partir de la entrada en vigor del tratado entre Canadá, Estados Unidos y México.

En el capítulo 5, Itzkuauhtli Zamora Saenz aborda los tipos de brecha digital y las consecuencias que tienen en nuevas formas de desigualdad y exclusión social. En este acápite el autor propone entender a la ciudadanía digital como un campo de nuevos derechos que le permite a la persona formar parte de la sociedad del conocimiento a partir del acceso y las capacidades para aprovechar la potencialidad que representan las TIC. El autor recupera algunos indicadores para entender la brecha digital que persiste en nuestro país en cuanto a la accesibilidad, el desarrollo de habilidades digitales y la participación política en redes sociodigitales. Con base en esta triada de indicadores, se afirma que la brecha digital es multiforme y constituye un obstáculo importante para el pleno ejercicio de este tipo de ciudadanía.

El capítulo 6, escrito por Alejandro Pisanty, representa la etapa final de la línea de trabajo sobre Ciberseguridad del proyecto LATAM Digital a la que fuera comisionado al autor en el año 2020. Presenta una visión de conjunto, orientada a una estrategia a futuro, centrada en un caso de estudio (México) en el contexto regional y mediante un análisis retrospectivo para la extracción de las lecciones más importantes aprendidas sobre el tema. Por su parte, Carolina Aguerre también contribuye, en el capítulo 7, a reflexionar desde su perspectiva sobre el tema central de la ciberseguridad. En dicho apartado se presenta una metodología para analizar la gobernanza de la ciberseguridad en el nivel nacional. Propone comprender a la ciberseguridad en un sentido amplio, es decir, abordando, a su vez, las problemáticas complementarias del ciberdelito y la ciberdefensa. La autora plantea una alternativa analítica, por un lado, a los modelos binarios de la gobernanza de Internet enfocados en el intergubernamentalismo *versus* el multisectorialismo y, por el otro, a los estudios que ponen el foco exclusivamente en los procesos de maduración de capacidades, descuidando el análisis de

los procesos de formación de preferencias por parte de los actores estatales, así como a las dinámicas que afectan a su convergencia y divergencia en los niveles nacional, regional y global.

Perla Carolina Gris Legorreta y Fernando Rocha Rosario son los autores del capítulo 8, en el cual se presenta una discusión sobre las condiciones que se requieren para transitar de la mera utilización de las TIC en la provisión de bienes y servicios públicos hacia su uso efectivo para establecer relaciones de intercambio entre los distintos actores que participan en el espacio público. Se incorpora un análisis conceptual de la democracia electrónica (e-democracia), así como de conceptos asociados, como son el gobierno electrónico, la participación y la gobernanza electrónicas. A partir de esta revisión teórica se identifica el estado del debate sobre estos temas. Asimismo, se discuten tres casos en los cuales se han utilizado las TIC para mejorar la interacción con la ciudadanía, esto permite identificar los desafíos que han tenido estos países en la implementación de estos modelos. En una temática coincidente, el capítulo 9, escrito por Aram Barra Ramírez y Pablo Collada Chávez, explora los principales avances en materia de participación ciudadana en México durante las últimas dos décadas, incluyendo los mecanismos de participación directa y las nuevas plataformas digitales y de infoactivismo. A través de esta revisión, los autores plantean una crítica constructiva y muy interesante que busca plantear caminos para la innovación en la participación ciudadana durante los próximos años.

Jaime Arturo del Río Monges y José Luis Clavellina Miller proponen, en el capítulo 10, que la economía digital ofrece diversas áreas de oportunidad para impulsar el desarrollo y el bienestar. En ese sentido, identifican que el uso de herramientas digitales para elevar la inclusión tanto financiera en zonas rurales, como de la población en situación de pobreza puede formar parte de una estrategia integral de combate a dicha situación. Sin embargo, la existencia de bienes y servicios intangibles que provee la economía digital y la falta de presencia física en un mercado o jurisdicción han dificultado el cobro de impuestos a las compañías digitales. Ante ello, la Organización para la Cooperación y el Desarrollo Económico (OCDE) ha planteado diversas propuestas encaminadas a reducir la elusión de impuestos que se revisan en este apartado. Los autores también pasan revista a las modificaciones legales

que ha realizado México para atender esta problemática, entre las que subrayan que impuestos ya existentes como el IVA y el ISR sean retenidos y pagados por estas empresas digitales.

El objetivo del capítulo 11, escrito por María Fernanda Viecens, consiste en identificar instrumentos de éxito que promueven la inclusión financiera. En este apartado se lleva a cabo una revisión de la literatura existente, con especial énfasis en la evidencia empírica. La autora hace un valioso esfuerzo por sintetizar lecciones aprendidas de la revisión de experiencias analizadas, las cuales considera que dan soporte al optimismo actual sobre el rol que las *Fintech* pueden tener como actores para promover la inclusión financiera. Finalmente, ofrece un marco de herramientas de política pública de las que disponen los gobiernos para asegurar las mejoras sostenidas en los indicadores de inclusión financiera en los países de la región latinoamericana.

En el capítulo 12, Lina Ornelas, comparte una serie de reflexiones a la luz de su experiencia en una de las empresas de innovación digital en Internet más importantes del mundo, la cual le permite al lector conocer, de una forma simple, los aspectos básicos del funcionamiento de la innovación basada en datos para su incorporación en cualquier tipo de organización. También destaca cómo la adopción o aplicación transversal de la innovación basada en datos, tanto en lo público, como en lo privado, pueden traer consigo una suma considerable de beneficios para amplios sectores de la población.

Hemos hecho un esfuerzo por sintetizar lo que a nuestro juicio son los aspectos más relevantes de todos los capítulos que se pueden recuperar para contar con un marco regulatorio flexible y pertinente a los principales cambios que se están llevando a cabo en esta revolución digital. Con el riesgo de simplificar la riqueza de cada uno de los capítulos, buscamos destacar los aspectos que articularon las diferentes reflexiones y propuestas de las y los diferentes autores de este libro.

Esperamos que los temas abordados en este texto sean una aportación importante a la discusión en nuestro país sobre la necesidad de una política digital robusta que sea el resultado y, al mismo tiempo, la promotora de un esquema de gobernanza en la materia que contribuya a disminuir la desigualdad y la injusticia social para alcanzar una efectiva sociedad del conocimiento. Para lograrlo, se requiere tomar en cuenta la voz y las condiciones concretas de diferentes grupos sociales, con especial interés en aquellos que se encuentran "desconectados" o al margen de los beneficios que representa el entorno digital. Aunque no haya una evidencia concreta y suficientemente probada sobre la relación entre la difusión de la tecnología digital y la disminución de la pobreza, la exclusión sistemática a la innovación y difusión tecnológica es un hecho que puede acentuar desigualdades estructurales (Mansell y Tremblay, 2015: 48). La construcción de una sociedad de conocimiento requiere de un fuerte compromiso por parte de las diferentes instituciones de gobierno para disminuir la desigualdad y la injusticia social. En aras de lograrlo, se requiere fortalecer un marco de derechos que favorezca el libre intercambio de información y que garantice la protección de los datos personales de las y los internautas. Para ello también será muy importante regular a los actores preponderantes en el sector y establecer medidas que eviten cualquier monopolio de la red. No se trata de ignorar o poner trabas a la innovación y desarrollo de las TIC que realiza el sector privado, como de garantizar alianzas público-privadas y reglas del juego que salvaguarden la libertad de expresión, la privacidad y la diversidad cultural que caracterizan a nuestro país, de manera que el contenido de la red no sea controlado y sesgado por intereses exclusivos de agentes privados o incluso gubernamentales. Evitar esta monopolización de propiedad y acceso, se convierte en una asignatura importante para la libertad política y civil en los Estados, pero también para salvaguardar la pluralidad cultural que los caracteriza.

BIBLIOGRAFÍA

Agudelo, M., Chomali, E., Suniaga, J., Núñez, G., Jordán, V., Rojas, F., Negrete, J., Bravo, J., Bertolini, P. y Katz, R. (2020).. *Las oportunidades de la digitalización en América Latina frente al Covid-19*. Santiago de Chile, Chile: CAF y CEPAL. Recuperado de https://bit.ly/3vwyRLI

Balderas, R. (2009). ¿Sociedad de la información o sociedad del conocimiento? *El Cotidiano* (158), 75-80.

Barroso Jerez, C. (2013). Sociedad del conocimiento y entorno digital. *Teoría de la educación. Educación y cultura en la sociedad de la información, 14*(3), 61-86.

BBC, Redacción. Twitter suspende a Trump permanentemente por el "riesgo de mayor incitación a la violencia". *BBC News Mundo*. Recuperado de https://bbc.in/3prinAE

Bell, D. (1973). *The Coming of Post-Industrial Society*. New York, Estados Unidos: Basic Books.

Bolaño, C.R.S. y Vieira, E.S. (2014). Economia Política da Internet e os Sites de Redes Sociais. *Eptic Online, 16*(2), 75-88.

Braithwaite, T. (2020). Prospering in the pandemic: the market winners. *The Financial Times*, 3 de julio.

Braithwaite, T. (2020). Prospering in the pandemic: the top 100 companies. *The Financial Times*, 18 de junio.

Castells, M. (2001). *La Galaxia Internet: reflexiones sobre Internet, empresa y sociedad*. Barcelona, Madrid: Plaza & Janés.

Castells, M. (2012). *Redes de indignación y esperanza: los movimientos sociales en la era de Internet*. Madrid, España: Alianza Editorial.

Chadwick, A., y Howard, P.N. (2009). Introduction: new directions in internet politics research. En A. Chadwick y P.N. Howard (Ed.), *Routledge handbook of Internet politics* (1-10). Londres y Nueva York, Estados Unidos: Routledge.

Christakis, N.A. y Fowler, J.H. (2010). *Conectados. El sorprendente poder de las redes sociales y cómo nos afectan*. Madrid, España: Santillana.

Deibert, R.J., Chadwick, A. y Howard, P.N. (2009). The geopolitics of Internet control: censoship, sovereignty, and cyberspace. En *Routledge Handbook of Internet Politics* (23-36). Londres y Nueva York, Estados Unidos: Routledge.

Deursen, A.J.A.M van, y van Dijk, J.A.G.M (2010). Measuring Internet Skills. *International Journal of Human-Computer Interaction*, (26), 891–916.

Dijk, J.A.G.M. Van (2009). One Europe, digitally divided. En A. Chadwick y Howard, P.N. (ed.), *Routledge Handbook of Internet Politics* (288-304). Londres, Inglaterra: Routledge.

Drucker, P.F. (1969). *The Age of Discontinuity*. Londres, Inglaterra: Heinemann.

Eshet-Alkalai, Y. y YAmichai-Hamburger, Y. (2004). Experiments in Digital Literacy. *Ciberpsychology & Behavior*, (7) 421-29.

Fernández V.A. (2019). Caminar en la era del smartphone. *Revista Mexicana de Sociología, 81*(4), 855-80.

Fuchs, C. (2009). Information and Communication Technologies and Society: A Contribution to the Critique of the Political Economy of the Internet. *European Journal of Communication, 24*(1), 69-87. doi: 10.1177/0267323108098947.

Gandy, O. H., y Farrall, K.N. (2009). Metaphoric reinforcement of the virtual fence: factors shaping the political economy of property in cyberspace. En A. Chadwick y P.N. Howard (ed.), *Routledge Handbook of Internet Politics* (349-63). Londres y Nueva York, Estados Unidos: Routledge.

Guerra, M. y Valeria J. (2010). *Políticas públicas de Sociedad de la Información en América Latina: ¿una misma visión?* Santiago de Chile, Chile: Comisión Económica para América Latina y el Caribe (CEPAL).

Hintz, A., Dencik, L. y Wahl-Jorgensen, K. (2017). Digital Citizenship and Surveillance Society. Introduction. *International Journal of Communication* (11), 731-39.

Krüger, K. (2006). El concepto de "Sociedad del conocimiento". *Revista Bibliográfica de Geografía y Ciencias Sociales, Geo Crítica, XI*(683). doi: 10.1344/b3w.11.2006.25676.

Mansell, R. y Tremblay, G. (2015). *La renovación de la visión de las sociedades del conocimiento para la paz y el desarrollo sostenible*. São Paulo, Brasil: UNESCO.

Marrero, A. (2007). La sociedad del conocimiento: Una revisión teórica de un modelo de desarrollo posible para América Latina. *Arxius*, (17), 63-73.

Mossberger, K. (2009). Toward digital citizenship: addressing inequality in the information age. En A. Chadwick y P.N. Howard (ed.), *Routledge Handbook of Internet Politics* (173-85). Londres, Inglaterra: Routledge.

Natal, A. Benítez, M. y Ortiz, G.. (ed) (2014). *Ciudadanía digital*. Ciudad de México, México: UAM, Unidad Iztapalapa y Unidad Lerma; Juan Pablos Editor.

Noreña, A. (2020). Tributo a Internet en la pandemia. *Reforma*, 17 de mayo.

Olivé, L. (2007). *La ciencia y la tecnología en la sociedad del conocimiento. Ética, política y epistemología*. Ciudad de México, México: Fondo de Cultura Económica.

Pineda, M. (2009). Desafíos actuales de la sociedad del conocimiento para la inclusión digital en América Latina. *Disertaciones. Anuario electrónico de estudios en comunicación social, 2* (1), 10-25.

Ramonet, I. (2020). La pandemia y el sistema-mundo. *La Jornada*, 25 de abril. Recuperado de https://bit.ly/35JkDMA

Tobón, S. Guzmán, C.E. Hernández, J.S. y Cardona, S. (2015). Sociedad del Conocimiento: Estudio documental desde una perspectiva humanista y compleja. *Revista Paradigma, XXXVI*(2), 7-36.

UNESCO. *Hacia las sociedades del conocimiento* (2005). París, Francia: UNESCO.

Unión Internacional de Telecomunicaciones (2020). ITU launches new study paper on broadband and connectivity solutions for rural and remote areas. *ITU News*. Recuperado de https://bit.ly/3C7XlMc

Watson, P.J. (2021). Merkel Says Big Tech Shouldn't Have Power to Decide Who Has Free Speech. *Summit.News*, 11 de enero. Recuperado de https://bit.ly/3hy7sAw.

CAPÍTULO 01

LA POLÍTICA DIGITAL EN MÉXICO: SIGUIENDO A LA INNOVACIÓN TECNOLÓGICA

JUDITH MARISCAL AVILÉS*
CÉSAR RENTERÍA MARÍN**

* Profesora investigadora del Centro de Investigación y Docencia Económicas (CIDE) y directora del Centro Latam Digital. Es miembro Nivel III del Sistema Nacional de Investigadores y especialista en cuestiones de política pública y asuntos regulatorios aplicados a las tecnologías de la información y comunicación (TIC).

** Profesor investigador del Centro de Investigación y Docencia Económicas (CIDE). Doctor en Administración y Políticas Públicas por la Universidad Estatal de Nueva York. Especialista en tecnologías de la información en organizaciones.

La transformación digital está cambiando nuestras economías y sociedades a un grado nunca imaginado. La dinámica innovación tecnológica ha generado una evolución constante del mercado de tecnologías de información y comunicación (TIC) desde finales de la década de 1980. Cada ola de innovación tecnológica trae nuevos actores relevantes y relega a otros, así como cambios en los retos de política pública; también vislumbra novedosas herramientas disponibles para enfrentar actuales y viejos desafíos. La Internet y especialmente la banda ancha, como tecnologías de propósito general, son ejemplos recientes de innovaciones que suponen cambios en la política digital.

Desde esta perspectiva, una revisión histórica de la política digital en México nos permite observar que el gobierno ha tenido que establecer reglas para enfrentar retos, en un marco tecnológico cambiante, donde las innovaciones se suceden unas por otras de manera constante. Por ejemplo, a finales de la década de 2000, el gobierno federal estableció políticas para la expansión de la red nacional de banda ancha en el país, mientras estaba ya considerando o estableciendo los retos que enfrentaría el sector en materia de asignación de espectro radioeléctrico para el impulso de la banda ancha móvil.

Para describir con claridad la compleja política digital en México, hemos seccionado la evolución histórica de este concepto en tres grandes transformaciones que ha sufrido el sector de telecomunicaciones. En cada cambio u ola, delinearemos los contextos nacional e internacional sobre los que se sustenta dicha política. Posteriormente, para cada una de estas etapas describimos las principales reglamentaciones que se diseñaron para hacer frente a las nuevas necesidades que se enfrentaron. Estas políticas se catalogan en tres tipos. Primero, el establecimiento de reglas del juego para entrar a ampliar el acceso a Internet, y particularmente al de alta velocidad, la banda ancha. Segundo, las regulaciones para enfrentar los desajustes de mercado en el sector. Y tercero, las políticas para contrarrestar las discordancias sociales en las posibilidades de acceso y uso de Internet, es decir, la brecha digital.

Nuestro análisis comienza con la primera gran transformación del sector de telecomunicaciones, que ocurrió a raíz de dos importantes cambios: uno global en el paradigma de política económica y la evolución tecnológica de las telecomunicaciones.

El primero tiene que ver con una ola de reformas en el ámbito internacional sobre el nivel de participación del Estado en la economía, marcados principalmente por los procesos de privatización y liberalización de mercados que históricamente constituían un monopolio del Estado. El cambio tecnológico principal fue el abaratamiento de la infraestructura de telecomunicaciones, que mitigó el argumento de monopolio natural sobre el que había operado históricamente el sector de telecomunicaciones. Desde entonces, sería viable, desde el punto de vista de la eficiencia económica, tener distintos proveedores en dicho sector.

Después de la liberalización del sector, la industria de las telecomunicaciones en México, como en la mayoría del mundo, experimentó un periodo de desarrollo sostenido: se adoptó una nueva generación de tecnologías, la inversión aumentó exponencialmente, al igual que la cobertura del servicio (en particular de telefonía móvil), y los precios al consumidor disminuyeron. Las TIC se convirtieron en una herramienta esencial para la economía, la política y la sociedad. Esta segunda transformación del sector, caracterizada por el *boom* de la telefonía móvil y la Internet, sentaron nuevos retos regulatorios, fundamentalmente la de políticas para ampliar el acceso a los servicios y mitigar la brecha digital.

La emergencia de la banda ancha afectó rápidamente las posibilidades de servicios públicos y comerciales que brinda la Internet y su expansión pronto se volvió una prioridad en los gobiernos en el nivel internacional. En México, tal como en otros países, esta urgencia de desplegar el acceso de banda ancha aunada a la necesidad de mitigar la brecha digital sugirió que la actividad del sector privado debía complementarse con una mayor intervención estatal para orientar las inversiones en banda ancha. Así, se generó un impulso para el despliegue de redes de acceso de nueva generación, que en muchos casos incluye inversiones públicas en la actualización, ampliación y habilitación de infraestructura de banda ancha (Galperin, Mariscal y Viecens, 2013a y 2013b).

En este capítulo detallaremos el contexto y la política nacional de cada una de estas tres transformaciones. El capítulo se compone de cinco secciones. En la primera, describimos la política digital correspondiente al fin del monopolio natural. En la segunda analizamos el auge de la telefonía móvil y de la Internet. En la

tercera discutiremos la política digital de banda ancha. Posteriormente, en la cuarta sección, describiremos los problemas crónicos presentes a lo largo de cuatro décadas de política digital nacional. Y finalmente, presentamos nuestras conclusiones sobre la evolución de la política digital nacional en nuestro país.

PRIMERA TRANSFORMACIÓN: FIN DEL MONOPOLIO NATURAL (DÉCADA DE 1990)

CONTEXTO

La primera gran transformación del sector inició en la década de 1980, cuando el panorama económico internacional comenzó a transitar de un modelo de intervención del Estado en los mercados a uno de apertura y desregulación. Esto respondió a un cambio en el paradigma de desarrollo: el de un Estado propietario a uno regulador, en donde el mercado se convirtió en el agente de desarrollo. Asimismo, las políticas económicas proteccionistas dieron paso a la liberalización del comercio.

Esta misma ruta de cambio fue seguida por el sector de telecomunicaciones. Desde su emergencia, a principios del siglo XX, este se caracterizó por constituir un modelo de producción basado en un monopolio natural. Esta noción hace referencia a situaciones en las cuales, frente a economías de escala y de alcance,[1] cada combinación de un bien se produce de manera más barata por una sola empresa que por muchas. En este contexto, existe mayor bienestar entre consumidores cuando un monopolio regulado es el proveedor de dicho bien. Así, la mejor configuración industrial era tener un productor único y las compañías telefónicas contaban con protección frente a la competencia (Mariscal, 1998). De hecho, las compañías de teléfono eran, a excepción del mercado de Estados Unidos (EUA), monopolios estatales.

1 En términos de teoría económica, se dice que existen economías de escala cuando el costo medio de producción en el largo plazo disminuye cuando se amplía el total de la producción.

Sin embargo, en el transcurso de la década de los ochenta, la innovación tecnológica provocó una convergencia entre los sectores de las telecomunicaciones y la informática, lo que generó cambios en la configuración del mercado. Dicha innovación tecnológica modificó las características de producción al disminuir las economías de escala y alcance, y reducir los costos de entrada en el mercado con la introducción de nuevos procesos de producción; la transmisión de información mediante fibra óptica y microondas, y la aparición de la telefonía celular, que ofrecían rendimientos superiores al cableado de cobre (Mariscal, 1998). Con la posibilidad de ofrecer el servicio por otros medios, la esencia de monopolio natural fue nulificada y con ello se dio la posibilidad de entrada al mercado de otras empresas que podían construir redes alternativas a más bajo costo, así como nuevos productos y servicios, como la telefonía móvil y la televisión por cable.

El nuevo panorama tecnológico promovió un replanteamiento de la regulación hacia esquemas fundamentados en la liberalización del sector y, en la gran mayoría de los casos, la privatización de empresas públicas de telecomunicaciones. No obstante, si bien hubo una convergencia mundial hacia la privatización de la compañía incumbente y crear un mercado, cada país llevó a cabo este proceso de forma diferente. El objetivo en común fue la privatización, pero las estructuras de mercado elegidas fueron muy diversas. Por citar algunos ejemplos, Argentina y Canadá se inclinaron por un modelo de monopolios múltiples, acotados por jurisdicciones regionales de servicios; India permitió la operación competitiva de proveedores privados de servicios básicos; y Estados Unidos promovió la competencia en el segmento de servicios locales, a la vez que permitió la participación de empresas de telefonía local en servicios de larga distancia con la condición de que existiera otro operador en las zonas en donde querían entrar (Mariscal, 2004). En México y el mundo, la primera gran ola de las innovaciones tecnológicas en el sector apareció a la vez que el concepto de desarrollo predominante en la época también se transformó. El paradigma de un Estado que debía intervenir ampliamente en el mercado dio lugar a la idea de un sector privado como agente del desarrollo.

Esta etapa de creación de mercado generó un círculo virtuoso de crecimiento; aumentaron la inversión, la adopción de nuevas tecnologías y también la asequibilidad de los servicios. Entre 1990 y 1999 se generaron incrementos considerables en la penetración de servicios de telefonía, de modo que para 1999 la mitad de los hogares contaba con ellos (IFT, 2020). Sin embargo, como era de esperarse, este crecimiento fue desigual tanto al interior de los países, como entre éstos. Las empresas invirtieron en donde era rentable hacerlo y los gobiernos alrededor del mundo no diseñaron, salvo pocas excepciones, una política de cobertura social lo suficientemente efectiva para aminorar la desigualdad en la adopción de las tecnologías de información y comunicación.

POLÍTICA DIGITAL NACIONAL

La política digital nacional siguió la tendencia mundial y consistió primordialmente en la creación del mercado de telecomunicaciones a través de la privatización y liberalización a la competencia de un sector que antes era un monopolio del Estado.

La aparición de la fibra óptica como un recurso de infraestructura esencial que potenciaba la provisión de telecomunicaciones y también optimizaba el servicio de electricidad en el país, dio lugar a la creación de la Red Troncal de Telecomunicaciones, a cargo de la Comisión Federal de Electricidad (CFE).

La primera reforma en el sector ocurrió durante el sexenio de Salinas (1988-1994) y fue parte de una agenda más amplia que buscaba transitar de Estado interventor en el mercado a uno de mercado como motor de una economía abierta. La reforma comenzó en 1990 con la privatización de Telmex, el monopolio del Estado en el sector de telefonía fija local y de larga distancia, y concluyó después de la instauración de los órganos reguladores de telecomunicaciones, en 1996, y el de competencia, en 1997.

Desde mediados de la década de 1980, la política económica mexicana se caracterizó por procurar una disciplina fiscal y una internacionalización del comercio y la inversión. De hecho, para 1986, los ajustes económicos estructurales se radicalizaron en México, en buena medida a raíz de la entrada del país al Acuerdo General sobre Aranceles Aduaneros y Comercio (GAAT, por sus siglas en inglés). Este cambio en el panorama económico implicó una transformación en las relaciones entre el gobierno y el sector privado, por lo que el mismo proceso de transición económica también se tradujo en un proceso de construcción de coaliciones políticas.

Telmex fue privatizada como una empresa integrada verticalmente.[2] Otras opciones fueron descartadas, como establecer monopolios regionales o separarla horizontalmente en servicios de telefonía local, larga distancia y celular. La visión de la administración durante el sexenio de Salinas (1988-1994) incluía el objetivo de integrar el respaldo de grupos clave en la amplia agenda de transiciones económica y política. En particular, el cambio hacia una economía abierta al comercio e inversión internacional dependía en gran medida del respaldo del sector empresarial con orientación exportadora y financiera. Pero también necesitó del apoyo del sindicato de telefonía. Por lo tanto, se decidió privatizar Telmex como una empresa integrada verticalmente, así como fortalecerla en términos financieros y regulatorios, con el fin de crear un "campeón nacional" que pudiera competir con las grandes compañías internacionales y, en particular, de Estados Unidos, que entrarían al mercado mexicano en 1996.

La liberalización del sector, sin embargo, fue parcial. Por ejemplo, el gobierno impuso un embargo temporal a la competencia del segmento de telefonía de larga distancia durante siete años. Al mismo tiempo, el de telefonía local permaneció sin competencia hasta 1998, porque las reglas de operación no se publicaron hasta ese entonces. Además, la secuencia en el proceso de reforma generó una institucionalidad precaria. No fue sino hasta 1995 cuando se creó la Ley Federal de Telecomunicaciones (LFT) y con ella el decreto para construir una agencia reguladora, la Comisión Federal de Telecomunicaciones (Cofetel).

En 1990, Telmex se privatizó sin contar con una ley sectorial ni con una agencia reguladora. De ese modo, fue hasta 1995 que la LFT abrió a la competencia todos los segmentos del sector y ordenó la creación de los órganos reguladores, en 1996, la Cofetel

[2] En términos de teoría económica, se dice que existen economías de escala cuando el costo medio de producción en el largo plazo disminuye cuando se amplía el total de la producción.

y el de la competencia, la Comisión Federal de Competencia (CFC), en 1997. La primera fue creada como un órgano desconcentrado del gobierno y su mandato estaba supeditado a la Secretaría de Comunicaciones y Transportes (SCT); no tenía la suficiente autonomía legal para establecer sus procedimientos de investigación y de toma de decisiones.

Si bien, la Cofetel tuvo limitaciones de diseño institucional para corregir los desajustes causados por un monopolio recién privatizado, el principal obstáculo para cumplir su tarea fue el lento y burocrático sistema de litigios. Por ejemplo, la mayoría de las empresas reglamentadas utilizaron amparos para suspender temporalmente las resoluciones regulatorias, mismos que podrían retrasar la acción regulatoria durante dos o tres años. Otro ejemplo fue la resolución de la CFC de 1997, declarando a Telmex como empresa con poder sustancial de mercado en cinco mercados relevantes: servicio local, larga distancia nacional e internacional, interconexión y reventa de servicios de larga distancia. Telmex presentó un amparo contra dicha resolución, el cual detuvo la acción regulatoria hasta que en 2007 el pleno de la CFC revocó sus resoluciones y cerró el expediente.

La forma en que se privatizó el mercado de la telefonía celular durante esta etapa se mostraría crucial en las décadas por venir. Este mercado inició en México en 1987, acorde con el modelo de los monopolios regionales —se establecieron nueve zonas en el país—. La empresa privada Telmex obtuvo la licencia sobre todas estas con condiciones de duopolio, es decir, cada región estaba abierta sólo a dos operadores–. En el momento de la privatización, este mercado era muy pequeño, incluso la infraestructura privatizada sólo cubría 34% del territorio nacional. Sin embargo, el drástico abaratamiento y optimización del desempeño de los teléfonos celulares y de la infraestructura de comunicación celular desencadenaron la masificación de este mercado y los inicios de la convergencia tecnológica.

El principal reto de la política nacional durante este periodo fue de índole regulatorio. Concretamente, el reto fue transitar hacia un mercado efectivo con una agencia encargada de ordenar a un otrora monopolio. La empresa dominante tenía una naturaleza dual de proveedor y competidor; por un lado, era poseedora de la red

esencial de telecomunicaciones (la red fija y la red de microondas) fundamentales para que todos los competidores pudieran conectar y terminar sus servicios de telefonía. Sin embargo, por otro lado, también era una empresa directamente competidora en el sector de servicios de telefonía. En este contexto, la principal barrera de entrada al sector fue una tarifa de interconexión[3] muy alta. Estas barreras de mercado no hicieron posible que se creara un mercado con competencia efectiva.

A pesar de ello, durante este periodo el sector creció sostenidamente. Un empuje fundamental a este incremento fue la masificación de la telefonía móvil desde finales de la década de 1990, que excedió cualquier expectativa. De acuerdo con la Unión Internacional de Telecomunicaciones (UIT. ITU, por sus siglas en inglés), en 2013 había 6.8 mil millones de suscripciones a servicios de telefonía celular en el planeta –que estaba muy cercano a la población global de aquel entonces, 7.1 mil millones de personas (ITU, 2013). En América Latina, la telefonía móvil tuvo una tasa de crecimiento considerablemente mayor que en el resto del mundo; en 2013, por ejemplo, el promedio de suscripciones fue de 166 por cada 100 habitantes. Casi todos los países de la región tenían una penetración por encima de los 100 suscriptores por cada 100 habitantes (Wireless Intelligence, 2013). Uno de los principales factores que explican la masificación de la telefonía móvil fue la modalidad de servicio de prepago, que permitió a personas sin acceso a crédito y sin estabilidad en sus ingresos acceder a un servicio de comunicaciones por primera vez. De igual forma, la política de "el que llama paga" también fue un factor de empuje a este crecimiento.

No obstante, la bonanza en el sector de las telecomunicaciones no tuvo los mismos efectos para toda la población, y se caracterizó por un alcance profundamente desigual. Las disminuciones en los precios y la modernización del servicio y la infraestructura se concentró en áreas urbanas, de modo que aquellas poblaciones donde no era rentable ofrecer el servicio, quedaban excluidas de

3 La interconexión se define como "Los acuerdos comerciales y técnicos bajo los cuales los proveedores de servicios conectan sus equipos, redes y servicios para permitir que los consumidores tengan acceso a los consumidores, servicios y redes de otros proveedores de servicios" (UIT, como se cita en OCDE, 2009).

sus beneficios. Al mismo tiempo, las políticas sociales orientadas a la disminución de desigualdades no tuvieron el impacto suficiente para cerrar estas brechas.

Aunque Telmex conserva la dualidad de ser operador de una red esencial y competidor, la convergencia tecnológica permitió a empresas con infraestructura de televisión por cable entrar en los servicios de telefonía local y de larga distancia con relativa facilidad, de manera que existe un traslape de múltiples redes esenciales. Sin embargo, treinta años más tarde, y como veremos más adelante, después de una segunda reforma de telecomunicaciones, las barreras de entrada al sector han disminuido, pero la concentración de mercado continúa siendo muy alta.

SEGUNDA TRANSFORMACIÓN: EL *BOOM* DE LA TELEFONÍA MÓVIL E INTERNET (DÉCADA DE 2000)

CONTEXTO

Fue en el periodo de finales de la década de 1990 e inicios de la de 2000 cuando el uso de Internet y de la telefonía móvil explotó en todo el mundo. Estos factores crearon nuevas posibilidades, nuevos servicios públicos y comerciales, así como nuevas dinámicas de comunicación e interacción social. Desde el punto de vista del gobierno, a la par de las nuevas oportunidades que podrían ser capitalizadas mediante políticas públicas, emergieron otros retos que atender.

La masificación de la red encuentra sus antecedentes en la aparición del *World Wide Web*, el sistema abierto de intercambio de información lanzado en 1989 y que catapultó el uso del sistema comúnmente denominado Internet. Sin embargo, la posibilidad de dicha masificación se debió principalmente a que este servicio podría ser provisto mediante la infraestructura existente de telecomunicaciones (tanto la infraestructura de telefonía fija, como la de televisión por cable).

Finalmente, aunque las preocupaciones por la desigualdad en el acceso a las telecomunicaciones antecedieron esta etapa, con la masificación de la Internet y sus aplicaciones sociales, gubernamentales y comerciales, emergió el concepto de *brecha digital*, que describe la desigualdad generada a causa de los potenciales beneficios del acceso y uso de Internet que no pueden gozar quienes están imposibilitados de ese servicio. La brecha digital reconoce no sólo la imposibilidad de acceder a Internet; sea por falta de oferta del servicio en sus lugares de residencia o por falta de ingresos para contratarlo, sino también la falta de habilidades computacionales para hacer uso efectivo de la Internet, cuando se dispone de este.

La brecha digital, sin embargo, pronto se concibió como un fenómeno multidimensional que incorpora más inequidades. Por ejemplo, el crecimiento de la importancia en el acceso y uso de la telefonía móvil amplió el entendimiento de esa brecha. Nuevas perspectivas sobre este problema social identificaron los perjuicios asociados con la desigualdad en el acceso a la telefonía móvil –además de la del acceso a Internet–. Tongia y Wilson (2007), por ejemplo, relacionan esta asimetría con costos de exclusión de los mercados laborales y explican que dichos costos están aumentando tan rápido como el crecimiento de las redes de telecomunicaciones. De Fontenay y Beltran (2008) conciben la brecha digital como una fuerza que limita la habilidad social de alcanzar una productividad más alta. La desigualdad en la adhesión a tecnologías de la información representa una barrera en el acceso a insumos para los procesos de producción, particularmente en el sector de servicios; de igual manera, distorsiona el desarrollo individual de competencias y oportunidades laborales.

La creciente importancia de la banda ancha se suma como una extensión conceptual de la brecha digital, ya que el grado de incorporación y aprovechamiento de los contenidos en Internet son distintos, según la calidad de conectividad con la que se cuente (Jordán, 2010). Por tanto, las políticas de acceso universal no sólo deberían conectar a las personas y desarrollar habilidades digitales, sino también asegurar la provisión de un ancho de banda que permita consumos de información –transmisiones de video en tiempo real, por ejemplo– e interacciones sociales remotas de alto valor económico y social –como la educación a distancia y la telemedicina.

POLÍTICA DIGITAL NACIONAL

Para promover la cobertura de la Internet móvil y la transición hacia tecnologías de banda ancha móvil más veloces y eficientes en el uso del espectro radioeléctrico, el gobierno mexicano emprendió una amplia *política de administración* del mismo, que es el insumo fundamental de la telefonía celular. En México, el ejercicio regulatorio en el proceso de asignación de espectro ha sido particularmente lento; esto se ha asociado a una inacción de la Cofetel y a una larga historia de amparos promovidos por las empresas del sector. El resultado fue que el espectro se convirtió en un insumo artificialmente escaso que no fue asignado al mercado de forma continua limitando la competencia y la inversión en el sector.

Quizá la política de telecomunicaciones más ambiciosa durante este periodo fue el *despliegue de banda ancha*. Durante el mandato del presidente Calderón (2006-2012), se diseñaron diversas iniciativas para promoverlo. Sin embargo, no fue sino hasta principios de 2012 cuando el gobierno integró las numerosas iniciativas existentes bajo el paraguas de dos grandes programas: el primero, "Acciones para el desarrollo de la banda ancha y de Tecnología de Información y Comunicación", se centra en la promoción de los servicios de telecomunicaciones, mediante el fomento de la inversión pública y privada en infraestructura, y, el segundo, "Agenda Digital.mx" en el desarrollo de la demanda de servicios, fomentando la adopción y uso de TIC. La visión general tenía cuatro objetivos principales: promover la inversión en infraestructura en servicios de banda ancha a través de México, reducir el costo de dicha banda, aumentar la alfabetización digital, y promover la demanda de servicios.

Entre las iniciativas más importantes adoptadas por el gobierno del presidente Calderón, destaca una licitación para la explotación de capacidad no utilizada de la red troncal de fibra óptica propiedad de la CFE, la empresa eléctrica de propiedad estatal. La red de fibra óptica de la CFE extiende más de 34 000 kilómetros, con 36 pares de hilos de fibra, de los cuales sólo fueron licitados dos (Mariscal y Flores-Roux, 2009). La convocatoria establece un periodo de 20 años, durante el cual el operador seleccionado deberá realizar inversiones complementarias para aumentar la cobertura y capacidad de la red.

La administración del presidente Peña Nieto (2012-2018) lanzó una ambiciosa reforma constitucional a la LFT, que fue aprobada en 2013. El corazón de la mejora fue fortalecer la autonomía y las capacidades regulatorias de la agencia del sector. Pero la reforma fue más allá de empoderar al regulador, ya que consideró también un plan de banda ancha en el que se encomendó a la empresa paraestatal Telecomm-Telégrafos la ampliación de la red troncal de fibra óptica de la CFE y el despliegue de una futura red de banda ancha móvil basada en la banda de 700 MHz, denominada Red Compartida.

El retorno del Estado, planteado en la reforma de 2012 en términos de inversión, no fue, sin embargo, un regreso a los modelos de gasto público de antaño. La corrección contempló una visión contemporánea de inversión pública mediante la creación de asociaciones público-privadas y con un fuerte componente de mandatos de compartición de infraestructura. Dicha compartición fue una estrategia innovadora para poner a disposición de los operadores de telecomunicaciones infraestructura pasiva lista para instalar redes o equipos de telecomunicaciones. De esta manera, por ejemplo, las empresas tienen acceso a mástiles, antenas, gabinetes y otros equipos de telecomunicaciones, además de la compartición de un sitio ubicado y adecuado para la prestación de servicios. Los principales sujetos mandatados para compartir su infraestructura pasiva fueron las mismas entidades de gobierno (por ejemplo, edificios o vías de comunicación) y los operadores declarados dominantes o preponderantes –como parte de las medidas de regulación asimétrica.

La mayoría de los casos en el nivel internacional son de compartición de redes troncales para el despliegue de fibra óptica. En España, por ejemplo, la empresa Administrador de Infraestructuras Ferroviarias (Adif) licitó una red de fibra óptica que se extiende a lo largo del tendido ferroviario de ese país. Pero también hay casos de infraestructura de red urbana como en París y Londres donde se utiliza la red de alcantarillado para instalar redes de fibra óptica en toda la ciudad, con lo cual se logra entregar servicios al hogar o al edificio.

La principal política de telecomunicaciones concerniente a la corrección de desajustes en el mercado fue la *regulación*

asimétrica de las tarifas de interconexión, que es una herramienta para contrarrestar el poder del operador propietario de las mayores redes –otrora monopólicas– de telefonía fija y celular. Desde finales de los noventa se comenzaron a utilizar medidas de ese tipo para equilibrar las fuerzas de competencia de las empresas rivales en el mercado de la telefonía móvil en contextos donde existe una empresa con poder sustancial de mercado. Si bien, la regulación asimétrica se compone de distintas medidas, las tarifas de interconexión asimétrica tienen una relevancia especial para acelerar la penetración de mercado de los operadores entrantes para conseguir, en el mediano plazo, un mercado competido entre empresas relativamente equilibradas en términos de cuota de mercado.

En México, las tarifas de interconexión resultaron del acuerdo entre los propios operadores, lo cual ocasionó que, durante la mayor parte de las décadas de 1990 y 2000, fueran altas, convirtiéndose en una gran barrera para la competencia. La reforma de telecomunicaciones de 2012 impuso medidas de regulación asimétrica.

La mejora le otorgó al nuevo Instituto Federal de Telecomunicaciones (IFT) la capacidad para determinar la existencia de empresas con poder sustancial de mercado.[4] Las medidas de regulación asimétrica impuestas en la reforma son amplias, incluso, aun cuando estas se han instrumentado en otros países, en ninguno se han implantado todas a la vez. Algunas de estas medidas generan condiciones no sólo para una mayor competencia, sino para una mayor eficiencia en el mercado. La eliminación de *roaming* nacional y la compartición de infraestructura pasiva apuntan en esa dirección.

[4] Para ello, la reforma consideró dos mecanismos de determinación. Primero, la regulación *ex ante*, en la cual se creó la figura de empresas "preponderantes", que son las que cuentan con más de 50 por ciento de suscriptores, mientras que la figura de poder sustancial de mercado (el mecanismo *ex post*) será resultado de una investigación detallada de la competencia en el sector. El concepto preponderancia se puede entender como una estrategia para ejercer acción regulatoria inmediata sobre las empresas (en telecomunicaciones y radiodifusión) que desde hace muchos años han tenido poder sustancial de mercado en México y no han podido ser disciplinadas. Sin embargo, esta noción representa una medida estructural que no informa sobre poder sustancial de mercado, sobre prácticas desleales ni cuenta con un debido proceso de investigación.

Sin embargo, la desagregación del bucle local[5] parece haber llegado demasiado tarde. Esta es una política regulatoria implementada en otros países durante la década de 1990 –y correspondiente a las soluciones de la primera ola de cambios tecnológicos discutidos en la sección anterior de este capítulo–. El resultado inmediato de estas disposiciones fue la decisión del operador declarado preponderante en telecomunicaciones, América Móvil, de desincorporar sus activos para evitar la regulación asimétrica.

Finalmente, la respuesta del gobierno ante la emergente brecha digital se reflejó en una diversificación de las *políticas de acceso universal*. Los Centros Comunitarios de Aprendizaje constituyeron el primer esfuerzo por combatir la brecha de acceso y adopción. Esta política del sexenio del presidente Vicente Fox (2000-2006) instaló equipos de cómputo con conectividad en espacios públicos de localidades con alto grado de marginación. El objetivo del programa fue brindar capacitación a distancia para fortalecer el desarrollo individual en lo laboral y lo social. Un segundo proyecto en esta línea fue el programa Habilidades Digitales para Todos, cuyo objetivo fue desarrollar habilidades de cómputo en los estudiantes de educación básica.

La reforma de 2012 impulsó una ambiciosa agenda de digitalización en el país, representada principalmente en el decálogo del Programa de Conectividad Digital. Es en este plan en el que se enmarcaron los esfuerzos más recientes para mitigar la brecha digital. En general, la estrategia nacional para combatirla dependía más bien de la mejora de las condiciones de acceso a raíz de los beneficios brindados por la Red Compartida y los cambios en las políticas de asignación de espectro. Se destacan, sin embargo, dos programas ligados directamente con la brecha digital, que fueron México Conectado –un programa para brindar acceso gratuito a Internet en sitios públicos– y los Centros de Inclusión Digital –que ofrecen cursos de alfabetización digital, robótica, mecánica y programación.

[5] La desagregación del bucle local es la posibilidad de que una empresa pueda arrendar la infraestructura de red (o una parte de ella) de una empresa.

TERCERA TRANSFORMACIÓN: BANDA ANCHA (DÉCADA DE 2010)

CONTEXTO

Una vez que la cobertura de Internet alcanzó gran amplitud, el reto de inversión se trasladó a la necesidad de ampliar la capacidad de transmisión de la Internet, para lo cual sería importante reemplazar componentes de la infraestructura física existente. Desde mediados de la década de 2000, conforme Internet ya se había establecido como una tecnología de uso masivo, la preocupación por *desplegar Internet de banda ancha* [6] comenzó a dominar el panorama de la política digital en distintas partes del mundo. Las regulaciones orientadas en este sentido estuvieron motivadas principalmente por la creciente evidencia sobre la contribución de las telecomunicaciones, en particular de banda ancha, sobre el crecimiento económico y la creación de empleo (Koutroumpis, 2009; Czernich *et al.*, 2011). La infraestructura de telecomunicaciones siempre ha estado vinculada con el crecimiento económico (Hardy, 1980; Leff, 1984). Sin embargo, esta nueva evidencia demostró el efecto positivo de la adopción de banda ancha en la competitividad y el empleo, lo que ha creado un sentido de urgencia sobre la aceleración de desarrollo de dicha banda. Además, las inversiones durante las últimas dos décadas han favorecido, como se esperaba, las áreas urbanas con el mayor ingreso per cápita, agravando así las disparidades existentes en el acceso a los servicios (Grazzi y Vergara, 2011).

[6] La banda ancha es un concepto altamente idiosincrático y en constante cambio. Debido al rápido cambio tecnológico y la variación de condiciones y necesidades entre los países, es difícil llegar a un consenso estable sobre cuál es la velocidad mínima de transmisión de datos para considerar una conexión como de banda ancha. No hace mucho tiempo, por ejemplo, la Unión Internacional de Telecomunicaciones (UIT) en su Recomendación I.113 considera banda ancha a la capacidad de transmisión mayor que 1.5 Mbps. Por otro lado, la Federal Communications Commission (FCC) de EUA la definió como la transmisión de datos a una velocidad mayor a 200 Kbps. Actualmente, otras explicaciones parten de las capacidades que pueden ofrecer las redes de nueva generación y las aplicaciones emergentes de Internet (por ejemplo, la 4K TV). En enero de 2015, la FCC actualizó su definición de banda ancha de 4 Mbps a 25 Mbps. La Comisión de Regulación de Comunicaciones en Colombia está en proceso de cambiarla y podría pasar de 1024 Kbps (Resolución 2352 de 2010) a 4 Mbps o 20 Mbps.

Al igual que el papel clave del Estado para desplegar las redes eléctricas, de transporte y de las telecomunicaciones en el pasado, un nuevo consenso parece llamar a los gobiernos a asumir un papel similar en la modernización de la infraestructura de telecomunicaciones en el siglo XXI. Esta oscilación de péndulo, entre el alejamiento del Estado durante las décadas de 1980-1990 y su regreso a finales de la de 2000, es el resultado de cambios en las condiciones macroeconómicas y el consenso prevaleciente sobre el papel del gobierno en la economía (Vietor, 1994; Mariscal, 2002; Cowhey y Aronson, 2009; Bauer, 2010).

Existen varias razones que justifican la intervención del Estado en la promoción del acceso a la banda ancha. En primer lugar, la reducción de los incentivos para la inversión privada, como consecuencia de la crisis de 2008, producto del efecto combinado de una desaceleración de la demanda de servicios de telecomunicaciones y una contracción del crédito disponible (Katz, 2009). El ciclo de las políticas destinadas a promover la desregulación y la privatización de los operadores estatales, que se inició en América Latina a finales de 1980, estaba mostrando claras señales de perder impulso a mediados de la década de 2000. A primera vista, esto puede parecer sorprendente en la medida en que el ciclo de liberalización provocó un aumento significativo de la cobertura del servicio, un incremento exponencial de la inversión en telecomunicaciones, y un círculo virtuoso de la introducción de nuevas tecnologías y la adopción generalizada de nuevos servicios (Estache *et al.*, 2002; Jordán *et al.*, 2010). Sin embargo, en un contexto de incertidumbre económica mundial, los operadores privados han sido reacios a hacer grandes inversiones en nuevas infraestructuras de red (en particular, las inversiones de alto riesgo y baja rentabilidad esperada, tales como expandir la red troncal de fibra óptica fuera de los grandes centros urbanos). En segundo lugar, en otros servicios basados en redes de infraestructura física (energía, agua, ferrocarriles, por mencionar algunos), las telecomunicaciones funcionan como *servicios públicos* [7] para la economía.

[7] Un *servicio público* (también denominado en inglés *public utility*) es considerado una actividad económica necesaria para el interés público, por lo que podrían considerarse servicios que son públicos por naturaleza.

También, Cave y Martin (2010) señalan otros motivos de promoción de la banda ancha por parte del Estado, tales como equidad, impulso industrial y dinamización de la economía.

A principios de la década de 2010, la banda ancha apareció en la agenda de gobierno de la gran mayoría de los países, tanto industrializados como en desarrollo, tal como lo evidencia la proliferación de planes nacionales de banda ancha que contemplan algún tipo de intervención del Estado para el aceleramiento de su despliegue. En 2005, sólo 21 países en desarrollo tuvieron un programa de acceso universal, mientras que en 2010 más de dos terceras partes de 144 países considerados en desarrollo tuvieron un plan de banda ancha o un programa de acceso universal (Broadband Commission, 2012).

En cuanto a los planes de banda ancha en América Latina, se observan numerosas similitudes en el diagnóstico de la situación, las motivaciones y los objetivos perseguidos. Uno de los principales consensos en este sentido es la limitación de redes troncales nacionales de fibra óptica para el despliegue de banda ancha. Las diferencias importantes, sin embargo, surgen en cuanto a los instrumentos de política elegidos por los gobiernos en la expansión, precisamente, de las redes nacionales de fibra óptica. Algunos países han optado por la intervención preponderante del Estado, aportando capital de inversión para la infraestructura o incluso incorporando la operación de dichas redes a la actividad gubernamental.

Un segundo cambio importante durante este periodo fue el abaratamiento de tecnologías de *Internet móvil*, como los teléfonos inteligentes y las redes de transferencia de datos LTE, que han contribuido a la democratización del acceso a Internet por vía de la banda ancha móvil (Mariscal, Gamboa y Rentería, 2014). En los países en desarrollo, la telefonía móvil ha sobrepasado considerablemente a la fija como el principal medio de comunicación. Incluso, se estima que la móvil tenga un efecto dos veces más grande en el crecimiento económico en países en desarrollo, en comparación con naciones industrializadas (Waverman, Meschi y Fuss, 2005). Esto se debe principalmente a las dificultades de desplegar redes alámbricas de telecomunicaciones, tanto interurbanas como intraurbanas, en las vastas zonas rurales de la región.

La tendencia de crecimiento de la banda ancha móvil, más la marcada estabilización de la banda ancha fija en número de suscripciones y la capacidad de transmisión de datos de las redes 4G, ponen de manifiesto que dentro de unos pocos años el debate sobre el acceso a Internet será primordialmente sobre medios inalámbricos. La banda ancha móvil se ha convertido en el principal medio de conexión a Internet en los países de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) desde 2008 y de América Latina desde 2010.

La banda ancha móvil ofrece una oportunidad única para dar acceso de alta velocidad en países en desarrollo. Esta plataforma no requiere de la cuantiosa inversión necesaria en infraestructura que demanda la banda ancha fija para su despliegue y puede alcanzar velocidades de transmisión de datos importantes. Las redes con tecnología LTE, conocidas comúnmente como 4G alcanzan velocidades alrededor de los 20 Mbps, aunque el límite teórico de su velocidad es de 1 Gbps. La banda ancha móvil no depende de una infraestructura dedicada por cliente y cuenta además con una gran ventaja: su ubicuidad.

Por lo tanto, la universalización de la banda ancha y la mejora de su capacidad de transmisión en países en desarrollo (que no cuentan con la capacidad de inversión o de atracción de la inversión suficientes para establecer redes nacionales de fibra óptica o redes FTTH)[8] quizá dependan principalmente del aumento de la cobertura de redes celulares y la evolución en el corto plazo hacia tecnologías 3G y 4G (Mariscal, Gamboa y Rentería, 2014).

Más aún, la población de bajos recursos usa equipos móviles poco sofisticados para conectarse a Internet y acceder a información que contribuye a eliminar obstáculos que enfrentan cotidianamente (Samarajiva y Zainudeen, 2008; Donner, 2008). El teléfono móvil está ganando cada vez más importancia como plataforma para promover el desarrollo en campos diversos como el económico, el social y el político, y en temas clave como agricultura, salud, educación y finanzas.

Para que la banda ancha móvil pueda brindar los beneficios potenciales de la adopción a Internet se requieren redes inalámbricas.

8 FTTH es, por sus siglas en inglés, la forma común para referirse a las redes de Fibra al Hogar (*Fiber To The Home*).

Para ello es necesario asignar eficientemente el espectro radioeléctrico; éste es el insumo básico para el desarrollo de dichas redes para servicios de voz y datos. Actualmente, la penetración de telefonía móvil en México es la menor de América Latina, exceptuando el caso de Cuba.

Por otro lado, el Internet se ha vuelto un espacio social, colaborativo y móvil. En 2001, se fundó Wikipedia, un sitio de Internet en el cual las personas pueden crear colaborativamente artículos de enciclopedia. En 2004 y 2005, respectivamente, se fundaron freelancer.com y Amazon Mechanical Turk, los primeros sitios de contacto directo entre empresas y profesionistas para subcontratar masivamente actividades de alguna de ellas. En 2006, Google compró una *startup* especializada en almacenar y reproducir videos compartidos por las personas (YouTube). En 2004 y 2006 se fundaron Facebook y Twitter, respectivamente. En 2007 se lanzó el iPhone, el primer teléfono inteligente y Netflix comenzó su servicio de transmisiones. A finales de 2009, Internet ya era social y móvil.

Estas innovaciones cimentaron nuevas dinámicas de interacción en la red durante la década de 2010; la Internet es un espacio social, colaborativo y móvil, con un consumo intensivo de transmisiones de video en vivo. La convergencia tecnológica y el desarrollo de la banda ancha han dado lugar a la emergencia de servicios conocidos como Over-The-Top (OTT), los cuales proveen audio, video y otros medios audiovisuales a través de la Internet, compitiendo directamente con los servicios tradicionales de las empresas de telecomunicaciones y radiodifusión. Los servicios OTT son un espacio de innovación en el contexto actual, pero hasta el momento se pueden englobar en tres grandes categorías: la televisión por protocolo de Internet (IPTV), por ejemplo, Netflix; los servicios de voz por protocolo de Internet (VpIP), por ejemplo, Skype; y los servicios de mensajería multimedia instantánea, por ejemplo, WhatsApp.

La Internet social y móvil más la disponibilidad de banda ancha son terreno fértil para la proliferación de servicios de telecomunicaciones OTT, mismos que están creciendo a una tasa acelerada. Hasta la fecha, este tipo de servicios no están regulados. Para ello, uno de los temas clave es la neutralidad de la red; un acuerdo de principios de no discriminación del tráfico de Internet cuando este recurso se vuelve escaso.

POLÍTICA DIGITAL NACIONAL

Además de la instauración de la red compartida, descrita en la sección anterior, que planifica el uso de la banda de 700 MHZ para ampliar la cobertura de banda ancha móvil, la reforma de telecomunicaciones de 2012 impulsó la creación de un mercado secundario de espectro al autorizar a los concesionarios la negociación con privados de cesión o arrendamiento de sus propias licencias de espectro (sujeto a aprobación del IFT). La instrumentación de un mercado secundario de espectro incentiva a la innovación tecnológica y gerencial, al permitir a las empresas comerciar libremente sus concesiones, se garantiza que éstas se asignen más eficientemente.

El componente inalámbrico de la red compartida es fundamental para aumentar la cobertura de la banda ancha móvil. La reforma estableció la construcción de una red pública que desplegará infraestructura de acceso móvil reservando el espectro más valioso que existe actualmente en el mundo: 90 MHZ en la banda de los 700 MHZ, conocida como el *dividendo digital*. Se trata de una red mayorista; venderá capacidad al mayoreo a otras empresas y no podrá competir en el mercado minorista. En otros países se está subastando al mercado esta banda para ofrecer servicios móviles de nueva generación como telefonía 4G o LTE. Este emprendimiento viene acompañado de ciertos espacios de incertidumbre. Por ejemplo, además del alto costo de oportunidad que representa reservar para el proyecto del gobierno un espectro muy valioso para el mercado, el modelo de negocio es complejo. Para que exista suficiente demanda para rentar capacidad a esta red mayorista, los actuales operadores del sector tendrían que convertirse en revendedores (operadores móviles virtuales) cuando ellos ya han invertido en su propia capacidad para desplegar servicios al usuario final.

Si bien la banda de 700 MHZ ofrece muy alta calidad, el precio al que accedan tendrá que ser atractivo para que ellos no utilicen su propia capacidad. Se argumenta que esta red debe enfrentar una regulación muy fuerte, porque nace como empresa dominante (en esta banda) y por ello se deben regular precios. Si estos son muy altos no habrá suficiente demanda y si son muy bajos, el modelo no será rentable. Si la red mayorista ofrece a los actuales operadores no sólo capacidad de última milla, sino también capacidad para operar en todo el mercado con una alta calidad de espectro, la

tarifa no tendría por qué estar regulada. Con la entrada de nuevos actores al mercado, como es el caso de AT&T y con las redes que poseen Telcel, Telefónica y Iusacell, podría existir una competencia basada en infraestructura, de tal forma que no sea necesaria la regulación de precios.

CUATRO DÉCADAS DE POLÍTICA DIGITAL: EVOLUCIÓN Y PROBLEMAS CRÓNICOS

A pesar de la constante evolución tecnológica e industrial del sector y, por lo tanto, de la política digital nacional instrumentada en cada una de estas tres transformaciones, identificamos dos problemas crónicos. En primer lugar, se encuentra la debilidad institucional de los organismos reguladores del sector y de los órganos a cargo de los planes de expansión de la red nacional de infraestructura. Este problema se ha observado en múltiples formas, por ejemplo, en la ausencia de leyes rectoras del sector e incluso de los mismos órganos reguladores durante la primera transformación o en las limitaciones legales para prevenir *ex ante* prácticas competitivas monopólicas o sancionarlas *ex post*. Asimismo, la brecha digital en el país es un problema crónico que puede contribuir a magnificar el nivel de desigualdad socioeconómico del país. Tal como el problema de la debilidad institucional, el problema de la brecha digital se ha manifestado en varias dimensiones, pues no sólo se refiere al no acceso a Internet, sino también a la ausencia de capacidades para el uso de las tecnologías emergentes o la incapacidad de acceder a una Internet de banda ancha. A continuación detallamos las condiciones de estos dos problemas crónicos.

DEBILIDAD INSTITUCIONAL

Han pasado casi tres décadas desde que el gobierno mexicano inició la primera generación de reformas en el sector de telecomunicaciones. Desde entonces, la industria ha crecido aceleradamente adoptando tecnología de punta, expandiendo el servicio y disminuyendo tarifas. Sin embargo, una de las barreras más significativas para el desarrollo del sector fue una institucionalidad precaria. La

secuencia que siguió el proceso de reforma, en la que la ley y los órganos reguladores aparecieron cinco años después de la privatización, desfavoreció la competencia efectiva en el sector. La mayor parte de las actividades de la Cofetel se limitaban a dar opiniones y recomendaciones no vinculantes sobre distintos temas, entre los que destacan el otorgamiento de concesiones, la generación de normas, los planes técnicos, la licitación del espectro radioeléctrico y la imposición de sanciones. Hasta su extinción, la Cofetel se mantuvo como una unidad administrativa subordinada de la SCT, sin mayores poderes de decisión en asuntos clave como concesiones, permisos y sanciones. Esto ocasionó uno de los problemas que más se discutió durante la década de 2000: la "doble ventanilla" entre la Cofetel y la SCT. La falta de una autonomía real de la Cofetel y sus poderes limitados llevó a un proceso regulatorio lento e ineficaz, en parte, porque la entidad no disponía de la autoridad suficiente para tomar acciones decisivas y oportunas.

La reforma en telecomunicaciones de 2012 buscó solventar este problema crónico, para ello, se ordenó la creación de un órgano constitucionalmente autónomo –el IFT– que sustituyera a la Cofetel. Le concedió autonomía en términos de presupuesto, legislación y toma de decisiones. Además de las facultades en materia de regulación, también se le otorgó la función de instrumentar la política de competencia en telecomunicaciones y radiodifusión. El nuevo IFT tiene mayores atribuciones de sanción sobre el comportamiento económico de las empresas e incluso para obligar la separación estructural de aquellas con prácticas monopolísticas. El IFT tiene también potestad para recabar información de las compañías sobre el desempeño del mercado, lo que contribuirá a reducir la asimetría de información, problema al que tradicionalmente se enfrentan los organismos regulatorios. Incluso, se han eliminado prácticamente las posibilidades de estancar la acción regulatoria a través del juicio de amparo.

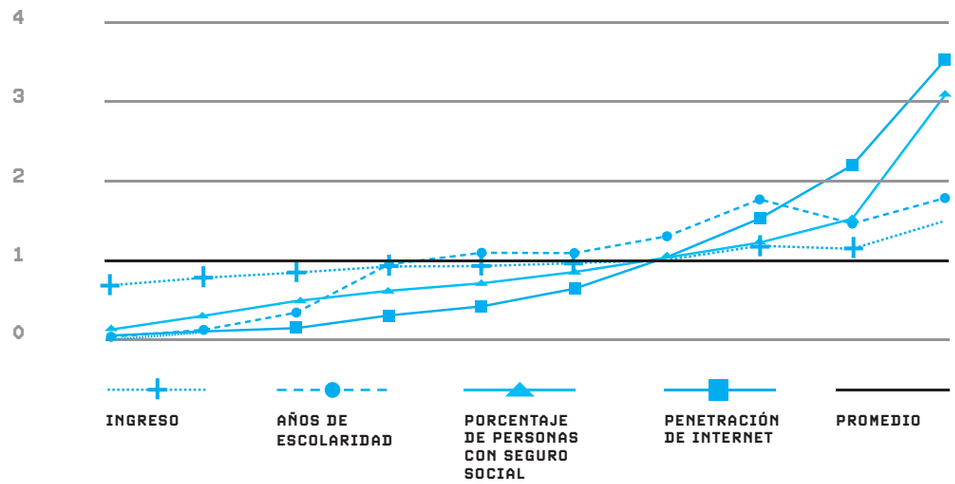
El énfasis en la fortaleza del regulador no es trivial; en términos de competencia de mercado, de acuerdo con la literatura en la materia, los reguladores autónomos y colegiados en su toma de decisiones juegan un papel fundamental en la mejora de la competencia. Esto debido a que el proceso por el cual las instituciones

tienen un impacto en el desarrollo de las telecomunicaciones es a través del uso de normas, reglas y contratos para proveer incentivos que buscan alinear las decisiones de las empresas al *interés público*. Por tanto, las posibilidades de éxito de las políticas regulatorias dependen fundamentalmente de la efectividad de las instituciones en las que el proceso regulatorio toma lugar. La literatura sobre órganos en la materia sugiere que un regulador autónomo contribuye a disminuir la concentración del mercado, aumentar la cobertura y la productividad de las empresas; genera certidumbre en el mercado y promueve la inversión (Wallsten, 2000; Fink *et al.*, 2002; Mariscal *et al.*, 2014). Asimismo, las diferencias en la provisión de servicios de telecomunicaciones emergen de los marcos institucionales que condicionan la inversión a través de mecanismos como la concesión –y protección– de derechos de propiedad o de explotación, así como un marco de certidumbre jurídico que garantice políticas regulatorias transparentes, predecibles, justas y creíbles (Heinz y Zelner, 2001; Levy y Spiller, 1996).

BRECHA DIGITAL

El problema de la brecha digital tiene una fuerte asociación con las condiciones de pobreza y desigualdad de un país. Una nación con graves problemas de pobreza y desigualdad tendrá una brecha digital mayor, debido a las limitaciones de acceso por ingreso, como se describió arriba. Por ejemplo, México tiene alto nivel en ambos problemas. De acuerdo con estimaciones de la Comisión Económica para América Latina y el Caribe (Cepal), en 2016, México tenía un índice de Gini de 50.4, sólo por debajo de Brasil y Colombia; en términos de pobreza, este mismo organismo internacional registró que 41.5% de la población en el país vivía en esta condición en 2018, cifra por encima del valor en la región para el mismo año: 29.8%. En el caso mexicano, en la gráfica 1 se observa un alto nivel de desigualdad en los indicadores de desarrollo humano (ingreso, salud y educación), pero ninguno de ellos tiene el nivel de desigualdad que tiene el acceso a Internet. La brecha digital es de una magnitud mayor incluso que la desigualdad por el ingreso, donde los deciles I y II tienen una penetración de Internet menor de 2%, mientras que el decil más rico tiene una penetración de 68 por ciento.

GRÁFICA 01. DESIGUALDAD EN INGRESO, EDUCACIÓN, SALUD Y PENETRACIÓN DE INTERNET, POR DECILES DE INGRESO



NOTA: LOS VALORES ESTÁN ESTANDARIZADOS EN SU MEDIA.

FUENTE: elaboración propia sobre la base de ENOE, 2012.

También se reconoce que la brecha digital no sólo se explica por causas económicas, pues también existe la imposibilidad de acceso a las TIC por carencia de habilidades digitales, de beneficios percibidos del servicio e incluso por cuestiones culturales. Este problema se define como la brecha de adopción y se refiere a la no adopción de las TIC en la vida de las personas, no por cuestiones relacionadas con el precio o el ingreso, sino por falta de conocimiento de sus potenciales usos en la vida cotidiana o por la carencia de habilidades que permita a las personas utilizar dichas tecnologías. La falta de capacidades para el uso de las tecnologías no es un asunto menor. Como referencia, en México 51.2% (ENDUTIH, 2018) de las personas no usuarias de computadora declararon que es porque no saben usarla, lo que hace evidente la necesidad de desarrollar capacidades de apropiación tecnológica entre la población.

En México, las circunstancias para combatir la brecha digital son adversas. No sólo por la alta desigualdad que impera en el país, sino también por la geografía. La brecha digital es una función de dos variables críticas: la densidad de población de las localidades (y sus condiciones geográficas) y el nivel de ingreso de los hogares. La primera es relevante, porque es un determinante fundamental de

los costos de provisión del servicio para las empresas de telecomunicaciones y su retorno esperado sobre el ingreso. En una ciudad con alta densidad de población, las inversiones en construcción de infraestructura son más redituables para las empresas que en comunidades dispersas y poca población. Esto tiene el efecto de desincentivar la inversión o desarrollar estrategias de negocio tipo *cream skimming*.[9] La segunda variable es el nivel de asequibilidad del servicio. Esto es una relación entre el precio del servicio y la capacidad de las familias para adquirir los de telecomunicaciones, según su costo; aunque sea el mismo, la Internet es más asequible en lugares donde tienen un ingreso promedio más alto que la media.

Si bien, han existido desde la década de 1990 acciones de gobierno para mitigar la brecha digital, estas no han sido suficientes. Las principales políticas públicas se han centrado en proveer equipo de cómputo y conectividad en sitios públicos. Los actos más contundentes con respecto a la mitigación de la brecha digital han ocurrido en el marco de la competencia, principalmente en la puesta a disposición de más espectro para la provisión de servicios. Como se discutió arriba, la banda ancha móvil se perfila como el mejor instrumento para dar acceso a Internet en comunidades de difícil acceso. La acción del gobierno para mitigar la brecha digital es importante porque las TIC tienen la capacidad de actuar como cajas de resonancia: bien amplían la desigualdad entre las personas o bien las reducen (De Fontenay y Beltran, 2008). La potencial amplificación es causada por la incapacidad de los miembros más vulnerables de la sociedad de adquirir un servicio que tiene externalidades positivas. El hecho de que alguien no tenga la posibilidad de adquirir un servicio TIC hoy implica que tendrá limitadas sus opciones de desarrollo personal y de eficiencia económica en comparación con quien sí tuvo acceso a los servicios de telecomunicaciones (De Fontenay y Beltran, 2008).

9 El concepto de *cream skimming* se refiere al desarrollo de competencia únicamente en los segmentos más rentables de la población, lo que genera un desequilibrio de cobertura y precios entre las zonas con rentabilidad alta y baja.

CONCLUSIONES

Desde hace ya cuatro décadas, las telecomunicaciones no han dejado de ser un sector dinámico y con un creciente protagonismo por sus efectos sociales y económicos. Pero también se trata de un sector que exige un constante aprendizaje y evolución de las instituciones del gobierno, no sólo para instrumentar políticas públicas y políticas regulatorias adecuadas a los problemas técnico-económicos que plantea la evolución del sector, sino también para adecuar las instituciones gubernamentales y adaptarse a nuevos temas que requieren la atención del gobierno. La política digital es un concepto en evolución, porque lo "digital" es un concepto en constante cambio; cada vez lo digital aglutina e impacta nuevas esferas de la vida social, por ejemplo, la privacidad de las personas, las relaciones laborales y comerciales a través de la economía de plataformas (o economía *gig*), o la ética de la toma de decisiones basadas en la inteligencia artificial. Hoy, por ejemplo, la gobernanza de los sistemas de inteligencia artificial se está convirtiendo en un reto importante en la evolución de la política digital.

Aunque la historia reciente en la materia en el ámbito nacional da cuenta de sus cambios continuos, existen algunos problemas crónicos de política pública o de capacidades institucionales. En este capítulo revisamos dos de ellos: la debilidad institucional y la brecha digital. Pero otros retos, como las prácticas monopólicas, la asequibilidad de los precios al consumidor o la conformación de un ecosistema digital pueden representar también retos que no han sido resueltos del todo por el gobierno mexicano.

Con las posibilidades que han ofrecido las tecnologías emergentes durante casi cuatro décadas, consideramos que el análisis mostrado en este capítulo representa simplemente una fotografía del estado del arte de la política digital, de lo cual muchos retos regulatorios serán obsoletos en los años por venir. Por otro lado, un gran desafío de los gobiernos en cuanto a la política pública, pero sobre todo a la regulatoria de las telecomunicaciones ha sido mantener el paso a las innovaciones tecnológicas, las cuales siempre van un paso adelante de la regulación. Entonces, quizá el reto crónico más importante que ha enfrentado la política digital nacional ha sido (y seguirá siendo) la aparente condena de siempre ir un paso atrás de la innovación tecnológica, pero con la obligación de siempre ir un paso adelante de la obsolescencia regulatoria. La política digital tiene un permanente deber de urgencia por regular bien y a tiempo.

BIBLIOGRAFÍA

Bauer, J. (2010). Changing roles of the state in telecommunications. *International Telecommunications Policy Review*, *1*, 127-145.

Broadband Commission (2012). *The state of broadband 2012: Achieving digital inclusion for all*. París: UIT y UNESCO.

Cave, M. y Martin, I. (2010). Motives and means for public investment in nationwide next generation networks. *Telecommunications Policy*, *34*(9), 505-512.

Cofece-OCDE (2009). *Recomendaciones para promover un marco regulatorio más favorable a la competencia en la interconexión entre redes de Telecomunicaciones*. Recuperado de https://bit.ly/3Ka6o1Y

Cowhey, P. y Aronson, D. (2009). *Transforming Global Information and Communication Markets*. Cambridge: The MIT Press.

Czernich, N., Falck, O., Kretschmer, T. y Woessmann, L. (2011). Broadband infrastructure and economic growth. *The Economic Journal*, *121*(552), 505-532.

De Fontenay, A.B. y Beltran, F. (2008). Inequality and economic growth: Should we be concerned by the digital divide. *International Telecommunications Society*, *17*.

Donner, J. (2008). Research Approaches to Mobile Use in the Developing World: A Review of Literature. *The Information Society*, *24*(3), 140-159.

Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en Hogares (ENDUTIH) (2018). México: Instituto Nacional de Geografía y Estadística. Recuperado de https://bit.ly/35fUGV5

Estache, A., Manacorda, M. y Valletti, T. (2002). Telecommunications reforms, access regulation, and Internet adoption in Latin America. *Economica*, *2*(2), 153-217.

Fink, C., Mattoo, A. y Randeep, R. (2002). *An assessment of telecommunications reform in developing countries*. Washington DC: Banco Mundial.

Galperin, H., Mariscal, J. y Viecens, M.F. (2013a). Los planes nacionales de universalización, en Jordán, V., Galperin, H. y Peres, W. (eds.), *Banda Ancha en América Latina: más allá de la conectividad*. Santiago de Chile: CEPAL, Diálogo Regional sobre Sociedad de la Información y Unión Europea.

Galperin, H., Mariscal, J. y Viecens, M.F. (2013b). One goal, different strategies: an analysis of national broadband plans in Latin America. *Info*, *15*(3), 25-38.

Hardy, A. (1980). The role of the telephone in economic development. *Telecommunications Policy*, *4*(4), 278-286.

Heinz, W.J. y Zelner, B.A. (2001). The institutional environment for telecommunications investment. *Journal of Economics & Management Strategy*, *10*(1), 123–147.

IFT (2020). Banco de Información de Telecomunicaciones. Penetración Histórica de Telefonía Fija. Recuperado de https://bit.ift.org.mx/BitWebApp/

ITU (2013). Measuring the Information Society. Ginebra: International Telecommunication Union. Recuperado de https://bit.ly/3K6Ou09

Jordán, V. (2010). Banda ancha: la nueva brecha digital. En Cepal (ed.), *Acelerando la revolución digital: banda ancha para América Latina y el Caribe* (85-120). Santiago, Chile: Cepal.

Jordán, V., Galperin, H. y Peres, W. (2010). *Acelerando la revolución digital: banda ancha para América Latina y el Caribe*. Santiago, Chile: Cepal.

Katz, R. (2009). El retorno del keynesianismo a las nuevas redes de comunicaciones. *Revista Telos*, *78*, 13-27.

Koutroumpis, P. (2009). The economic impact of broadband on growth: A simultaneous approach. *Telecommunications policy*, *33*(9), 471-485.

Leff, N. (1984). Externalities, information costs, and social benefit-cost analysis for economic development: an example from telecommunications. *Economic Development and Cultural Change*, *32*(2), 255-276.

Levy, B. y Spiller, P. (1996). *Regulations, Institutions, and Commitment. Comparative Studies of Telecommunications*. Cambridge: Cambridge University Press.

Mariscal, J. (1998). La Reforma en el Sector de las Telecomunicaciones en México: un Enfoque de Economía Política. *Política y Gobierno*, 2(1), CIDE.

Mariscal, J. (2002). *Unfinished Business: Telecommunications Reform in Mexico*. Santa Barbara, California: Praeger.

Mariscal, J. (2004). Telecommunications reform in Mexico from a comparative perspective. *Latin American Politics and Society*, *46*(3), 83-114.

Mariscal, J. y Flores-Roux, E. (2009). *Propuesta de licitación de la fibra oscura propiedad de la CFE. Solución que genera escasez artificial, tanto presente como futura*. Lima: Dirsi.

Mariscal, J., Gamboa, L. y Rentería, C. (2014). The democratization of Internet access through mobile adoption in Latin America. En Goggin, G. y Hjorth, L. (eds.), *The Routledge Companion to Mobile Media* (104-113). Nueva York: Routledge.

Samarajiva, R. y Zainudeen, A. (eds.). (2008). ICT infrastructure in emerging Asia: policy and regulatory roadblocks. IDRC, Ottawa, Canada, and Sage Publications, New Delhi, India.

Tongia, R. y Wilson, E. (agosto, 2007). Turning Metcalfe on his head: The multiple costs of network exclusion. Trabajo presentado en The Research Conference on Communications, Information, and Internet Policy.

Vietor, R. (1994). *Contrived Competition: Regulation and Deregulation in America*. Boston, Massachusetts: Belknap Press of Harvard University Press.

Wallsten, S. (2000). *Telecommunications privatization in developing countries: The real effects of exclusivity periods*. Stanford, CA.

Waverman, L., Meschi, M. y Fuss, M. (2005). The impact of telecoms on economic growth in developing countries. *The Vodafone policy paper series*, *2* (3), 10-24.

Wireless Intelligence (2013). GSMA data. *HHI in Mobile Telephony Market. Spectrum allocated for mobile telephony services.* Recuperado de https://bit.ly/3siocRc

CAPÍTULO 02

DERECHOS DIGITALES EN MÉXICO Y OTROS PAÍSES: REGULACIÓN EN CONSTANTE TRANSFORMACIÓN

JUAN PABLO AGUIRRE QUEZADA*

* Instituto Belisario Domínguez. El autor agradece a los prestadores de servicio social Kevin García Ángeles y Víctor Ramón García Gorostieta.

En la década de los noventa, del siglo XX, la Internet, con su entonces llamada "autopista de la información", aceleró diferentes actividades cotidianas entre millones de personas de todo el mundo como las compras, el comercio, la educación, los trámites gubernamentales, el periodismo y la comunicación. Esta transformación estuvo acompañada de nuevos desafíos en la defensa de los derechos de los usuarios, de acuerdo con la normatividad de cada país; además de que se requirió la participación de cuerpos de seguridad especializados para atacar diversos delitos que aprovecharon las ventajas cibernéticas (terrorismo, trata de personas, fraudes, suplantación de identidad y piratería, entre otros).

Por lo anterior, la defensa de la libertad de expresión, el adecuado uso de los derechos de autor, el empleo de la banca y el comercio digital, la protección de datos personales, los protocolos de seguridad y el acceso a la educación, entre otros, fueron algunos de los temas que requirieron de leyes que pudieran regular sus actividades; por ello, congresos de diferentes países se dieron a la tarea de estudiar casos específicos y redactar normatividades que permitieran el uso óptimo de los servicios que se proporcionaban a través de Internet. Las experiencias fueron muy variadas, tantas como las de los usuarios de cada nación, aunque con ciertos criterios comunes que han permitido generar marcos regulatorios para prevenir y atacar diferentes delitos que pueden cometerse por Internet.

La convivencia social a través de la red, con usuarios de diferentes países y servidores en distintas partes del globo, originó desafíos de ciberseguridad. Paulatinamente, los países adoptaron leyes para afrontar tales desafíos globales, mismos que, debido a los avances tecnológicos, generaban delitos que rebasaban las fronteras. Asimismo, la puesta en marcha de políticas públicas en materia de ciber policía permitió atacar a delincuentes vinculados con el terrorismo o el lavado de dinero, delitos desarrollados a causa de la expansión de la red, pero también ante la defensa de los derechos digitales.

Un avance importante en la regulación de los derechos digitales es el Convenio sobre la ciberdelincuencia —conocido también como Convenio de Budapest—, el cual establece medidas y rubros de cooperación internacional que deberán adoptarse a escala nacional en los países firmantes. Entre los temas abordados por este instrumento destacan: acceso ilícito, ataques a la integridad de los datos y del sistema, falsificación informática, fraude cibernético, delitos relacionados con la pornografía infantil, infracciones a la propiedad, complicidad, responsabilidad de las personas jurídicas, sanciones, ámbito de aplicación, cooperación internacional, extradición y confidencialidad, entre otros (Consejo de Europa, 2001). Este convenio fue firmado en la capital de Hungría, el 23 de noviembre de 2001.

Dicho instrumento jurídico ha sentado las bases para una normatividad más avanzada en diversos países. En ese sentido, el presente estudio se divide en dos apartados. En el primero, titulado "Los derechos digitales en organismos internacionales", se refieren los marcos regulatorios para Internet y las tecnologías de la información a escala internacional, así como las directrices recomendadas por la Organización de las Naciones Unidas (ONU) y la Organización para la Cooperación y el Desarrollo Económicos (OCDE). En el segundo se señalan las características de la Normatividad en países seleccionados, en la que se abordan los casos de Alemania, Brasil, Canadá, Chile, España, Estados Unidos de América, México y Panamá, a fin de señalar tanto los alcances logrados en dichas legislaciones como los desafíos a resolver.

LOS DERECHOS DIGITALES EN ORGANISMOS INTERNACIONALES

A. Organización de las Naciones Unidas (ONU)

La *Declaración Universal de Derechos Humanos*, de 1948, y la *Declaración y Programa de Acción de Viena*, de 1993, son los documentos rectores universales para la defensa de los derechos en toda la población mundial. Por ello, el tema de los derechos digitales está fuertemente vinculado a estas bases jurídicas, en cuanto a libertades de expresión, de pensamiento, la vida, seguridad y reconocimiento de personalidad jurídica, entre otros. Cabe destacar que el artículo 12 de la Declaración Universal sostiene que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a

su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques" (ONU, 1948). En tanto que el artículo 19 refiere que "todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión" (ONU, 1948). Por lo que son los fundamentos jurídicos internacionales base de los derechos digitales.

La Organización de las Naciones Unidas (ONU), por medio de la Asamblea General, ha aprobado diferentes acuerdos, a fin de garantizar el respeto de los derechos humanos en las tecnologías de la informática. Ejemplo de ello es la resolución 68/167, que hace énfasis en proteger los derechos de las personas en Internet, principalmente el derecho a la privacidad, al exhortar a todos los Estados parte a que:

a) Respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales.
b) Adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos (ONU, 2013).

Respecto de la defensa de los derechos humanos en Internet, la Asamblea General de la ONU aprobó la resolución sobre la promoción, protección y disfrute de los derechos humanos en Internet, en la cual:

> Afirma que los mismos derechos que tienen fuera de línea las personas también deben protegerse en línea, en particular la libertad de expresión, lo que es aplicable independientemente de las fronteras y por conducto de cualquier medio de su propia elección, de conformidad con el artículo 19 de la Declaración Universal de Derechos Humanos y del Pacto Internacional de Derechos Civiles y Políticos (ONU, 2018).

Es decir, esta iniciativa se fundamenta en el derecho de la libertad de opinión y de expresión, por lo que el uso de Internet es una

herramienta para la recepción de ideas, búsqueda de información y difusión mediante cualquier medio de comunicación (lo que respecta a Internet). Por lo que la defensa de los derechos de los usuarios de la red de banda ancha es defendida a escala internacional con los documentos rectores existentes. Asimismo, el Pacto Internacional de Derechos Civiles y Políticos reúne diferentes acuerdos aplicables al uso de los derechos digitales, mediante el reconocimiento de los derechos humanos, tales como la libertad de pensamiento, de asociación, la prohibición de propaganda de guerra y la facultad de asociación, entre otros. De este modo, dicho acuerdo reconoce que:

> No puede realizarse el ideal del ser humano libre en el disfrute de las libertades civiles y políticas y liberado del temor y de la miseria, a menos que se creen condiciones que permitan a cada persona gozar de sus derechos civiles y políticos, tanto como de sus derechos económicos, sociales y culturales (PIDCP, 1976).

Por tanto, la defensa de los derechos digitales toma en cuenta las bases garantistas existentes, como la defensa universal de los derechos humanos.

Si bien la resolución sobre la promoción, protección y disfrute de los derechos humanos en Internet no es vinculante para los Estados parte, sí fortalece el debate a escala mundial acerca de los derechos digitales que puede tener la población. Así, el organismo ha realizado diferentes llamados a fin de que el acceso a la red sea una realidad para las personas que viven en los países más pobres, además de sumarse a iniciativas como el día del Internet seguro, que se conmemora el 11 de febrero de cada año, o esfuerzos para que el contenido que se maneja en esta tecnología sea apropiado para niñas, niños y adolescentes, entre otros. En ese sentido, la cooperación que realiza este organismo internacional con la sociedad civil ha permitido la creación de sinergias que defienden la normatividad de las tecnologías de la información y la comunicación (TIC). Ejemplo de ello son los Principios Rectores sobre las Empresas y los Derechos Humanos, adoptados por el Consejo de Derechos Humanos de la ONU, mediante la resolución 17/4, del 16 de junio de 2011, los cuales contemplan tres puntos principales:

a) El deber del Estado de proteger los derechos humanos; *b)* la responsabilidad de las empresas de respetar los derechos humanos; y *c)* acceso a mecanismos de reparación (ACNUDH, 2011: 3).

Uno de los últimos esfuerzos de la ONU para lograr fines globales que reduzcan la desigualdad, fomenten la prosperidad y el cuidado del medio ambiente son los 17 Objetivos de Desarrollo Sostenible (ODS), adoptados en 2015. En el tema número nueve, referente a industria, innovación e infraestructura, la meta 9c refiere la necesidad de "aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020" (ODS, 2020). Por lo cual el derecho digital de acceso a las TIC se está ampliando para intentar que todas las personas usen estas comunicaciones. Si bien el acceso a Internet no está explícitamente incluido en los demás objetivos, es indudable que esta tecnología contribuirá en los esfuerzos mundiales para alcanzar las soluciones a los desafíos planteados.

Entre los planteamientos que la ONU ha realizado para mejorar el goce de los derechos digitales entre sus países miembros destaca que las iniciativas propuestas en el tema de datos abiertos garanticen las prerrogativas de la intimidad de las personas, a fin de "evitar casos como el de Facebook-Cambridge Analítica, en el que se compartió la información personal de hasta 87 millones de usuarios con fines políticos" (ONU, 2018). A este respecto, es deber, no sólo de gobierno, sino también de particulares salvaguardar la defensa de los datos personales, con tal de evitar que esa información exponga a las personas a ser víctimas de delitos que pongan en riesgo su integridad o patrimonio.

Un esfuerzo para la protección de datos personales, que ha sido reconsiderado por personal de la ONU ante la necesidad de tener normatividades en materia de derechos digitales, es el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, del 28 de enero de 1981 –conocido también como Convenio de protección de datos 108+– (INAI, 2020). Dicho acuerdo es fundamental para la defensa de los derechos digitales a escala mundial, ya que, si bien su origen fue para la vigencia de los países pertenecientes a la Unión Europea, la suscripción de diferentes convenios multi

y bilaterales fomentó la adopción y cumplimiento de sus postulados por diversas naciones. Incluso, la ONU señaló que "todos los Estados miembros de la ONU deben ratificar el Convenio de protección de datos 108+ e implementar de inmediato las salvaguardas para los datos personales recopilados con fines de vigilancia y otros fines de seguridad nacional" (ONU, 2018). Por lo tanto, este instrumento jurídico se convirtió en un documento rector a escala internacional en el tema de la protección de los derechos digitales. Cabe destacar que la Cámara de Senadores de México aprobó tanto el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal como su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos (realizados en Estrasburgo, Francia, el 28 de enero de 1981 y el 8 de noviembre de 2001, respectivamente), de Acuerdo con el *Diario Oficial de la Federación*, del 26 de abril de 2018, por lo que nuestro país también se sujeta a estos principios.

Parte de la salvaguarda de las prerrogativas digitales es el derecho a la privacidad. En consecuencia, diferentes países parte presentaron a la Asamblea General de la ONU una iniciativa de resolución (A/C.3/71/L.39) referente al derecho a la privacidad en la era digital. Dicho documento reconoce que:

> Un entorno abierto, seguro, estable, accesible y pacífico en el ciberespacio es sumamente importante para la realización del derecho a la privacidad en la era digital, (1) reafirma el derecho a la privacidad, según el cual nadie debe ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, y el derecho a la protección de la ley contra tales injerencias, establecidos en el artículo 12 de la Declaración Universal de Derechos Humanos 1 y el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos (ONU, 2016).

De manera que la comunicación en Internet es considerada una actividad humana, con alcance en diferentes derechos humanos, plasmados tanto en documentos rectores de la ONU, como en las legislaciones de los distintos países. Es decir, si bien existe la defensa de los derechos digitales, faltan diferentes avances en su ejercicio a escala local, de tal suerte que este organismo

internacional realiza diferentes resoluciones, propuestas y acuerdos con tal de mejorar las relaciones humanas; además de prevenir y combatir los delitos que se originan en esta red informática.

Finalmente, la ONU se ha enfocado en impulsar esfuerzos que permitan el uso de Internet a la población de los países con menos recursos como medida para reducir la brecha digital que acaso puede generar mejores condiciones de vida para los usuarios, además de facilitar lo estipulado en la meta 9.3 de los ODS para "aumentar el acceso de las pequeñas industrias y otras empresas, particularmente en los países en desarrollo, a los servicios financieros, incluidos créditos asequibles, y su integración en las cadenas de valor y los mercados" (ODS, 2020), de manera que un cambio en el acceso, uso y defensa de los derechos digitales permitirá un desarrollo social con mayores impactos positivos.

B. Organización para la Cooperación y el Desarrollo Económicos (OCDE)

La Organización para la Cooperación y el Desarrollo Económicos (OCDE) ha señalado en el informe Perspectivas de la OCDE sobre Economía Digital 2017 que:

> La política pública gubernamental no ha avanzado a la par de la innovación digital, ni de la transformación de las economías y las sociedades que dirigen las grandes empresas de tecnología. Señala que los países deben redoblar sus esfuerzos, invertir más en educación y en la adquisición de habilidades, además de fomentar un mayor uso de las tecnologías modernas como el análisis de datos masivos y los servicios informáticos en la nube, en especial entre las empresas pequeñas, para que el cambio digital sea más productivo e incluyente (OCDE, 2017).

Dicho organismo encuentra en los derechos digitales una serie de oportunidades para fortalecer las habilidades cotidianas de la población, sobre todo en áreas de crecimiento en educación, economía o datos abiertos; lo cual incidiría en transformaciones sociales en las que se necesitará regular los diferentes marcos normativos, a fin de brindar beneficios tangibles a las y los usuarios de Internet de los países miembros.

La OCDE considera a Internet como un medio que ha logrado grandes transformaciones en la sociedad, a la vez que ha impulsado el comercio, así como que el alcance a las redes de las TIC no ha sido para toda la población. Acerca de esto, el organismo reconoce que:

> Al reducir el costo del acceso a la información y ampliar los medios para compartir conocimientos, estas redes permiten empoderar a las personas, fomentar una mayor participación ciudadana y mejorar la prestación de servicios públicos, además de contribuir a crear oportunidades de nuevos bienes, servicios, modelos de negocio y empleos (OCDE, 2016: 3)

Es decir, la OCDE observa, por medio del uso de la banda ancha, el goce de diferentes derechos, entre los que destaca el ejercicio de la ciudadanía mediante procesos de desarrollo democrático; pero también las posibilidades de adquisición de bienes y mercancías, lo que contribuye al bienestar social.

Sin embargo, para el pleno uso de los derechos digitales, se observa que la carencia de infraestructura en diferentes países miembros imposibilita que la población goce de estas prerrogativas. En ese sentido, "es frecuente que las áreas suburbanas de muchas ciudades carezcan de infraestructuras básicas para los proveedores de telecomunicaciones y que la gestión de derechos de vía constituya un gran obstáculo para el despliegue de red y la inversión conjunta en infraestructuras" (OCDE, 2016: 22). Asimismo, la OCDE sugiere que, para un mejor acceso de la población al Internet, y a los diferentes usos y derechos que existen en las TIC, se requiere que:

> La reducción de los costos de despliegue para estimular tanto la competencia como la inversión en infraestructuras y su expansión puede exigir reformas normativas. Si se facilita el acceso a derechos de vía y espectro y se incentiva el uso compartido de infraestructuras, especialmente de infraestructura pasiva, se fomentará la expansión de la banda ancha (OCDE, 2016: 24).

La infraestructura es un medio que permite acercar a la sociedad usuaria de servicios digitales a sus derechos; en consecuencia, impedir o restringir el uso de Internet por parte de los diferentes

gobiernos atenta contra las prerrogativas legales que tiene la población, tal es el caso de la censura existente en diversas partes del mundo, expuesta por diferentes organizaciones de la sociedad civil.

Por lo anterior, la OCDE ha formulado diferentes mecanismos que regulan distintas actividades relacionadas con tales derechos. Uno de esos documentos es Principios de la OCDE sobre Inteligencia Artificial, el cual considera que la inteligencia artificial (IA) debe velar por un uso para el beneficio de las personas, en particular, y del planeta, en general; además de impulsar el bienestar general, el desarrollo sostenible y el crecimiento inclusivo. De acuerdo con Ángel Gurría, secretario general de la OCDE:

> La inteligencia artificial está revolucionando nuestra forma de vivir y trabajar, y ofrece unas ventajas extraordinarias a nuestras sociedades y economías. Ahora bien, también plantea nuevos desafíos y siembra incertidumbre y preocupaciones de carácter ético. Compete, por tanto, a los gobiernos asegurarse de que el diseño de los sistemas de IA respete nuestros valores y leyes, de forma que las personas puedan confiar en que su seguridad y privacidad serán objeto de una consideración prioritaria (OCDE, 2019).

Cabe destacar que los principios postulados por la OCDE no son vinculantes para sus 36 países parte y los seis adherentes. No obstante, es destacado el interés de estas 42 naciones por generar un esfuerzo que permita un mejor uso de las TIC, con consecuencias positivas y apego a la normatividad para las principales economías.

Si bien el organismo ha fortalecido los derechos digitales en temas como la economía o el comercio, la OCDE ha realizado diferentes llamados a la defensa de los derechos humanos dentro de estos segmentos, lo que ha tenido impactos en las relaciones humanas a través de las TIC. Un ejemplo es la solicitud de que las empresas de los países parte deban "revisar y actualizar sus políticas corporativas relativas a temas como fuerza laboral, derechos humanos, transparencia y corrupción, y darlas a conocer" (OCDE, 2018). Pese a ello, la OCDE está más limitada que la ONU en cuanto al tema de defensa de las garantías individuales, enfocada más en cuestiones de mercado entre las principales economías.

Al respecto, algunos expertos consideran que las Directrices para Empresas Multinacionales, actualizadas por la OCDE en 2011, fueron consecuencia de la aprobación de los Principios Rectores sobre Empresas y Derechos Humanos por parte de la ONU, que tienen como fin:

> Crear una sinergia y convergencia a nivel internacional respecto a los estándares existentes sobre la responsabilidad de las empresas en materia de derechos humanos. Constituyen un elemento importante en este ámbito, y contribuyen al desarrollo de una cultura de conducta empresarial responsable (Cantú, 2014).

De manera que los derechos digitales tienen sinergias con diferentes documentos rectores de organismos internacionales, lo que al final tiene un impacto en las leyes nacionales.

La OCDE puede tener un importante efecto en sus 36 países miembros, además de naciones asociadas. A este respecto, se proporciona información sobre la normatividad en países seleccionados, de los cuales, seis de ellos (Alemania, Canadá, Chile, España, Estados Unidos y México) son miembros de dicho organismo, mientras que otro (Brasil) es considerado socio clave para este organismo. Finalmente se incluye a Colombia por ser un candidato a ingresar a la OCDE.

NORMATIVIDAD EN PAÍSES SELECCIONADOS

ALEMANIA

En este país el marco regulatorio de los derechos digitales está consagrado en su Ley Fundamental de la República Federal de Alemania (Constitución), ya que en su artículo 1º refiere que "la dignidad humana es intangible. Respetarla y protegerla es obligación de todo poder público" (Fazit, 2020). Lo cual sirve como marco legal para la defensa de los derechos digitales. Asimismo, esta nación es firmante de diferentes acuerdos de respeto en materia de derechos humanos, tanto en la Unión Europea como en la ONU, por lo que se adhiere a los tratados internacionales para este fin. Cabe destacar

que en dicha ley no hay referencia al Internet o a la palabra digital, es por eso que la defensa de derechos en general, incluido las acciones de comunicación, es la que aborda las prerrogativas en las TIC.

La Ley Fundamental señala, en su artículo 5º, relativo a la libertad de prensa, que:

> Toda persona tiene el derecho a expresar y difundir libremente su opinión oralmente, por escrito y a través de la imagen, y de informarse sin trabas en fuentes accesibles a todos. La libertad de prensa y la libertad de información por radio, televisión y cinematografía serán garantizadas (Gloger, 2019).

Por lo que aplica también para las TIC, debido a lo referente a las imágenes. Cabe decir que en Alemania existe la prohibición de censurar, pese a ello, el gobierno ha hecho llamados para ejercer de forma responsable esta libertad de expresión, tal como sucede con el Código del Consejo de Prensa alemán.

La mencionada Ley Fundamental, en su artículo 10, incluye también el secreto epistolar, tanto en las telecomunicaciones como en el medio postal. En cuanto al funcionamiento de la administración pública a escala nacional, el artículo 87f señala la gestión en el servicio de correos y de las telecomunicaciones. Debido a que los derechos digitales son un tema en constante transformación, la carta magna alemana considera, en su apartado de disposiciones transitorias y finales, el rubro de telecomunicaciones, en el artículo 143b. No obstante, es importante señalar que el documento en turno sí plantea ciertas restricciones a los derechos digitales, ya que el artículo 18 se refiere a la privación de los derechos fundamentales:

> Quien, para combatir el régimen fundamental de libertad y democracia, abuse de la libertad de expresión de opinión, particularmente de la libertad de prensa (artículo 5º, apartado 1), de la libertad de enseñanza (artículo 5º, apartado 3)[...] de asociación (artículo 9º), del secreto de las comunicaciones postales y de las telecomunicaciones (artículo 10)... pierde estos derechos fundamentales (Ley Fundamental de la República Federal de Alemania, 2020).

La cancelación de estas garantías es declarada por la Corte Constitucional Federal.

En ese contexto, el Tribunal Federal de Justicia de Alemania (máxima autoridad judicial) ha tomado decisiones en materia de derechos digitales, tales como declarar legal el uso de bloqueadores de anuncios en línea, o retirar imágenes de sátira que perjudican la imagen de mandatarios extranjeros. Asimismo, otras dependencias gubernamentales han generado regulaciones como prohibir a Facebook recolectar datos de usuarios de WhatsApp e investigar a empresas por exportar software espía sin permiso legal, entre otras (R3D, 2020).

BRASIL

Cuenta con el Marco Civil de Internet, que entró en vigor a finales de abril de 2014. Esta ordenanza se divide en cinco principales apartados: disposiciones generales, derechos y garantías de los usuarios, la provisión de conexión y de aplicaciones de Internet, el ejercicio del poder público y disposiciones finales. En dicha ley destaca el tercer capítulo, pues incluye temas de gran importancia para los derechos digitales; a saber: la neutralidad de la red, protección de datos personales y comunicaciones privadas, custodia de registro de conexión, uso de aplicaciones, daños ocasionados por terceros y solicitudes judiciales de registros, entre otros (Câmara dos Deputados, 2015).

En el caso brasileño, el Marco Civil de Internet fue pensado como normatividad necesaria, cuyo propósito es la defensa de los derechos humanos en las actividades realizadas en las TIC. Es preciso señalar que este proceso fue impulsado desde la sociedad civil y "garantiza la neutralidad de la red y el derecho a la privacidad de las telecomunicaciones. De esta forma, Brasil se suma a Holanda, Chile y Eslovenia, el reducido club de países que han garantizado por ley la neutralidad de la red" (Gutiérrez, 2014). Por la densidad de población y la cantidad de usuarios de la llamada banda ancha, la puesta en marcha de esta legislación significó un referente internacional de gran importancia, ya que es un esfuerzo por regular mejores conductas por parte de los usuarios. Del mismo modo, la custodia de los registros de conexión generó mejores condiciones de seguridad ante las amenazas de los

delitos que se cometen a través de esta herramienta. Esta ley es de carácter general, aplicable a todas las entidades federativas, todos sus municipios y el Distrito Federal.

Al realizar un análisis detallado del Marco Civil de Internet de Brasil se puede apreciar que el artículo 7º reconoce el acceso a la banda ancha como un factor esencial para el ejercicio de la ciudadanía, además de asegurar derechos digitales como inviolabilidad de la intimidad y de vida privada, el secreto del flujo de las comunicaciones por Internet (salvo por orden judicial), inviolabilidad y secreto de sus comunicaciones privadas, no suspensión de la conexión a Internet (salvo por deuda), calidad de la conexión, claridad en la información de los contratos de servicios, imposibilidad de suministrar a terceros sus datos personales, el borrado de los mismos, accesibilidad para personas con discapacidad y la aplicación de las normas de protección y defensa del consumidor. Igualmente, el artículo 8º aborda la garantía del derecho a la privacidad y a la libertad de expresión, en el sentido de su aplicación "en las comunicaciones es condición para el pleno ejercicio del derecho de acceso a Internet (Câmara dos Deputados, 2015). Esta ley es un importante ejemplo de cómo la defensa de los derechos digitales pasa de un término general a incluir aspectos específicos en su normatividad.

CANADÁ

Es uno de los países con mayor apertura a escala internacional en el uso de Internet, al tener nula censura en las diferentes expresiones de su uso. Sin embargo, han existido diferentes lineamientos para regular estas actividades. Ejemplo de esto es la Copyright Modernization Act, ley que establece límites a los derechos de propiedad mediante advertencias a los usuarios. Fue aprobada a finales de junio de 2014. Entre los puntos que aborda están la actualización de derechos y protecciones de los autores de acuerdo con los estándares internacionales, la responsabilidad de los proveedores de Internet e infracciones de derechos de autor, el facilitar la consulta de material protegido para empresas (bibliotecas y centros educativos), permitir el uso a estudiantes y educadores, ciertos usos para consumidores, prerrogativas similares para fotógrafos y otros creadores, neutralidad tecnológica de las TIC y la revisión de dicha ley cada cinco años

(Cámara de los Comunes de Canadá, 2012). Por lo anterior, es factible que en 2022 la Copyright Modernization Act pueda ser modificada.

Pese a esta legislación, algunas voces señalan que la normatividad seguida en Canadá no se adecúa a la que se aplica a sus socios comerciales mediante acuerdos internacionales, entre ellos el Tratado entre México, Estados Unidos y Canadá (TMEC), al afirmar que:

> Obligan a México (pero no a Canadá) a establecer un mecanismo de "notificación y remoción" de expresiones en Internet, por el cual los proveedores de servicios en Internet tendrían la obligación de censurar cualquier expresión en Internet cuando una persona que se ostente como titular de derechos de autor denuncie la presunta infracción de sus derechos o, de lo contrario, correr el riesgo de ser responsabilizados por la supuesta infracción (artículo 20) (R3D, 2018).

Por esta razón, existe el reto de armonizar diferentes leyes internacionales a fin de generar igualdad de condiciones con las leyes aplicables en Canadá.

Complementariamente, la Personal Information Protection and Electronic Documents Act (PIPEDA) ha normado la protección de datos personales en Canadá, basados en las prerrogativas otorgadas en la Carta de Derechos y Libertades de aquel país (Canadian Charter of Rights and Freedoms), con el fin de proteger la privacidad de los usuarios de Internet. Hay que señalar que "los estatutos existentes a nivel provincial puede prevalecer sobre la Ley Federal" (Library of the Congress, 2017) por lo que aun con una legislación de este tipo existen lagunas legales que pueden afectar el uso seguro de las TIC para los ciudadanos canadienses; aunque, de acuerdo con la cita, no habla de medidas para los usuarios menores de edad.

Entre las características de la PIPEDA destacan: regulación de actividades realizadas por empresas de TIC (Google, Facebook, etcétera); aplicaciones para teléfonos inteligentes; obligaciones en materia de privacidad; acciones de transparencia; retención de datos y medidas de seguridad, entre otros (Library of the Congress, 2017). A este respecto, las redes sociales no tienen normas específicas en esta ley para su regulación.

COLOMBIA

El marco jurídico para Internet en aquel país se ha basado en solucionar problemas relacionados con los derechos de autor, el crecimiento y mejores condiciones de uso para la población, combate a la pornografía infantil, o la regulación de telecomunicaciones, entre los temas más destacados. De acuerdo con una búsqueda realizada en la página del Senado de la República de Colombia, no existen leyes dedicadas a la banda ancha de forma exclusiva (Senado de Colombia, 2020). Por lo que la defensa de los derechos de los usuarios de apega a la normatividad existente.

La defensa de los derechos digitales en Colombia tiene su fundamento en el título II de la constitución, el cual refiere a las garantías, derechos y deberes a las que está sujeta la población colombiana. Al respecto, el artículo 15 señala que:

> Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas (Corte Colombia, 2016).

Es decir, se cuidan derechos que pueden incidir en las relaciones humanas digitales, tales como privacidad, imagen o protección de datos personales. La carta magna colombiana hace énfasis en que todas las formas de comunicación privada son inviolables, únicamente pueden ser interceptadas en caso de que existiera una orden judicial.

La constitución de Colombia garantiza la libertad de conciencia, por lo que hay libertad de expresión, pensamiento y opiniones (artículos 16 y 20). Si bien la censura está prohibida, existe el derecho de rectificación en caso de alguna controversia derivada de dichas garantías.

En el debate actual sobre los derechos digitales en aquel país destacan temas como el reconocimiento facial en protestas en contra de la neutralidad en la red, ciberseguridad, amenazas a periodistas por la red y vigilancia de los usuarios, entre otros. Un ejemplo de ello es el proyecto Cámaras inDiscretas, que consiste en el:

> Análisis del fallido sistema de vigilancia en el sistema de transporte bogotano, Transmilenio. Este estudio de Fundación Karisma (Colombia) ofrece una perspectiva sobre el uso del reconocimiento facial en sistemas de videovigilancia y muestra los fallos que se evidencian en el diseño e implementación de este tipo de proyectos (Hernández, 2018).

Derivado de lo anterior, el tema de las prerrogativas de los usuarios es cuestionado bajo los enfoques del libre tránsito y el rechazo de posibles espionajes.

CHILE

En la nación andina, el tema de los derechos digitales está incluido en la Ley de Neutralidad en la Red (Ley 20453), la cual establece disposiciones para las concesionarias de servicio público de telecomunicaciones en Internet:

> No podrán arbitrariamente bloquear, interferir, discriminar, entorpecer ni restringir el derecho de cualquier usuario de Internet para utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal a través de Internet, así como cualquier otro tipo de actividad o uso legal realizado a través de la red (Ley 20453, 2010).

Igualmente, la normatividad hace referencia a la prohibición de limitar el derecho de un usuario a incorporar o utilizar cualquier clase de instrumentos legales, publicación de la información relativa a las características del acceso a Internet ofrecido, consagración del principio de neutralidad en la red para los consumidores y usuarios de Internet protección de los derechos de los usuarios de Internet, reglamento de prestación de servicios y condiciones mínimas de servicio, entre otros. Esta normatividad entró en vigor el 26 de agosto de 2010.

Por otra parte, la normatividad usada para los sitios gubernamentales de Internet para el servicio de los ciudadanos contempla disposiciones como el Instructivo Presidencial N° 005 – 2001, *sobre* desarrollo del Gobierno Electrónico; la Norma Técnica para el desarrollo de Sitios Web de los órganos de Administración del Estado,

de 2006; la ley Nº 20.285, sobre Acceso a la Información Pública; el Plan Estratégico de Gobierno Electrónico 2011-2014; o las disposiciones transitorias de las Normas técnicas sobre sitios electrónicos y plataformas web abiertas; las cuales destacan por incluir temas de derechos digitales como:

> Accesibilidad para discapacitados, utilización de licencias abiertas, cumplimiento de estándares W3C, datos abiertos (*Open Data*), el uso de herramientas automáticas para verificar el cumplimiento de estándares, codificación, utilización de dominios de gobierno, y los elementos que se deben incorporar para dar protección a los datos personales de los ciudadanos que sean entregados a través de las plataformas digitales (Sobre la normativa web en Chile, 2020).

En el caso chileno, ha existido una continuidad a las reformas legales que permitan leyes acordes con las necesidades sociales en el uso de Internet.

Entre los asuntos que actualmente están en el debate de los derechos digitales en Chile sobresale la puesta en marcha de la Agenda Digital 2020, que contempla 63 medidas que tienen como responsables a diferentes instituciones gubernamentales con temas como: derechos para el desarrollo digital; conectividad; servicios en línea del Estado; emprendimiento e innovación digital; impulso a empresas de TIC; ofrecimiento de mejores competencias en educación y empleo con el uso de estas tecnologías (Agenda Digital 2020, 2020). Por el contrario, otras voces han argumentado la falta de compromiso por parte de las compañías proveedoras para defender los datos personales de los usuarios, ya que "si bien la notable mejora de algunas empresas da cuenta de un interés positivo, el estancamiento de otras da cuenta de que este interés no es transversal a todo el sector de las telecomunicaciones" (¿Quién defiende tus datos?, 2020). Esta es un área de interés para mejorar las condiciones legales de uso de Internet en beneficio de la población chilena.

ESPAÑA

Uno de los principales desafíos que ha afrontado la legislación en Internet en dicho país es la gestión de los derechos digitales, es decir, "un término que engloba a varias técnicas que permiten al dueño de los derechos, o distribuidor de un contenido de formato digital, controlar cómo puede emplearse el material por los usuarios en cualquier tipo de dispositivo electrónico" (Millán, 2006). Por lo que la variedad del uso de Internet genera la demanda de soluciones específicas para atender las necesidades de los usuarios. Un ejemplo de lo anterior es el derecho al olvido, el cual fue dictaminado en tribunales de la Unión Europea, por lo que terminó rigiendo para todos los países integrantes en una decisión supranacional (Sánchez, 2019).

El gobierno español refiere la importancia legal acerca de la normatividad que requieren las TIC; por lo que la motivación jurídica es:

> La extraordinaria expansión de las redes de comunicaciones electrónicas y en especial de Internet así como la incorporación de esta última a la vida económica y a la actividad comercial, hacen necesario establecer un marco jurídico adecuado que genere en todos los actores intervinientes la confianza necesaria para el empleo de este nuevo medio (Gobierno de España, 2020).

El marco jurídico de los derechos digitales en el país ibérico está compuesto por las siguientes leyes:

- Ley Orgánica 15/1999, de 13 de diciembre de Protección de Datos de Carácter Personal.
- Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico. Ley 34/2002
- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias.
- Ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios.
- Ley 42/2010, de 30 de diciembre, de medidas sanitarias frente

al tabaquismo y reguladora de la venta, el suministro, el consumo y la publicidad de los productos del tabaco.

- Ley 13/2011, de 27 de mayo, de regulación del juego (Gobierno de España, 2020).

Un avance registrado en España fue la puesta en vigor de la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico, también conocida como Ley 34/2002, la cual aborda cuatro puntos centrales: *a)* Comercio electrónico; *b)* Contratación en línea; *c)* Información y publicidad; y *d)* Servicios de intermediación. Por lo que los últimos debates en cuanto a los derechos digitales en España se ha centrado en afianzar los últimos cambios legislativos, tales como la neutralidad de la red, asegurar el derecho universal al Internet, seguridad de los usuarios al navegar, validez de la educación, rectificación de opiniones, respeto a los derechos de los menores, y desconexión laboral, entre otros (Castillo, 2018).

ESTADOS UNIDOS

En EU existen leyes federales y locales acerca de la defensa de los derechos humanos, en general, y de políticas digitales, en particular, por lo que en ocasiones los esfuerzos normativos de los estados generan garantías especificas para los habitantes en sus demarcaciones. Ejemplo de esto son los esfuerzos realizados en California, que durante 2018 aprobó estrictas leyes de privacidad en Internet, consistentes en que:

> Las empresas reguladas por el CCPA tendrán una cantidad de obligaciones para los consumidores, incluidas las divulgaciones, el Reglamento de protección general de datos (RGPD), como los derechos de los interesados en los datos de consumidores (interesado), una 'exclusión' para determinadas transferencias de datos y una 'participación' requisito para menores" (Microsoft; 2020).

Asimismo, contempla el debate acerca de la neutralidad de esta red. Sin embargo, las decisiones nacionales que puedan tomarse respecto a los derechos digitales pueden tener repercusiones en otros países, en gran medida por los acuerdos internacionales suscritos por Estados Unidos, tal como sucede con el TMEC, el cual:

> Innova en términos negativos allí donde otras negociaciones ya ofrecían pocas garantías. El capítulo de Comercio Digital introduce una versión diluida de las exigencias presentes en el nuevo TPP de introducir reglas de protección de la información personal, permitiendo también que esa protección conste en compromisos voluntarios de parte de las empresas (Lara, 2018).

Por lo que este tipo de instrumentos ha servido para plasmar diferentes leyes en los ámbitos de influencia más allá de sus fronteras.

Además de políticas digitales en la macroeconomía, los acuerdos internacionales firmados por Estados Unidos también repercuten de forma digital tanto al interior, como al exterior de aquella nación. Una muestra es, nuevamente, el TMEC, ya que:

> Restringe políticas de localización de datos que podrían usarse para limitar la transferencia de datos personales, y prohíbe las restricciones a las transferencias transfronterizas de datos, dejando serias limitaciones a la capacidad de los países de fijar reglas protectoras de la información personal (Lara, 2018).

Estos posicionamientos homologan las leyes al interior de los estados de EU, además de generar directrices en los países asociados, lo que facilita las relaciones comerciales, culturales y sociales entre la población estadounidense y el resto del mundo.

Tiene lugar añadir que en el vecino país del norte existen diferentes leyes de protección de datos personales como Health Insurance Portability and Accountability Act (HIPAA), de 1996, relativa a la salud; Children's Online Privacy Protection Act, de 1998, sobre la privacidad de los menores de edad al usar Internet; Sarbanes-Oxley Act, de 2002, para la protección de inversionistas; o Fair and Accurate Credit Transactions Act (FACTA), de 2003, acerca de las finanzas personales electrónicas. Estos son algunos ejemplos del marco regulatorio del Internet en Estados Unidos.

MÉXICO

El marco regulatorio de las tecnologías de la información en México está compuesto por la *Constitución Política de los Estados Unidos Mexicanos*, el Código Civil Federal, Código de Comercio, Código Federal de Procedimientos Civiles, Código Fiscal de la Federación, Código Penal Federal, Ley de la Propiedad Industrial, Ley Federal de Protección al Consumidor, Ley Federal del Derecho de Autor, Ley Federal de Telecomunicaciones y Ley de Información Estadística y Geografía. Cabe destacar que en la legislación nacional no existe una ley específica que lleve su nomenclatura, por lo que la normatividad lo considera como telecomunicación electrónica. No obstante, algunos autores destacan que, si bien "Internet no está comprendido en esa categoría, no se puede asegurar por completo que el Internet tenga un cuerpo jurídico que lo regule" (Trejo, 2006: 27).

El acceso a los derechos digitales está plasmado en el artículo 6º de la *Constitución Política de los Estados Unidos Mexicanos*, que en su tercer párrafo señala:

> El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e Internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios (CPEUM, 2020: 12).

Dicha inclusión fue añadida de acuerdo con el Decreto publicado en el *Diario Oficial de la Federación* (DOF) del 11 de junio de 2013, lo que refuerza la defensa de la libertad de expresión a través de diferentes medios, entre ellos las tecnologías de la información y comunicación.

Los derechos digitales en México han sido considerados con una legislación acorde con los desafíos que enfrentan los usuarios de Internet, pero en la práctica aun faltan condiciones para su aplicación. De acuerdo con Claudio Ruíz:

> Los derechos en Internet son un concepto que tiene que construirse en el tiempo, es una lucha constante, y donde activistas particularmente en México han hecho un trabajo importante en materia de libertad de expresión, de privacidad y de protección de datos (Ruiz, 2016).

Por ello la normatividad ha cambiado de acuerdo al desarrollo de los usos de las TIC, pero todavía persisten problemas sociales entre los usuarios.

El rubro de la defensa de los derechos humanos en los medios digitales en nuestro país ha abierto diferentes debates acerca de mejoras y adiciones a la legislación existente. Al respecto, la Asociación para el Progreso de las Comunicaciones (APC) sugiere que:

> En pocos lugares esas tensiones son tan palpables como en México. La complejidad política, la seria crisis de derechos humanos y los constantes cuestionamientos institucionales por parte de la sociedad civil ameritan un análisis serio, que abone al debate democrático, pensando en las oportunidades que entrega Internet para el ejercicio de los derechos humanos desde el contexto local (APC, 2016).

En consecuencia, la aplicación de mejores prácticas continuará a futuro, de acuerdo con la evolución del Internet, en su momento llamada la "autopista de la información".

COMENTARIOS FINALES

Los derechos digitales en diferentes partes del mundo retoman las leyes existentes, en especial lo referente a los derechos humanos. Es por eso que diferentes acuerdos internacionales como la *Declaración Universal de Derechos Humanos*, el Pacto Internacional de Derechos Civiles y Políticos o el Convenio sobre la Ciberdelincuencia (Convenio de Budapest) han sido las bases de normatividades para establecer ordenanzas que defiendan las prerrogativas de los usuarios en distintos países. Con ello, se investiga desde el país en que se comete un presunto ilícito a través de las TIC, en la medida en que la regulación lo permita.

Si bien concurren avances de diferente magnitud en las leyes relativas a Internet en los países seleccionados, temas generales como la neutralidad de la red, protección de datos personales,

acceso a la información pública, ciberseguridad, propiedad de autor, protocolos para el comercio electrónico u operaciones financieras han sido incorporados y son susceptibles de tener mejoras que serán añadidas por los diferentes gobiernos en cuanto los temas lleguen a la opinión pública y se busquen nuevas soluciones relacionadas con los derechos digitales.

Pese a los avances logrados a escala internacional sobre las legislaciones de Internet, aun existen países con baja cobertura en el acceso a estas tecnologías. Es por ello que dentro de los Objetivos de Desarrollo Sostenible de la ONU se incluye este reto para el beneficio de la población. Quizás el gran reto de los derechos digitales a escala mundial es que todos los habitantes del planeta tengan un pleno acceso a las TIC con calidad, como una prerrogativa universal.

BIBLIOGRAFÍA

Agenda Digital 2020 (2020). "Desde una agenda digital a la transformación digital". Recuperado de https://bit.ly/3ujuX8e

Asamblea General de la Organización de las Naciones Unidas (ONU) (2013). *68/167. El derecho a la privacidad en la era digital*. Recuperado de https://bit.ly/3LjqYyC

Asamblea General de la Organización de las Naciones Unidas (ONU) (2018). *38/... Promoción, protección y disfrute de los derechos humanos en Internet*. Recuperado de https://bit.ly/348IjcV (fecha de consulta: 9 de marzo de 2020).

Asociación para el Progreso de las Comunicaciones (APC) (2016). *Internet en México. Derechos humanos en el entorno digital*. Recuperado de https://bit.ly/3umUpd1 (fecha de consulta: 17 de abril de 2020).

Câmara dos Deputados (Cámara de Diputados de Brasil) (2015). *Marco Civil Brasileño de Internet en español*. Recuperado de https://bit.ly/3onoYva (fecha de consulta: 26 de marzo de 2020).

Cantú Rivera, H.F. (2014). La OCDE y los derechos humanos: el caso de las Directrices para Empresas Multinacionales y los Puntos de Contacto Nacional. *Anuario Mexicano de Derecho Internacional*, vol. XV, 611-658. Recuperado de https://bit.ly/3AZbXxe (fecha de consulta: 24 de marzo de 2020).

Castillo, C. del (2018). "Estos son los 17 nuevos 'derechos digitales' aprobados por el Congreso". *elDiario.es*, 18 de octubre. Recuperado de https://bit.ly/3GoNaDx (fecha de consulta: 14 de abril de 2020).

Consejo de Europa (2001). *Convenio sobre la Ciberdelincuencia (Convenio de Budapest)*. Recuperado de https://bit.ly/3AY7KJX (fecha de consulta: 5 de marzo de 2020).

Constitución Política de Colombia (2016).

Constitución Política de los Estados Unidos Mexicanos (CPEUM) [1917] (2020).

Fazit Communication GmbH (2020). Protección de los derechos humanos. En Fazit Communication GmbH; Ministerio de Relaciones Exteriores, Berlín. *La actualidad en Alemania* (50). Fráncfort del Meno, Alemania: en línea. Recuperado de https://bit.ly/3scd5JP (fecha de consulta: 24 de marzo de 2020).

Gobierno de España (2020). *Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico*.

Gloger, K. (2019). *Artículo 5: Libertad de prensa*. Mayo de 2019. Recuperado de https://bit.ly/3L7nZsQ (fecha de consulta: 25 de marzo de 2020).

Gutiérrez, B. (2014). "Brasil aprueba el Marco Civil de Internet, modelo para la Carta Magna de la Red". *elDiario.es*, 30 de marzo. Recuperado de https://bit.ly/35DAYlK (fecha de consulta: 25 de marzo de 202ww0).

Hernández Bauzá, V. (2018). *Derechos Digitales: cómo nos vigilan*. Asociación para el Progreso de las Comunicaciones. Recuperado de https://bit.ly/3LclXHR (fecha de consulta: 6 de abril de 2020).

House of Commons (Cámara de los Comunes de Canadá) (2012). Copyright Modernization Act. Recuperado de https://bit.ly/3rqxoEc (fecha de consulta: 31 de marzo de 2020).

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) (2020). *Convenio nº 108 del Consejo de Europa, de 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal*. Recuperado de https://bit.ly/3sjajCi (fecha de consulta: 17 de marzo de 2020).

Lara, J.C. (2018). USMCA y el futuro de Internet. Recuperado de: https://bit.ly/3GuuD8W (fecha de consulta: 15 de abril de 2020).

Ley Fundamental de la República Federal de Alemania (2020). Recuperado de https://bit.ly/3GkEoGM (fecha de consulta: 26 de marzo de 2020).

Library of the Congress (Biblioteca del Congreso de Canadá) (2017). Online Privacy Law: Canada. Recuperado de https://bit.ly/3onhE2N (fecha de consulta: 1 de abril de 2020).

Microsoft (2020). *Ley de privacidad del consumidor de California (CCPA)*. Recuperado de https://bit.ly/3AUKhtg (fecha de consulta: 13 de abril de 2020).

Millán Tejedor, R.J.(2006). *Distribución de libros electrónicos en redes*. Recuperado de https://bit.ly/3s8MahW (fecha de consulta: 9 de marzo de 2020).

Ministerio de Transportes y Telecomunicaciones y Subsecretaría de Telecomunicaciones (Subtel) (2010). Ley 20453. Consagra el principio de neutralidad en la red para los consumidores y usuarios de Internet. 26 de agosto de 2010. Recuperado de https://bit.ly/3upx0rf (fecha de consulta: 6 de abril de 2020).

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) (1976). *Pacto Internacional de Derechos Civiles y Políticos* (PIDCP). Recuperado de https://bit.ly/3Lcw3ZA (fecha de consulta: 10 de marzo de 2020).

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) (2011). *Principios Rectores sobre las empresas y los derechos humanos*. Recuperado de https://bit.ly/3Hrwk8p (fecha de consulta: 11 de marzo de 2020).

Organización de las Naciones Unidas (ONU) (1948). *La Declaración Universal de Derechos Humanos*. Recuperado de https://bit.ly/34xnHuH (fecha de consulta: 18 de marzo de 2020).

Organización de las Naciones Unidas (ONU) (2016). *El derecho a la privacidad en la era digital*. Recuperado de https://bit.ly/3ookB35 (fecha de consulta: 18 de marzo de 2020).

Organización de las Naciones Unidas (ONU) (2018). *Las iniciativas de datos abiertos deben tener en cuenta el derecho a la intimidad*. Recuperado de https://bit.ly/3Gq9rB5 (fecha de consulta: 13 de marzo de 2020).

Organización de las Naciones Unidas (ONU) (2020). *Objetivos de Desarrollo Sostenible* (ODS). Recuperado de https://bit.ly/3J6M1m5 (fecha de consulta: 12 de marzo de 2020).

Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2017). *El acceso y utilización desiguales podrían frenar el potencial de la economía digital, señala la OCDE*. Recuperado de https://bit.ly/32URFrQ (fecha de consulta: 19 de marzo de 2020).

Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2018). *Diversos países se comprometen a redoblar esfuerzos para impulsar una conducta empresarial más responsable mediante un nuevo instrumento desarrollado por la OCDE*. Recuperado de https://bit.ly/3GkHc6M (fecha de consulta: 24 de marzo de 2020).

Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2019). *Cuarenta y dos países adoptan los Principios de la OCDE sobre Inteligencia Artificial*. Recuperado de https://bit.ly/3J2bI77 (fecha de consulta: 23 de marzo de 2020).

Organización para la Cooperación y el Desarrollo Económicos (OCDE) y Banco Interamericano de Desarrollo (BID) (2016). *Políticas de banda ancha para América Latina y el Caribe*. Recuperado de https://bit.ly/3GrFn7W (fecha de consulta: 20 de marzo de 2020).

¿Quién defiende tus datos? (2020). Recuperado de https://bit.ly/3H-qHD0Q (fecha de consulta: 8 de abril de 2020).
Red en Defensa de los Derechos Digitales *(R3D) (2018). El acuerdo comercial entre Canadá, Estados unidos y México (USMCA) amenaza gravemente los derechos digitales*. Recuperado de https://bit.ly/34zcN7n (fecha de consulta: 31 de marzo de 2020).
Red en Defensa de los Derechos Digitales (R3D) (2020). *Alemania*. Recuperado de https://bit.ly/3HqA2zh (fecha de consulta: 26 de marzo de 2020).
Ruiz, C. (2016). *Derechos digitales en México. ¿Hacía donde vamos?* Recuperado de httpshttps://bit.ly/3J5iysO (fecha de consulta: 17 de abril de 2020).
Sánchez, Á. (2019). "El abogado general da la razón a Google y limita el derecho al olvido a la UE". *El País*, 10 de enero. Recuperado de https://bit.ly/3JiZmIb (fecha de consulta: 31 de marzo de 2020).
Senado de Colombia (2020). *Leyes de la República*.
Sobre la normativa web en Chile (2020). Recuperado de https://bit.ly/3HtPMl8 (fecha de consulta: 6 de abril de 2020).
Trejo García, Elma del Carmen (2006). *Regulación Jurídica de Internet*. Recuperado de https://bit.ly/3gkTMrZ (fecha de consulta: 9 de marzo de 2020).

CAPÍTULO 03

CIUDADANÍA DIGITAL, PRIVACIDAD Y PROTECCIÓN DE DATOS PERSONALES

JIMENA MORENO GONZÁLEZ*
FRANCISCO ADRIÁN GARCÍA GARCÍA**

* Profesora de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE), abogada por la Universidad Nacional Autónoma de México (UNAM) y maestra en dirección internacional por el Instituto Tecnológico Autónomo de México (ITAM). Especialista y profesora en derecho internacional público, regulación, privacidad y datos personales.

** Economista (UNAM) y maestro en ciencias sociales por la Facultad Latinoamericana en Ciencias Sociales (Flacso-México). Profesor asociado en la división de Administración Pública, del Centro de Investigación y Docencia Económicas (CIDE), especializado en desarrollo social y apropiación de las tecnologías de la información y la comunicación.

Las tecnologías de la información y la comunicación (TIC) han revolucionado nuestra forma de involucrarnos en distintas esferas de la vida social, desde la extensión de su uso, a finales del siglo XX. Hoy en día, con sus múltiples posibilidades de interacción inmediata, facilitan el día a día de millones de usuarios en el mundo. El ámbito público ha sido parte de estos cambios: por el lado de quienes gobiernan, cada día es más notorio el papel que tienen las TIC en cuanto a la comunicación política y gubernamental, así como su papel en el diagnóstico para el diseño de políticas públicas y la toma de decisiones; en cuanto a los ciudadanos comunes, las nuevas tecnologías permiten comunicar a las masas de los principales acontecimientos, generar discusión y promover el involucramiento en torno a las acciones de quienes gobiernan. Estos hechos han llevado a que se hable cada vez más sobre la construcción de ciudadanía digital como nunca en la historia, las sociedades del globo cuentan con desarrollos tecnológicos que abren la posibilidad de formas innovadoras de participación en sociedad y de resolución a problemas públicos. No obstante, este panorama se caracteriza por su desigualdad, ya que no todos los países ni todos los individuos han podido aprovechar las tecnologías de la misma manera: mientras que en países como Estonia el gobierno electrónico, con sus trámites y servicios y sus mecanismos de participación plenamente digitalizados, funcionan a plenitud, las regiones periféricas se enfrentan a transiciones tecnológicas más lentas, mediadas por desigualdades sociales que tienen un profundo carácter histórico.

Es en este escenario, donde apareció la pandemia de la Covid-19 a principios de 2020. De manera inmediata, los gobiernos de todo el mundo se valieron de los avances tecnológicos para coordinar acciones que pudieran coadyuvar a mitigar el nuevo gran riesgo para la salud pública. A reserva de conocer el balance final, y en comparación con situaciones similares acaecidas siglos atrás, es innegable que las TIC han jugado un papel dominante en mejorar la forma en la que la humanidad ha enfrentado la emergencia. No obstante, al margen de la coyuntura, es necesario reflexionar sobre el contexto en el que se han implementado estas medidas y cuáles son los alcances en la marcha de la vida pública.

El objetivo del presente texto es promover el debate en este ámbito, mediante el análisis de la participación de la ciudadanía digital. Partimos del hecho de que existe evidencia sustantiva para afirmar su gran potencial para el involucramiento en los asuntos públicos, no obstante, no deben pasarse por alto los condicionantes en la estructura social que la hacen inaccesible a gran parte de la población, y que están asociados a la llamada brecha digital. Por tanto, en la segunda sección del documento, analizamos qué es la ciudadanía digital y cuáles son las dimensiones desde donde se le estudia. En el apartado siguiente, abordamos el alcance de la ciudadanía digital en la vida pública a partir de dos enfoques: desde un nivel de régimen, donde identificamos los principales elementos de por qué la ciudadanía digital mejora la vida en democracia; y desde el nivel de gobierno, acotado a cómo el gobierno electrónico contribuye a la gestión eficiente de recursos públicos, y algunas de sus principales implicaciones en materia de cumplimiento a derechos. En la cuarta sección del documento, a partir de la pregunta de quiénes pueden ser ciudadanos digitales en México, revisamos algunos datos notables para dimensionar la brecha digital como condicionantes para el ejercicio de la ciudadanía. Posteriormente, vinculamos las implicaciones de la ciudadanía digital respecto de algunas acciones principales que han tomado los gobiernos en el mundo para hacer frente a la pandemia de la Covid-19. Para tales efectos, acotamos nuestro análisis a los campos de la salud pública y la educación, y discutimos sus beneficios y posibles problemas en términos de derecho a la privacidad y a la protección de datos personales. Por último, elaboramos un apartado con conclusiones y reflexiones para el futuro.

NOCIONES PARA COMPRENDER LA CIUDADANÍA DIGITAL

Para abordar el fenómeno de la ciudadanía digital, primero es necesario entender qué es la ciudadanía; Marshall (como se cita en Sojo, 2002: 27) la define como “un estatus asignado a todos aquellos que son miembros plenos de una comunidad. Todos los que posean dicho estatus son iguales con respecto a derechos y deberes”.

Este mismo autor identifica que la ciudadanía se constituye por tres pilares: derechos civiles, relacionados con la libertad de expresión y de culto, por ejemplo; derechos políticos, asociados al derecho de participación política; y derechos sociales, que se refieren al derecho al bienestar económico. A partir de esta definición, es preciso resaltar que la ciudadanía es, en primer lugar, un estatus asignado. Ahora bien, aunque en los Estados modernos la ciudadanía está asociada con la idea de igualdad, propias de la Ilustración, en términos reales el acceso a dicho nivel se caracteriza por tener un carácter de proceso histórico, relacionado con movilizaciones políticas. Por ejemplo, en los tiempos de la independencia de las Trece Colonias, se discutía en torno a si el derecho a la participación política debería estar reservado solamente para hombres propietarios. En ese caso, la inclusión de mujeres y descendientes de esclavos como ciudadanos con facultades de participar en la vida pública de dicho país fue un proceso que se consolidó hasta la mitad del siglo XX. Dicho lo anterior, para abordar el tema de la ciudadanía digital en los apartados subsecuentes, rebasamos las definiciones normativas, que acotan a los ciudadanos en términos de aquellos individuos mayores de edad, sujetos a derechos y obligaciones con el Estado, con el fin de adoptar un enfoque más cercano hacia la un esquema de integración en la sociedad y las condiciones de posibilidad de participación de lo público.

El caso de George Floyd, el hombre asesinado por la policía de Minneápolis, es un ejemplo contundente de las manifestaciones de la ciudadanía digital. El video se hizo viral a las pocas horas, se filtraron datos personales de la víctima y el victimario, un grupo de ciudadanos salió a las calle de la ciudad a manifestarse, con consignas de indignación y exigencia de justicia, y la corporación de policía local separó del cargo a los oficiales relacionados con el caso. No obstante, a los pocos días, las manifestaciones rebasaron las fronteras estatales y se esparcieron por Estados Unidos; en los estados del sur histórico revivieron los debates en torno a la disputa de la memoria del país, se manifestaron consignas contra estatuas erigidas a antiguos esclavistas; el paroxismo de la ola de protestas ocurrió cuando gran número de ciudadanos se manifestaron afuera de la Casa Blanca. Pero el asunto no paró ahí y la noticia llegó a prácticamente la totalidad del globo. En México, el

asesinato de George Floyd fue la pauta para que en redes sociales usuarios comunes y figuras públicas se manifestaran en contra del racismo y sus repercusiones, no sólo en Estados Unidos sino también en el contexto mexicano (González, 2020).

TRES DIMENSIONES DE LA CIUDADANÍA DIGITAL: NORMA, BRECHA DIGITAL Y SUBJETIVIDAD

De vuelta a la generalidad de la definición de la ciudadanía digital, retomamos la propuesta de Jorring, Valentim y Porten-Cheé (2019) para exponer las tres dimensiones desde las cuales se aborda la definición de ciudadanía digital: el campo normativo, las condiciones y el contexto donde tiene lugar. Acorde con estos mismos autores, en la primera dimensión el concepto se entiende como la forma ideal de actuar en línea, en consideración de debates éticos y morales que tiene consigo la participación de lo público a través de Internet. Para ejemplificar, los autores recuperan la definición de Curran y Ribble (como se cita en Jorring, Valentim y Porten-Cheé, 2019: 17), que define a la ciudadanía digital como las normas del comportamiento apropiado y responsable [de la participación] respecto del uso de la tecnología. Dentro de esta aproximación, se discute también la relación que existe entre la educación y la ciudadanía digital (Ribble, 2012; Gleason y von Gillern, 2018), a partir de preguntarse cuáles son los valores y las habilidades necesarias que han de transmitirse en los sistemas educativos para que los estudiantes puedan formarse adecuadamente para participar de manera activa en la interacción con sus pares a través de medios digitales (Jorring, Valentim y Porten-Cheé, 2019: 18).

En contraste con la perspectiva normativa, se encuentra también aquella que apela al entendimiento de la ciudadanía digital desde sus condicionantes estructurales, así como los estudios con una perspectiva del contexto. Para las referencias correspondientes al primer grupo, la ciudadanía digital se entiende como la posibilidad de cada cual para participar en la sociedad en línea a partir de un número considerable de diferencias en el acceso; en

consecuencia, la potencia del Internet para mejorar las democracias sólo podrá concretarse en la medida en que la totalidad de la población se encuentre en condiciones de igualdad para acceder a la red (Mossberger, Tolbert y McNeal, 2008; Jorring, Valentim y Porten-Cheé, 2019: 18). Como se observa, la idea de abordar a la ciudadanía digital desde las desigualdades para ejercerla está en línea con la dimensión del derecho al bienestar propuesta por Marshall (Sojo, 2002).

¿Dónde radican las desigualdades mencionadas? La más evidente es el acceso a un ordenador con conexión a Internet, pero los estudios de esta índole se orientan a estudiar otras desigualdades, como la velocidad de la conexión, tipo de dispositivo para el acceso, hábitos en línea, capacidades y habilidades para el logro de diversas tareas en los dispositivos, el tiempo conectado a la red (entre otras), en relación con la pertenencia a grupos socioeconómicos que pueden estar definidos a partir de ingreso, edad, escolaridad, tipos de localidad, de oficio (por mencionar algunos); y es en tales diferencias donde se fundamentan las llamadas brechas digitales. En continuidad con esta perspectiva, Shelley *et al.* (como se cita en Jorring, Valentim y Porten-Cheé, 2019: 19) afirman que la ciudadanía digital es un proceso de conversión influenciado por aptitudes orientadas a tener como consecuencia el cierre de brechas digitales. De esta última definición es preciso hacer énfasis en la intención del término *proceso*, lo cual sugiere que la sola existencia de Internet, redes sociales, foros, bases de datos abiertas y demás no deviene en la instrumentación automática de la ciudadanía digital, sino que ésta es posible solamente en la medida en que los gobiernos promueven activamente el acceso a la red y a las capacidades para apropiarse de su uso. Finalmente, queda la perspectiva en la que la ciudadanía digital es entendida como un concepto dependiente del contexto, donde subyace la interacción del ejercicio de la ciudadanía clásica con factores políticos, sociales, culturales y socioeconómicos (Jorring, Valentim y Porten-Cheé, 2019). Esta corriente de aproximación se centra más en las experiencias sensibles que los ciudadanos tienen cuando ejercen su ciudadanía digital y en las formas en que se apropian de los espacios virtuales para reivindicar derechos o generar acciones relacionadas con el activismo.

Los estudios de este campo pueden tener una perspectiva más escéptica en cuanto a las posibilidades de Internet para ampliar y mejorar la participación de los ciudadanos en los asuntos públicos y su interacción con las autoridades gubernamentales, ya que se centran en observar cómo estructuras existentes de poder y exclusión se entrelazan con los usos de las nuevas tecnologías para reproducir estos esquemas y generar nuevas experiencias de sometimiento y segregación en los sujetos. Por ejemplo, autores como Latonero *et al.* (2019) identifican de qué manera la identidad digital reproduce mecanismos de segregación social entre migrantes refugiados en Italia, mientras que Eubanks (2014) analiza de qué manera el uso de datos masivos para la asignación de recursos en programas de asistencia social contribuye a perpetuar esquemas de discriminación entre poblaciones marginadas y precarizadas. Conforme a lo expuesto, las formas de involucrarse en sociedad a través de la ciudadanía digital pueden tener múltiples aristas, y resalta el hecho de cómo la apropiación de las TIC ha redefinido la construcción de ciudadanía fuera de los espacios en línea. Así, en los párrafos siguientes abordaremos algunas de estas dimensiones, profundizaremos en algunos aspectos principales de esta redelimitación, relacionados con el cumplimiento de derechos civiles, políticos y económicos.

CIUDADANÍA DIGITAL Y PARTICIPACIÓN PÚBLICA

Para el desarrollo del presente apartado proponemos analizar los alcances de la ciudadanía digital desde dos aristas analíticas distinguibles: régimen y gobierno. El gobierno lo asumimos como un núcleo de poder acotado a las posiciones en la cúspide del aparato de Estado, a partir del cual se desprenden la dirección política y los aparatos burocráticos para la gestión pública (O'Donnell, 2015: 14; Cotta, 1996: 313-316; Panebianco, 1996: 370, 392). Por su parte, el régimen puede definirse como los patrones que determinan los canales de acceso a las principales posiciones del gobierno (O'Donnell, 2015: 13). Aunque en el plano tangible los dos niveles de análisis están superpuestos, creemos que este esquema es útil

para comprender el desarrollo de la ciudadanía digital. De forma más concreta, al analizarla desde su impacto en la esfera de régimen, establecemos un nexo entre ciudadanía digital y democracia, en el entendido de que la expansión del uso de las TIC promueve la participación política y la construcción de mayorías, ya que, mediante el constante intercambio de información entre ciudadanos, estos pueden involucrarse mejor en la toma de decisiones públicas, controlar las acciones de sus gobernantes y coordinar acciones para tener incidencia en la sociedad.

Por su parte, al acotar la esfera de análisis en el nivel gubernamental, aunque no sea deseable, se puede desvincular el lazo entre ciudadanía digital y democracia; en estricto sentido, es posible que haya ciudadanos digitales en sociedades sin democracia, en el entendido de que los gobiernos pueden aprovechar de igual forma el desarrollo de las TIC para la provisión y gestión de servicios públicos. De este modo, acotamos las implicaciones de ciudadanía digital respecto de tareas más cercanas a la administración pública eficiente, orientadas a partir de la adopción paulatina del gobierno electrónico.

I) La ciudadanía digital en los procesos contemporáneos de democratización

El propósito del presente apartado es definir de qué manera el ejercicio de la ciudadanía digital puede contribuir a mejorar las democracias. Para tales efectos, es preciso partir de las razones que puede haber para que las sociedades acuerden vivir en este régimen. Dahl (1999: 117-118) apunta que los gobiernos democráticos ofrecen "en medida mucho mayor que cualquier otra alternativa, un proceso pacífico y ordenado por medio del cual la mayoría de los ciudadanos pueden instarlo a hacer lo que ellos más desean que haga y a evitar hacer lo que más desean que no se haga", todo ello, dentro de un marco de pretensión de búsqueda de la máxima libertad posible, la promoción del desarrollo personal y la disponibilidad de oportunidades para la satisfacción de preocupaciones políticas urgentes. Dicho lo anterior, Schumpeter (1983: 343) define al régimen democrático como el sistema institucional donde los individuos adquieren poder de decisión a través de una lucha de competencia por el voto.

Estas luchas deben entenderse como los procedimientos electorales, que son requisito mínimo para los regímenes democráticos, y que han de cumplir con características como la regularidad del procedimiento, la universalidad del voto y la igualdad de condiciones para quienes contienden por el poder. A partir de las ideas expuestas, se pueden identificar los primeros dos principios por los que la incorporación de las TIC en el ejercicio de la ciudadanía mejora la vida en democracia: establecen circunstancias para la participación de mayorías y, de este modo, contribuyen a dotar a los individuos de poder de decisión. Internet, con grandes cantidades de información en tiempo real y sus múltiples plataformas de interacción, faculta a quienes cuentan con una conexión a la red a tener acceso continuo al seguimiento de las acciones de quienes gobiernan y, de este modo, poder obtener mejores condiciones para discernir por quién votar. No obstante, esta primera visión se encuentra acotada al procedimiento de los mecanismos electorales, cuando, en realidad, la vida democrática exige contemplar la formación de instituciones que apuntalen la incorporación de la ciudadanía en la toma de decisiones (Dahl, 1999). Ahora bien, ¿de qué manera se construyen las instituciones democráticas? Castoriadis (1995) sostiene que éstas no surgen a partir de la existencia de sujetos ideales que están dotados *a priori* de interés en la *res* pública, sino que se construyen en la práctica misma de actitudes democráticas en el día a día, a manera de participación permanente. En términos más concretos, la democracia y la participación ciudadana exigen educación y práctica en situaciones comunes, y es esta la tercera razón por la que Internet puede mejorar las democracias, ya que cuenta con espacios y mecanismos para que, de manera constante, los ciudadanos puedan informarse de los asuntos públicos, sean internacionales, nacionales o locales, pero no sólo para elegir por quién votar, sino también para emitir sus opiniones y para entrar en contacto con las posturas de otros (Cáceres *et al.*, 2015).

Este punto da la pauta para la cuarta razón: Internet es un espacio para el intercambio de opiniones, y también sirve como punto de referencia para que grupos de ciudadanos coordinen acciones para emprender actos políticos más allá de sus actividades en línea, que pueden estar asociadas a movimientos sociales (Sierra

y Gravante, 2016). En este rubro, puede retomarse el ya mencionado caso de George Floyd, donde miles de ciudadanos salieron a manifestar su rechazo a las calles, o el ejemplo paradigmático de la *primavera árabe*, a comienzos de la década de 2010, donde, a través del uso de sitios como YouTube y Twitter, numerosos jóvenes manifestaron su deseo de vivir en democracia y de cambiar las formas de participar en la vida pública de sus respectivos países, y cuyas consecuencias persisten en la región (Bowen, 2019). A partir de lo anterior, se puede comenzar a esbozar la quinta razón por la cual la ciudadanía digital puede mejorar la vida en democracia, que es la posibilidad que tiene Internet para replantear el involucramiento de la ciudadanía en la toma de decisiones públicas. Para este punto, apelaremos a dos cuerpos de literatura especializada que, aunque no necesariamente comparten las mismas premisas, son útiles para esclarecer el tema. En primer lugar, se encuentran los estudios en el campo de la gobernanza. Esta perspectiva tiene un enfoque en la dimensión gerencial del gobierno y su papel en la resolución de problemas públicos y en la gestión de recursos colectivos. Así, la promoción de la ciudadanía digital implica la instrumentación de esquemas de gobernanza, donde los tomadores de decisiones se valen de herramientas de comunicación y participación para crear soluciones conjuntas con el resto de los actores interesados, como pueden ser académicos, consultores especializados, activistas, empresarios o simples ciudadanos de a pie. Con esta premisa surge el llamado gobierno abierto, que puede definirse, de acuerdo con la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2016: 1), como "Una cultura de gobernanza basada en políticas públicas y prácticas innovadoras y sostenibles que se basan a su vez en unos principios de transparencia, rendición de cuentas y participación que promueven la democracia y el crecimiento inclusivo".

En este campo, Valenti *et al.* (2015) distinguen la proliferación de *gobernautas* en las principales ciudades de América Latina, entendidos como los gobernantes que se valen de las redes sociales para mostrar cercanía con la ciudadanía, escuchar demandas y comunicar acciones de gobierno y posturas en debates públicos; es decir, cada vez más los tomadores de decisiones consideran las redes sociales como un medio para el diálogo con

los ciudadanos. Dentro de este tipo de medidas destacan también las de portales de gobierno y desarrollo de aplicaciones. En el primer caso, los portales electrónicos se han convertido en espacios para comunicar acciones, rendir cuentas y poner a disposición de la ciudadanía distintos mecanismos de consulta de información pública. En cuanto a las aplicaciones para dispositivos móviles en entornos urbanos, estas funcionan como un medio para el levantamiento de demandas de miles o millones de ciudadanos, de modo que los gobernantes, a través de tecnologías de procesamiento de datos masivos, pueden hacer diagnósticos específicos en cuanto a las necesidades concretas en campos como la infraestructura pública o la seguridad.

Además de la literatura sobre gobernanza, existe otro cuerpo de teoría que permite identificar el ejercicio de la ciudadanía digital con los mecanismos de control (*accountability*). En la literatura existen al menos tres mecanismos de control: vertical, horizontal y social. El control vertical se refiere al voto, ya que a través de este mecanismo de participación, la ciudadanía puede premiar o castigar a sus gobernantes. No obstante, esta figura es insuficiente, debido a que es imposible saber a ciencia cierta si un ciudadano está utilizando su voto para elegir una agenda que sea afín a sus intereses o si está castigando a un gobernante en turno (Przeworski, Manin y Stokes, 2002: 38). Por otra parte, O'Donnell (2001) identifica los mecanismos de control horizontal como aquellas agencias gubernamentales que tienen la facultad de controlar o sancionar a otros agentes cuando, en principio, cometen actos que pueden ser consideradas como delito. Finalmente, el tercer tipo de control refiere a aquellos casos en los que grupos de la sociedad civil, organizados en movimientos sociales o en organizaciones no gubernamentales, monitorean la legalidad de las acciones del Estado, muchas veces orientados por escándalos mediáticos que pueden estar asociados a casos de corrupción (Peruzzotti y Smulovitz, 2002: 28). En ese sentido, un caso emblemático fue la renuncia del primer ministro islandés en 2016 (s/a, 2016), luego de que la filtración de los llamados *Panama Papers* lo vinculó a actos de corrupción. Después de que la información se hiciera viral en redes sociales, los islandeses participaron durante días de protestas en las calles, el gobierno del país tuvo que aceptar la renuncia y convocar a nuevas elecciones para el Ejecutivo.

Hasta este punto, se han mencionado dos formas de cambiar el involucramiento de la ciudadanía en la toma de decisiones: mediante esquemas digitales en los que los gobernantes recuperan la opinión ciudadana y a través de movilizaciones sociales. Sin embargo, queda uno más por destacar, y es la posibilidad de cambiar las reglas en cuanto a quiénes participan directamente en la toma de decisiones. Este mecanismo implica, en primer lugar, replantear los esquemas de representación democrática, entendida como la participación de aquellos individuos que hablan en nombre de un grupo en particular (Gurza e Insunza, 2010). En ese sentido, Internet puede llegar a modificar los términos en los que lo representantes hablan en nombre de sus representados, debido a que da voz directa a estos últimos. Así, es posible pensar en formas de participación directa en las cuales los ciudadanos se involucren en consultas con carácter vinculante a través del uso de dispositivos móviles y ordenadores. En resumen, a la pregunta de por qué el ejercicio de la ciudadanía a través de Internet contribuye al mejoramiento de la vida democrática, esbozamos los siguientes elementos: *1)* quien cuenta con una conexión a Internet, accede constantemente al desarrollo de los asuntos públicos; *2)* dota de gran información para que los ciudadanos puedan elegir por quién votar; *3)* contribuye a la práctica ciudadana en el día a día, ya que permite el diálogo con otros ciudadanos; *4)* permite coordinar acciones colectivas con otros ciudadanos; *5)* replantea los mecanismos de involucramiento de los ciudadanos en la toma de decisiones públicas.

II) Gobierno electrónico: eficiencia para la asignación de recursos públicos

En recuperación del marco analítico propuesto al inicio del apartado, dejamos de lado la perspectiva de la ciudadanía digital y su relación con el régimen democrático, para dar cabida a sus implicaciones en cuanto a la administración pública eficiente y lo correcta gestión de los asuntos públicos. Posteriormente, proponemos una reflexión sobre cómo la instrumentación de estos mecanismos debe pensarse todo el tiempo en un marco de protección de derechos civiles. Dado que, tal como especificamos, ambas dimensiones, régimen y gobierno, son esferas superpuestas en términos reales, en el párrafo anterior ya se adelantaron algunas características de las posibilidades de Internet en la Administración, cuando se habló de los esquemas de gobernanza y de gobierno abierto. Por tanto, el eje de la exposición se colocará sobre la manera en cómo el gobierno electrónico se ha orientado a hacer más eficiente la asignación de recursos públicos. En términos formales, este puede definirse como aquellas actividades que el gobierno desarrolla a partir del uso de las TIC, con el fin de mejorar la eficiencia en la gestión pública y en los servicios públicos, en un marco regido por la transparencia (Castoldi, como se cita en Rodríguez, 2004: 5). Como puede observarse, en estos términos, el gobierno es entendido como un ente orientado a la gestión y provisión, y debe perseguir principios de eficiencia tal y como ocurre con las empresas. La idea es que los gobiernos puedan eficientar sus procesos burocráticos, con el fin de ofrecer trámites y servicios de calidad. El gobierno electrónico se ha instrumentado como un medio para reducir el tiempo en distintos tipos de trámites; transparentar los procesos, como mecanismos de combate a la corrupción, y valerse de la aplicación de tecnologías de recopilación y análisis de datos con el fin de implantar políticas públicas con soluciones óptimas (Sandoval-Almazán y Mendoza, 2011). Algunos ejemplos de la aplicación en México se observan en el trámite del acta de nacimiento, la puesta a disposición de chats para la atención ciudadana en las páginas gubernamentales, la posibilidad del pago de impuestos en línea, la transferencia de recursos a la población beneficiaria mediante el uso de banca en línea, entre otros. Visto así, es sobresaliente la manera en la que el gobierno electrónico puede mejorar la calidad de los servicios ofrecidos por los aparatos burocráticos del Estado.

Sin embargo, este apuntalamiento de la eficiencia de los servicios públicos abre la puerta a algunas situaciones problemáticas que, aunque no son exclusivas del índole pública, suelen tener una repercusión diferenciada, dada la dimensión política de los gobiernos. Tal como sucede en la esfera de las empresas privadas, desarrollar este tipo de aplicaciones en la gestión pública requiere del levantamiento, gestión y resguardo de gran cantidad de información sobre la ciudadanía, lo que lleva a discutir: quién tiene acceso a esos datos, qué medidas de seguridad se instauran para su uso y qué actores están involucrados en su tratamiento.

Dado que es una relación directa del individuo con el Estado por medios digitales, se debe crear un marco regulatorio que garantice la protección de la información digital e imponga sanciones claras a los responsables por un uso indebido. Tener certeza jurídica es indispensable para generar una relación de confianza entre individuos y el gobierno.

A manera de ejemplo, estas discusiones suelen aparecer cuando los gobiernos implementan identificaciones digitales para sus ciudadanos, y es que, aunque son múltiples las ventajas de contar con una identidad digital que se convierta en un identificador único para los diversos trámites que los ciudadanos requieren del gobierno, su instrumentación debe asegurar que la información esté debidamente protegida y almacenada, y no se use más que para los fines para los que fue recabada. En el caso de nuestro país, el derecho a la protección de datos personales está consagrado en el artículo 16, segundo párrafo de la *Constitución de los Estados Unidos Mexicanos* y está catalogado como un derecho humano. Este tipo de mandatos en las leyes son de suma importancia, ya que el uso cada vez mayor de aplicaciones y el almacenamiento de datos personales se convierte en un desafío cada vez mayor para los gobiernos y desarrolladores de tecnología, para que puedan implementar medidas de seguridad y proteger la información almacenada, y así evitar el robo de identidad, los ciberdelitos y el abuso en el uso de la información. La cuestión de fondo es que la aplicación de las TIC en la gestión pública se lleve a cabo en un marco de diseño institucional con mecanismos de contrapesos para que los gobernantes no tengan posibilidades de hacer uso indebido de los datos de la ciudadanía. El contexto actual lo exige, ya que, tanto gobierno como empresas, adoptan una postura de vigilancia generalizada, que buscan obtener información para fines comerciales o políticos, y dejan en estado de vulnerabilidad e indefensión a los ciudadanos.

Así, es importante ahondar en las políticas de privacidad de los responsables en el manejo y almacenamiento de la información y en la exigibilidad de hacer transparente el uso de la información para que se use únicamente para los fines para los que fue recabada (Moreno Muñoz, 2017). En el apartado sobre medidas para hacer frente a la Covid-19 se ahonda más en este tema.

III) ¿Quiénes pueden ser ciudadanos digitales?

Como se mencionó en la primera sección, la brecha digital es un factor fundamental cuando se quiere hablar de ciudadanía en esa materia, ya que condiciona permanentemente su apropiación y ejercicio. Es decir, por muchas que puedan ser las ventajas del uso de Internet para la incorporación de mayorías en la vida pública, estos beneficios se anulan cuando buena parte de la población no tiene acceso a la red. En el presente apartado profundizamos en las dimensiones de la brecha digital y ofrecemos algunos datos relevantes para México.

Aunque el uso del discurso de la sociedad de la información tiene por lo menos 25 años, fue en 2017 cuando por primera vez en la historia la población usuaria de Internet en el mundo fue mayoría, al pasar a ser 51%. Dicho de otro modo, hasta hace no más de cinco años, la mayoría de la población mundial estaba excluida de fenómenos como el voto electrónico, la telesalud, la educación a distancia, el comercio electrónico, los juegos en línea, y de sitios como Facebook, Youtube o Twitter. Si bien en un primer momento de la ola de estudios de brecha digital el foco estuvo concentrado entre usuarios y no-usuarios de Internet, los horizontes se han profundizado y las aristas se han diversificado. Ahora mismo no sólo es necesario conocer si se cuenta con acceso a una conexión, sino también si se cuenta con acceso doméstico, cuál es la velocidad, qué tipos de dispositivos se utilizan, cuánto tiempo se usa y para qué se usa, por mencionar sólo algunos; los ejes de esta desigualdad en el acceso y uso de las TIC se observan entre grupos por nivel de ingreso, de escolaridad, edad, género, tipo de zona geográfica –rural o urbana–, posición en el mercado laboral, ubicación al interior de una ciudad, tipo de ocupación, sector de la economía, entre otros. Es decir, la brecha digital, entendida desde su multiplicidad de dimensiones, se explica entonces como una consecuencia de la expansión del uso de las TIC en sociedades que cuentan con estructuras jerarquizadas y apriorísticas de desigualdad.

El mapa 1 presenta dos dimensiones de la brecha digital en México: las diferencias geográficas y las distinciones de uso entre grupos de edad. Para el primer caso, existe un patrón visible. Las entidades que se posicionan en el grupo con menor porcentaje de hogares conectados –entre 25% y 44%– se ubican en la región

MAPA 01.

INTERNET EN MÉXICO: PORCENTAJE DE HOGARES CONECTADOS Y DIFERENCIAS EN FRECUENCIA DE USO EN GRUPOS DE EDAD, 2018

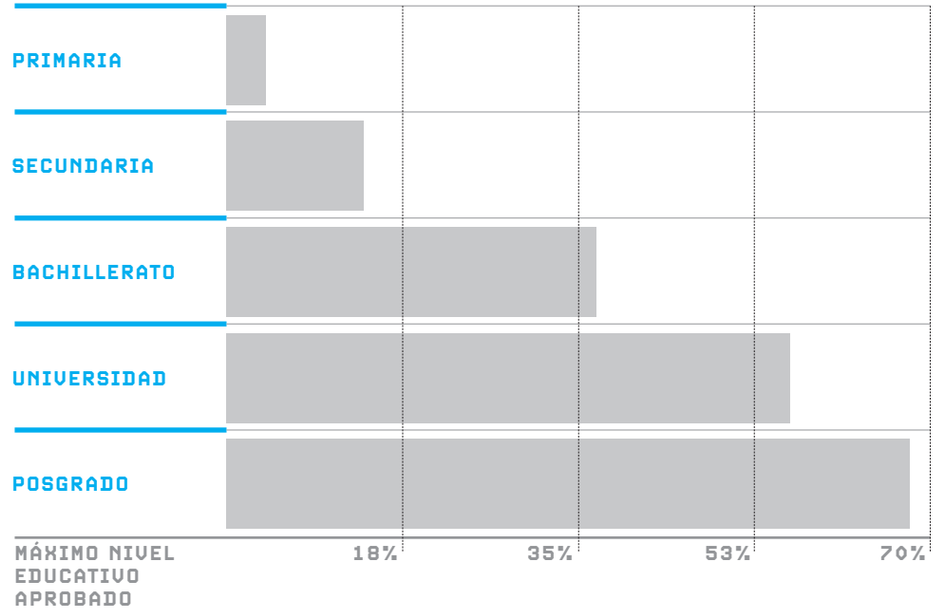
centro-sur del país, con dos importantes excepciones: la zona geográfica delimitada entre Ciudad de México y Jalisco –que abarca Guanajuato, Querétaro y Estado de México–, y la zona delimitada por las entidades de la península de Yucatán. Es decir, en términos de conectividad en hogares: existen mayores avances en los estados del norte. Por otra parte, fuera de esta región, sobresalen como entidades integrantes del grupo con mayor porcentaje de conectividad en hogares –entre 57% y 81%– Ciudad de México, Jalisco y Quintana Roo. De los primeros dos puede inferirse que su nivel de conectividad se explica porque son las dos zonas metropolitanas más grandes del país; por su parte, el de Quintana Roo, atípico en el sur, está asociado con su carácter de destino turístico internacional.

FUENTE:

elaboración propia con datos de Encuesta Nacional sobre Disponibilidad y Uso de las TIC en los Hogares, Inegi, 2018.

GRÁFICA 01.

PROPORCIÓN DE MAYORES DE 18 AÑOS QUE USARON INTERNET PARA INTERACTUAR CON GOBIERNO CONFORME EL NIVEL EDUCATIVO, 2018



FUENTE:

elaboración propia con datos de Encuesta Nacional sobre Disponibilidad y Uso de las tic en los Hogares, Inegi, 2018.

Para examinar la dimensión de brechas digitales por edad, a partir de los datos de la Encuesta Nacional sobre Disponibilidad y Uso de las TIC en los Hogares (ENDUTIH, 2018: separamos a la población de cada entidad en dos grupos: entre 6 y 45 años –jóvenes–, y mayores de 45; identificamos la proporción de población que declaró usar Internet a diario en cada grupo; y, mediante un coeficiente, comparamos la proporción de usuarios diarios de la red entre ambos grupos de edad.[1] Los resultados se muestran en el mapa –mayor área de las circunferencias significa mayor diferencia en la frecuencia de uso entre los dos grupos de edad–; resalta que las mayores diferencias se encuentran en aquellas entidades con el menor porcentaje de hogares conectados a Internet. Es decir, tener una conexión en el hogar es un factor asociado con la inclusión de población con mayor edad en el uso de Internet.

1 Si el valor del coeficiente es de 1, significa que la proporción de población que usa Internet a diario es exactamente igual entre jóvenes y mayores. Los valores mayores a 1 refieren a mayor uso entre jóvenes, y valores menores a 1 significan mayor uso entre mayores.

Ahora bien, en la primera sección del documento se mencionó que la educación es un factor clave para el desarrollo de la ciudadanía digital, ya que, a la vez que orienta el sentido de participación pública, dota de habilidades necesarias para el uso y apropiación de las herramientas tecnológicas. Esta situación se manifiesta con mayor claridad en la gráfica 1. Con datos de la misma ENDUTIH 2018: separamos a la población mayor de 18 años en niveles educativos conforme al último grado aprobado; dentro de cada nivel identificamos a la proporción de población que declaró haber usado Internet en el último año para interactuar con el gobierno; y, por último, comparamos las proporciones entre los niveles. Los resultados son evidentes: a mayor nivel educativo, mayor proporción de población que usa la red para tener interacción con representantes y tomadores de decisiones públicas. Si bien estas son apenas tres dimensiones de la brecha digital, son suficientes para dimensionar los retos a los que se enfrenta el país para la construcción exitosa de ciudadanos digitales, por tanto, es de suma importancia que estos condicionantes estructurales sean tomados en cuenta cada que el gobierno se vale del uso de las TIC para plantear soluciones a los problemas públicos.

RECURSOS DIGITALES COMO MEDIDAS DE RESPUESTA ANTE LA PANDEMIA DE LA COVID-19

Como se adelantó en la introducción, el uso de las TIC ha sido un componente fundamental en la estrategia de combate a la pandemia, y su contribución ha sido exitosa para comunicar la evolución de la pandemia, las principales acciones de los gobiernos, así como para coordinar medidas que inciden en el confinamiento. Sin embargo, estos hechos también han permitido vislumbrar algunos problemas principales en cuanto a la construcción y el ejercicio de la ciudadanía digital. Cabe especificar que el propósito del presente apartado no es proponer que los gobiernos dejen de valerse de las TIC para hacer frente a los problemas públicos, sino que, por el contrario, la pretensión es señalar aquellos temas que, fuera de la coyuntura de emergencia, existen y necesitan ser visibilizados y discutidos, con el fin de que el desarrollo y uso de tecnologías se plantee en términos de la ampliación del acceso a derechos y de la inclusión en la vida democrática del país. Para tales efectos, acotamos el análisis a las medidas emprendidas en materia de salud y educación, y en ambas buscamos responder: ¿qué acciones se han tomado? ¿De qué manera pueden ser problemáticas en términos de ciudadanía digital? y ¿qué medidas se pueden considerar para mejorar el acceso a derechos?

I) Salud

Las principales acciones de salud pública para hacer frente a la pandemia mediante el uso de las TIC están relacionadas con la promoción de recursos de telesalud, tanto para positivos o sospechosos de coronavirus, como para quienes presentan otro tipo de padecimientos no relacionados con la pandemia, con el propósito de evitar que la población tenga que salir de casa para acceder a los servicios de salud. En términos concretos, el impulso a la telesalud incluye: expedición de recetas médicas electrónicas, uso del historial clínico electrónico, consultas por videollamada y chats para el monitoreo de pacientes. La aplicación más destacada en este rubro es el rápido desarrollo de aplicaciones móviles auxiliares en el combate a la pandemia; en términos generales, estas plataformas son capaces de auxiliar al personal médico en diagnósticos y seguimientos de casos, a la vez que coadyuvan a la canalización de pacientes, difunden información sobre la pandemia, entre otras.

Antes de que la Covid-19 se esparciera por la totalidad del globo, China y Corea del Sur destacaron por este tipo de desarrollos. En el primer caso, se puso a disposición de la ciudadanía una aplicación para la detección de contactos cercanos con riesgo de contagio de coronavirus. El funcionamiento es sencillo: mediante el uso de aplicaciones de mensajería instantánea y códigos QR, los ciudadanos tienen acceso a una plataforma en la cual registran su nombre y número de identificación personal. Estos datos pueden ser asociados con otros registros similares de contactos cercanos y se cruzan con información sobre sospechosos o confirmados del virus. De ese modo, la aplicación manda una notificación de alerta a aquellos ciudadanos quienes estuvieron cerca de algún contacto con posible riesgo

de contagio. En el caso coreano, la aplicación es auxiliar en el diagnóstico de síntomas relacionados con coronavirus, además de que permite al gobierno monitorear la geolocalización de pacientes sospechosos y positivos confirmados, de modo que es posible notificar al sistema de salud cuando estos abandonan la zona de cuarentena para que sean multados o sancionados acorde con la legislación local. Esta medida de control de movilidad por parte del gobierno coreano parece estar asociada al éxito en el control de la pandemia. En América Latina se han desarrollado 28 aplicaciones diferentes en 12 países, cuyas funciones van desde la recolección de datos de salud, servicios de telemedicina, información general hasta seguimiento y rastreo (Aguerre, 2020: 4). Destacan los casos aplicados en Uruguay –CoronavirusUY–,[2] Argentina –CuidAR–[3] y México –App Coronavirus CDMX–.[4] En términos generales, en un símil con las versiones china y coreana, estas aplicaciones son auxiliares en el diagnóstico, el monitoreo de pacientes y la canalización a atención médica cercana.

Ahora bien, ¿cuáles pueden ser los principales problemas con el uso de estas aplicaciones? En países con regímenes autoritarios y con reglamentaciones débiles o inexistentes en temas de privacidad y protección de datos personales en donde carecen de órganos garantes para su protección, la geolocalización, el rastreo y el uso de información personal pone en entredicho la privacidad de las personas y existe el temor de que haya una vigilancia a la ciudadanía por parte del Estado. Si bien esta práctica en países democráticos también existe, tanto los mecanismos jurídicos para denunciar, como las instituciones gubernamentales de protección tendrían que ser transparentes y rendir cuentas. De cualquier forma, aunque se cuente con organismos democráticos, el carácter emergente de la pandemia puede considerar su instrumentación sin que queden resueltas cuestiones asociadas con la ética, el resguardo de la privacidad y el derecho a la protección de datos personales. El principal problema es que estas aplicaciones requieren del tratamiento de datos personales sensibles. Para comprender más a fondo, tomaremos como referencia la legislación mexicana para definir qué es esta información. El artículo 3, fracción X, de la Ley General de Datos Personales en Posesión de Sujetos Obligados (LGDPPSO) señala que los datos personales sensibles son:

> Aquellos que se refieren a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud, presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencias sexuales.

Es decir, puedan llevar a cometer actos de discriminación o que conlleven un riesgo grave para el titular. Los datos personales[5] y los datos personales sensibles no se pueden divulgar y se consideran confidenciales. Sin embargo, el derecho a preservar esa información tiene excepciones y una de ellas es por razones de seguridad nacional, seguridad pública, disposiciones de orden y salud pública –o para proteger los derechos de terceros, conforme a la LGDPPSO–. ¿Cómo se resuelve esta paradoja?

La ley impone medidas de resguardo y confidencialidad más severas y distingue entre datos personales y datos personales sensibles con el objeto de evitar cualquier tipo de riesgo o acto de discriminación. Aun cuando la ley prevé el uso de datos personales sensibles para casos de emergencia sanitaria, es importante señalar que se deberán, en la medida de lo posible, anonimizar y su uso deberá apegarse a los principios de finalidad, transparencia y proporcionalidad. Es decir, se deberán usar únicamente para los fines para los cuales fueron recabados, a la vez que el uso de la información debe ser

2 Disponible en https://bit.ly/3CjIaQs

3 Disponible en https://bit.ly/34am2ew

4 Disponible en https://bit.ly/3ttgp3D

5 Datos personales: cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información. Artículo 3, fracción IX de la LGDPPSO.

transparente y sujeta a una temporalidad. Debido a que la salud pública está considerada una excepción al derecho a la protección de datos personales y a la no intromisión a la vida privada, las medidas de rastreo, geolocalización, acceso a expedientes (por mencionar algunos), deberán ser proporcionales entre el acceso a la información personal y a la vida privada y a su uso, con un análisis exhaustivo sobre cada medida que se pretenda tomar. Las acciones en la materia deben orientarse por los siguientes requisitos: que sean idóneas –que la medida sea la óptima–, necesarias –se deberá evaluar la medida que cause menos daño– y proporcionales –usar la medida menos costosa y que menos vulnere a los ciudadanos (Alexy, 2014: 52-54)—, con la finalidad de evitar arbitrariedades y el abuso de la información de las personas por parte del Estado.

II) Educación a distancia

Las medidas de aislamiento han puesto en el centro de la discusión un reto que los sistemas educativos tienen en la mira desde tiempo atrás: la existencia de herramientas eficaces para estudiar a distancia, ya que, en la inmensa mayoría de países del globo, la respuesta inmediata para continuar los programas de aprendizaje fue el traslado a las aulas virtuales. Así, las medidas pueden resumirse en: puesta a disposición de plataformas en línea para el aprendizaje, repartición de dispositivos para conectarse a Internet, capacitaciones a docentes para la enseñanza en línea, acceso a materiales didácticos y recursos auxiliares para el aprendizaje y capacitación en línea para profesionales técnicos y estudiantes de nivel superior.

Si bien las medidas tomadas para hacer frente a la educación a distancia son similares en distintos países, los resultados de estas acciones emergentes dependerán de la estructura de los sistemas educativos y de los logros previos a la digitalización. En esta materia, el ejemplo más destacado en América Latina es Uruguay. La nación rioplatense instauró en 2007 el Plan Ceibal que, basado en el programa One Laptop per Child, tiene como objetivo dotar de un *notebook* a todos los estudiantes del país de entre 4 y 15 años (Edelman, 2015). Asimismo, en 2013 implantaron un par de medidas destacadas: lanzaron la plataforma Crea, en la cual docentes y estudiantes cuentan con acceso a aulas virtuales y a recursos didácticos para el aprendizaje, e instrumentaron clases en línea para cubrir el déficit del

país en docentes de inglés (Plan Ceibal, s./f). Si bien las estrategias de educación en línea en Uruguay no estaban pensadas originalmente para responder a un escenario de emergencia, sin duda son una ventaja para la educación a distancia respecto de países que no atendieron la universalización de ordenadores, la conectividad en escuelas y la interacción de alumnos en espacios virtuales.

Para mala fortuna, el caso uruguayo es atípico en Latinoamérica, y cabe preguntarse cuáles pueden ser las consecuencias de estas medidas en países que no están suficientemente preparados para la educación a distancia. Un primer problema por resolver son las condiciones de estudio en el hogar, ya que, de manera específica, en una escuela con ideales condiciones dignas, los estudiantes pueden desarrollar sus actividades en entornos adaptados para tal efecto: mesas, sillas, espacios iluminados, servicios básicos de infraestructura y demás requisitos para el correcto aprendizaje. Otro factor por considerar en el aprovechamiento de la educación en línea es el perfil socioeconómico de los padres. Como se ha mostrado (Bourdieu y Passeron, 1979), una parte considerable del desempeño académico de los estudiantes está explicado por la dotación de capital cultural con la que cuentan los padres y los mecanismos para transmitirlo a sus hijos. En términos de uso de las TIC, esto se traduce en que, muy probablemente, los alumnos que obtengan mejor rendimiento de la educación en línea serán aquellos cuyos padres posean mayores habilidades digitales y mayor disponibilidad de tiempo para resolver los deberes con sus hijos. En el entendido de que la escuela debe funcionar como un espacio igualador para estudiantes, dadas las condiciones de la educación en línea, su práctica permanente puede tener como consecuencia el ensanchamiento de brechas de desigualdad económica y social.

En resumen, la educación en línea tiene sus problemas más grandes fuera de Internet, y son los mismos problemas estructurales del sistema educativo: falta de infraestructura y amplia desigualdad de condiciones para hacer frente al aprendizaje. Dado que al cierre de la edición de este documento no es claro cuándo será el retorno a las escuelas, los tomadores de decisiones tendrán que pensar en acciones integrales que no amplíen la desigualdad. Así, resulta urgente: ampliar la conectividad en zonas donde no existe –o mejorarla donde la calidad es mala–, distribuir dispositivos para el

acceso, pensar en políticas integrales para el involucramiento de personas cuidadoras en el aprendizaje, generar estrategias de integración entre alumnos fuera del tiempo de estudio y pensar en mecanismos de evaluación que no castiguen a aquellos estudiantes cuya familia no les puede puede transmitir las habilidades mínimas necesarias para el mejor aprovechamiento de las herramientas tecnológicas.

CONCLUSIONES

En un mundo en donde la tecnología avanza cada vez más rápido, el uso de Internet no sólo se ha convertido en un medio de participación política, de expresión de opiniones y de preferencias políticas, religiosas, sexuales, del estado de salud, entre otros, sino que también permite ejercer derechos fundamentales como el acceso a la justicia –juicios en línea–, a la salud –telemedicina–, a la educación –en línea, acceso a información– y al trabajo –teletrabajo–. Sin embargo, las estructuras socioeconómicas desde las cuales los individuos se relacionan con la tecnología condicionan el disfrute de sus beneficios. Es una regularidad del desarrollo histórico que las innovaciones tecnológicas suelen estar por encima de las institucionales. Por tanto, en la sociedad contemporánea, la adopción de las TIC en el día a día requiere de la revisión constante de sus posibles consecuencias negativas y de los probables debates normativos en cada uno de los aspectos que se aplican. De ese modo, dado que dichas innovaciones no se pueden parar, los responsables de las organismos públicas deben velar porque el ejercicio de la ciudadanía digital logre consolidarse como una posibilidad de ampliación en la participación política y en el acceso a servicios públicos, y no como una nueva dimensión de segregación entre ciudadanos de primera –conectados– y de segunda –no conectados– ni como un mecanismo para concentrar el poder y la vigilancia estatal.

En lo que respecta al acceso a Internet en México, a partir de la reforma en telecomunicaciones del 11 de junio de 2013, la Constitución establece en el artículo 6, párrafo tercero, que el Estado deberá garantizar el derecho de acceso a las tecnologías de la información y comunicación incluyendo los servicios de Internet. Sin embargo, la falta de despliegue en infraestructura, los altos costos de interconexión, la baja calidad en los servicios en la red y los altos costos en

las tarifas han sido un impedimento para paliar las desigualdades. Por su parte, en materia de protección de datos se deberá generar una cultura digital en la cual la ciudadanía no sólo aprenda a conocer el derecho que tiene a su privacidad y protección de sus datos y cómo protegerse, sino también a que este derecho sea exigible.

La pandemia que azota al mundo en nuestros días ha puesto de relieve los principales problemas de adopción de tecnología en la sociedad contemporánea. Ningún país estaba preparado para enfrentar la epidemia, pero aún así los esfuerzos por aprovechar las nuevas tecnologías en su combate se han instaurado en la escala global. Estas aplicaciones han contribuido a solventar problemas emergentes, pero no debe pasarse por alto que cada gobierno las implanta desde contextos muy distintos, arrastrados desde años –o incluso decenios– previos a la pandemia. El gran riesgo al que nos enfrentamos es que, en este momento, las medidas extraordinarias no parecen tener una fecha exacta para su fin, y sus consecuencias como preceptos regulares son potencialmente negativas. En el plano educativo, señalamos los problemas que existen para educar a distancia en un país donde una parte importante de las entidades de la región centro y sur no superan 44% de conectividad en hogares. En términos de participación ciudadana, es que, tal y como expusimos a lo largo del documento, la educación, entendida como praxis democrática diaria y como adquisición permanente de habilidades para el disfrute del uso de la tecnología, determina la construcción de la ciudadanía digital. El gran riesgo de dejar fuera a los niños y jóvenes del desarrollo de las habilidades digitales es que, así como se mostró en el apartado de la brecha digital, el uso de Internet para establecer interacción con el gobierno seguirá siendo facultad exclusiva de la minoría más educada.

En cuanto a la esfera de la protección de datos, resulta fundamental que el Estado ponga especial atención en que el tratamiento de la información sensible de los ciudadanos por parte de los distintos usuarios, tanto públicos, como privados, se apegue a lo mencionados principios de idoneidad, necesidad y proporcionalidad. Y, más aún, que estos procedimientos se lleven a cabo con estricta transparencia y a partir de diseños institucionales que promuevan el involucramiento de la ciudadanía en la materia.

BIBLIOGRAFÍA

Aguerre, C. (2020). La delgada y móvil frontera de las Corona-Apps en América Latina. *Análisis Carolina*. Recuperado de https://bit.ly/3HzUWLr

Alexy, R. (2014). Constitutional Rights and Proportionality. *Revus*, (22).

Bourdieu, P. y Passeron, J. (1979). *La reproducción. Elementos para una teoría del sistema de enseñanza*. Barcelona: Laia.

Bowen, J. (31 de octubre de 2019). ¿Estamos ante el comienzo de una nueva primavera árabe en Medio Oriente? *BBC*. Recuperado de https://bbc.in/3hSXLNz

Cáceres, M., Brandle, G. y San-Román, J. (2015). Hacia la construcción de una ciudadanía digital. Nuevos modelos de participación y empoderamiento a través de Internet. *Revista de Investigación Social*, (15), 643-684.

Castoriadis, C. (1995). La democracia como procedimiento y como régimen. En Amoroso, B. (ed.), *La stratega democrática nella società che cambia* (15-32). Roma: Datanews.

Cotta, M. (1996). Los gobiernos. En Bartolini *et al.* (ed.), *Manual de Ciencia Política* (311-317). España: Alianza Editorial.

Dahl, R. (1999). *La democracia y sus críticos*. Barcelona: Paidós.

Edelman, A. (2015). *Plan Ceibal: "One Laptop per child" en Uruguay*. Montevideo, Uruguay: Universidad de Montevideo, Escuela de Negocios.

Eubanks, V. (2014). Big Data and Human Rights. En Peña, S., Eubanks, V. y Barocas, S. (ed.), *Data and Discrimination: Collected Essays* (48-52). Open Technology Institute. Recuperado de https://bit.ly/3pyHp0s

Fernández, M. y Burch, A. (9 de junio de 2020). La historia de George Floyd: el camino desde "Quiero emocionar al mundo" hasta "No puedo respirar". *The New York Times*. Recuperado de https://nyti.ms/35xrs3Q

Gleason, B. y von Gillern, S. (2018). Digital Citizenship with Social Media: Participatory Practices of Teaching and Learning in Secondary Education. *Educational Technology & Society*, 21(1), 200-212.

González, M. (5 de junio de 2020). Racismo en México: cómo la muerte de George Floyd desató en el país un debate "del que nadie quiere hablar". *BBC*. Recuperado de https://bbc.in/35Jv4j5

Gurza, A. e Insunza, E. (2010). Precisiones conceptuales para el debate contemporáneo sobre la innovación democrática. En Gurza, A. e Insunza, E. (coords.), *La innovación democrática en América Latina* (19-82). México: Publicaciones de la Casa Chata.

Instituto Nacional de Estadística y Geografía (Inegi). (2018). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías en los Hogares (ENDUTIH)*.

Jorring, L., Valentim, A. y Porten-Cheé, P. (2019). Mapping a Changing Field. A Literature Review on digital Citizenship. *Digital Culture and Society*, 4(2), 11-37.

Latonero, M., Hiatt, K., Napolitano, A., Clericetti, G. y Penagos, M. (2019). *Digital Identity in the Migration & Refugee Context: Italy Case Study*. Data & Society. Recuperado de: https://bit.ly/3vDs0Fa/

Moreno Muñoz, M. (2017). Privacidad, procesado automático de datos personales mediante aplicaciones y bots. *Dilemata*, (24), 1-23.

Mossberger, K., Tolbert, C.J. y McNeal, R.S. (2008). *Digital Citizenship: The Internet society, and participation*. Cambridge, Massachusetts: MIT.

Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2016). *Gobierno Abierto. Contexto mundial y el camino a seguir*. OCDE.

O'Donnell, G. (2001). Accountability horizontal. *Isonomía*, (14), 7-31.

O'Donnell, G. (2015). *La democracia en América Latina*. Nueva York: PNUD.

Panebianco, A. (1996). Las burocracias públicas. En Pasquino, G., Bartolini, S., Cotta, M., Morlino, L. y Panebianco, A. (eds.), *Manual de Ciencia Política*, (368-374; 386-398). España: Alianza Editorial.

Peruzzotti, E. y Smulovitz, C. (2002). Accountability social: la otra cara del control. En Peruzzotti, E. y Smulovitz, C. (coords.), *Controlando la política: Ciudadanos y medios en las nuevas democracias latinoamericanas* (23-52). Buenos Aires: Temas.

Plan Ceibal (S.F). *Ceibal en inglés*. Recuperado de https://bit.ly/35Nwwkl

Przeworski, A., Manin, B., Stokes, S. (2002). *Democracy, Accountability and Representation*. Cambridge: Cambridge University Press.

Ribble, M. (2012). Digital Citizenship for Educational Change. *Kappa Delta Pi Record*, 4(48), 148-151.

Rodríguez, G. (2004). Gobierno electrónico: Hacia la modernización y transparencia de la gestión pública. *Revista de derecho*, (21), 1-23.

s/a (5 de abril de 2016). El primer ministro de Islandia renuncia, tras el escándalo de #PanamaPapers, *Expansión*. Recuperado de https://bit.ly/3C9oZZw

Sandoval-Almazán, R. y Mendoza, J. (2011). Gobierno electrónico en México: una exploración municipal 2010. *AMCIS 2011 Proceedings-All Submissions*.

Schumpeter, J. (1983). *Capitalismo socialismo y democracia*. Barcelona: Orbis.

Sierra, F. y Gravante, T. (2016). Ciudadanía digital y acción colectiva en América Latina. Crítica de la mediación y apropiación social por los nuevos movimientos sociales. *La trama de la comunicación*, *20*(1), 163-175.

Sojo, C. (2002). La noción de ciudadanía en el debate latinoamericano. *Revista de la Cepal*, (76), 25-38.

Valenti, P., López-Ghio, R., Riorda, M., Starface, F. (2015).*El gobernauta latinoamericano. Estudio del perfil de los gobernantes latinoamericanos en redes sociales.* Banco Interamericano de Desarrollo. Recuperado de https://bit.ly/3Ca6qEt

CAPÍTULO 04

CIUDADANÍA DIGITAL, DATOS PERSONALES E INTELIGENCIA ARTIFICIAL: RETOS SOCIOÉTICOS PARA EL T-MEC

ISMENE ITHAÍ BRAS RUÍZ*

* Dirección de Posgrado e Investigación del Instituto de Estudios Superiores de la Ciudad de México "Rosario Castellanos" (IRC) y Facultad de Ciencias Políticas y Sociales, UNAM.

INTRODUCCIÓN

La ciudadanía digital tiene su semilla dentro de la sociedad de la información y el conocimiento, pero como todo proceso humano, ha tenido su evolución hacia la sociedad red e incluso ha ido insertándose en la economía del conocimiento. Por otro lado, la correlación rizomática de la ciudadanía digital ha permitido que la conexión entre los ciudadanos, el gobierno y otros poderes y/o grupos sea más personal y flexible. Gracias a estas dinámicas no se puede pensar en la ciudadanía digital si no se incorporan otras características de análisis como son la cultura, la alfabetización, la literacidad digital, entre otros.

Los gobiernos han aprovechado el uso de plataformas digitales tanto en el nivel comercial, como al generar aplicaciones propias o páginas informativas en la que exponen datos, avisos o información relevante; aunque algo que se ha destacado es la prestación de servicios que los ciudadanos deben realizar de manera física, llevándolos al espacio digital para mayor eficacia. Sin embargo, sólo en pocos países se han abierto los canales de comunicación (diálogo) entre las autoridades y la ciudadanía digital. En ese sentido, las administraciones públicas han encontrado en el mundo digital una forma de comunicación, aunque el flujo muchas veces es percibido de manera lineal y no rizomático. Por el contrario, la ciudadanía ha encontrado en el uso de las tecnologías de las información y la comunicación (TIC) el medio de revertir el diálogo transversal a través de las redes digitales y otros espacios que se acomodan no sólo a las distintas generaciones, sino a los grupos y comunidades.

Por ello la cultura digital ha sido un factor sustancial para entender el desarrollo mismo de la ciudadanía en esa materia. Muchas veces esta se ha confundido con la alfabetización digital, el mayor o menor grado de manejo de las TIC. No obstante, buena parte de las plataformas y aplicaciones digitales se han centrado en su diseño ambiental (affordance), para que sean lo que llamamos intuitivas, de ahí que gracias a esa ventaja, personas que carecen de elementos de alfabetización tradicional (niños pequeños, o comunidades con bajos niveles de lectoescritura) puedan hacer uso de la literacidad digital (comprensión del mundo a través de medios digitales) y conectarse no sólo con otras comunidades, sino exponer casos de injusticia, hacer visible una situación límite, falta de recursos para el desarrollo, entre otros. Recordemos que nos encontramos en una retórica del hipervínculo, en la que incluso los medios audiovisuales han comenzado a ganar terreno por sobre la lectura tradicional. Nuestra relación con las TIC ha trastocado la vida de prácticamente todas las personas en el planeta; en este tenor de ideas, se han desarrollado distintas culturas digitales transaccionales y transnacionales que apelan a diversas identidades, muchas de las cuales no son contenidas dentro de los límites geográficos de los estados Estados, sino que son fronteras líquidas. El ciberespacio, al tener una estructura rizomática, en red y en constante cambio, ha sido aprovechada por diversas comunidades alrededor del mundo; por tanto, se compone de distintas culturales digitales, formas de leer la realidad, retóricas particulares, diversas lectoescrituras en la red, que se encuentran y desencuentran pero que usan el espacio digital como su plataforma para hacer ver, oír y dialogar, por lo cual habría que hablar de ciudadanías digitales.

> Por ello, desde el contexto de la cibercultura, esto significa no sólo hablar de una nueva apuesta de la organización de la cultura general, sino de la relación de la informática con la vida social y la configuración desde una perspectiva que incluya a las Nuevas Tecnologías (Lévy, 2007), a las viejas y a todo el espacio social dentro de una nueva cosmovisión que organice todos los vínculos posibles entre los diversos componentes sociales, donde la ciudadanía se vuelve una ciudadanía digital, la cual tiene que ver con el desarrollo de nuevas necesidades y otras formas culturales de concebir y organizar el acceso a los servicios (Estupiñan *et al.*, 2016: 4).

Se trata de comprender que las ciudadanías digitales se logran hacer eco pese a la distintas condiciones socioeconómicas y socioculturales, incluso la brecha digital es uno de los factores que definen las identidades de estas comunidades que se han asumido como ciudadanas, aún cuando no lo hagan como digitales, porque la expresión y visibilización de sus ideas, valores, creencias se logran vincular en red.

Las diferentes culturas digitales se han fortalecido en la medida en que la presencia de la ciudadanía digital ha hecho uso de plataformas y redes como espacios públicos apropiados frente a diversos fenómenos que ahora son visibilizados y reclamados

a poderes fácticos u otras sociedades. De hecho, dicha ciudadanía se ha apropiado de las plataformas digitales comerciales para hacer sonar su voz, por lo que se espera una respuesta que permita diseñar nuevas políticas públicas y modificar las condiciones de existencia de esas comunidades. De ahí que la ciudadanía digital simbólicamente haga de estas plataformas el espacio público nuevo en el que tienen presencia distintos agentes. La agencia social en este sentido es inductiva, altamente dinámica y coconstructora de identidades, no sólo a partir de sus agremiados, sino de los intereses, valores y creencias que persiguen, lo cual permite mantener la conexión como una forma de generar cambios sociales, políticos, económicos, culturales, muchas veces en tiempo real, o como un testimonio de un pasado que todavía guarda memoria.

La relación de la ciudadanía digital con las plataformas comerciales genera nuevas articulaciones y correlaciones para las expresiones políticas de la ciudadanía organizada desde un nivel básico hasta uno complejo; al final se busca reorganizar a la sociedad desde sus instituciones y organizaciones mediante nuevos espacios públicos. Si bien es cierto que hay formas de interacción digital-física, la economización de las expresiones y peticiones de la ciudadanía cobran relevancia frente a los modelos burocráticos o de balances de poder no equitativos.

> Su fluidez, ubicuidad, rapidez y falta de intermediación las hacen detonadoras del discurso entre ciudadanos. [...] la comunicación es cada vez más sensorial, más dinámica y multidimensional, las tecnologías atraen, son más sencillas, económicas, portátiles incrementan paradójicamente las exigencias de una ciudadanía más compleja y efímera (Estupiñan *et al.*, 2016: 5).

La cultura digital es un reflejo claro de cómo la ciudadanía se inmiscuye cada vez más con temas políticos, económicos, sociales, religiosos, étnicos, educativos, que reflejen fielmente la necesidad de contar con gobiernos y estados que trabajen en la misma línea de las necesidades de la ciudadanía en sus sociedades; trabajo conjunto para resolver demandas o alzar peticiones. De ahí que Petrizzo, señale: "[...] el término ciudadanía se enmarca en el discurso sobre la justicia social y el vínculo del individuo con una comunidad política" (2005: 98).

Si bien no todas las demandas son o pueden ser atendidas en tiempo real, la visualización y viralización de las mismas ha hecho que los tiempos de respuesta por parte de los gobiernos, por lo menos discursiva, sea menor en relación con otros periodos; incluso el arribo de los *e-government* es una forma de ganar tiempo para actuar y resolver distintas dinámicas y peticiones ciudadanas en un lapso menor o, al menos que se deje constancia de que han sido impulsadas. No obstante, los trámites electrónicos o la puesta en marcha de las distintas plataformas ha acercado del todo a la ciudadanía a las funciones del Estado, aunque en varios países dicho acercamiento constituye un avance sustancial. De ahí que la ciudadanía digital recurra a los canales comerciales para su organización y difusión o una segunda difusión de la información de los canales oficiales.[1]

Sin duda, lo anterior lleva a reflexionar sobre el papel que cumplen las grandes empresas de tecnología, en especial las que se desarrollan a partir del uso de inteligencia artificial (IA), dado que todas tienen distintos objetivos y finalidades, pero en cualquier caso dependen en buena medida de la recolección, tratamiento y uso de datos, muchos de los cuales son de carácter individual, personal y privado. Tal información no es empleada con una sola finalidad, sino que recorre varios caminos, y hasta el día de hoy no hay plena certeza, por ejemplo, de su destrucción.

[1] Por ejemplo como el pago de impuestos, o diversos trámites civiles que se puede llevar por medios electrónicos, los perfiles de las y los candidatos a elecciones populares, la presentación de proyectos a concurso público, resultados de convocatorias, juicios y su seguimiento, datos abiertos de los gobiernos, son algunos ejemplos –entre muchos de los manejos que tiene–: se encuentran en la red para colaborar y transparentar la información a los ciudadanos. Si bien es cierto que el camino aún es largo para que los gobiernos sean plenamente transparentes, también hay que considerar que cada uno de estos responde dentro de cierta lógica de la retórica digital de la ciudadanía a la cultura digital del entorno. Gobiernos más cerrados, en los que es menos posible la aparición abierta, legal y legítima de la sociedad civil organizada, acompañados de menos niveles de conectividad o coartada, generará menos canales de comunicación y de información abierta; por el contrario, en las sociedades cuya retórica digital prioriza sus derechos civiles, la brecha digital –si no es menor– tiene centros en los que la concentración de conectividad se une con una actividad económica mayor y existe una mayor interculturalidad, tendrán que responder a esas diversas culturas digitales que exigen canales de comunicación, interlocución y respuesta (incluso en un menor tiempo).

La mayor parte de los datos de los ciudadanos alrededor del mundo están "protegidos" por diversas normativas nacionales o en apego a instrumentos internacionales. No obstante, la "regulación" de la IA en esta materia no lo está: por mencionar algunos casos, la opacidad de su manejo, el diseño y operación de algoritmos, la finalidad del uso de tales datos, la identificación de patrones, generación de perfiles de consumidores, la decisión autónoma de las máquinas, o los objetivos de grandes corporaciones. Es decir, una parte de nuestra información y de nuestra huella digital están protegidas respecto de la esfera privado-público, pero no de su tratamiento.

Una discusión seria del tema nos lleva sin duda a analizar el marco ético que se debe dar tras el trabajo de la IA y su operación; sin embargo, son tantos los agentes relacionados, que es necesario plantear el tema desde distintos ángulos. Por ejemplo, permitir que la ciudadanía digital no sólo pueda seguir su trabajo como una nueva dinámica en lo político, sino que las personas sepan específicamente y decidan qué se hace con sus datos; ya no es suficiente el derecho al olvido, sino a exigir la destrucción de esa información una vez que ha sido empleada para su objetivo y que las empresas o gobiernos sean claros al respecto.

En ese sentido, alrededor del mundo apenas tenemos el primer esbozo que complementa el tratamiento de datos con la regulación de la IA, en el caso de la Unión Europea, que tiene una visión centrada en las personas; por el otro lado, Estados Unidos y Reino Unido han tratado el tema de una manera por completo diferente, basándose principalmente en el tema de la seguridad nacional, por lo que la regulación de la IA no sólo está separada del sentido humano y su protección inmediata, sino que el marco jurídico que regula a esta industria se encuentra repartido entre varios instrumentos, esencialmente enfocados a la inversión, desarrollo y aplicación de la IA en distintas áreas. A la vez, contamos con marcos de referencia como el de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), que se encuentran y van de la mano de los países anglosajones, mientras que se han comenzado a dar discusiones en otros espacios, principalmente de profesionistas, académicos y desarrolladores en los cuales se insiste en que lo ideal es contar con principios éticos del uso de la IA centrados en las personas y que esto lleve a una mayor transparencia del diseño y operación de esta industria.

Nuestra región, básicamente por el caso de Estados Unidos, es la que mayor inversión y negocios en IA tienen en todo el mundo. Y aunque los tres países han regulado el tema de protección de datos, estos no se han logrado relacionar con la praxis de la industria que emplea la IA en la zona. Tal como señalamos, la protección a la información existe, pero al encontrarse con la IA, estos datos están incluso protegidos de nosotros mismos; como ciudadanos no tenemos derechos sobre ellos para su comercialización, recolección, uso, ni siquiera estamos enterados de cómo se emplean o con qué fines. Si bien la IA ha sido benéfica en muchas áreas como en salud, comercio electrónico, o aspectos metereológicos, existen claroscuros que no se han visto reflejados en el Tratado entre México, Estados Unidos y Canadá (T-MEC) y que exigen, al igual que se hizo en la Unión Europea y en otros ámbitos, una discusión ética y normativa.

El texto que se presenta parte justamente de la importancia que tienen para nuestras sociedades la ciudadanía digital y la relación con las corporaciones que emplean la IA, y los desafíos éticos y técnicos que tiene frente la ciudadanía en este campo.

REFLEXIONAR SOBRE LA CIUDADANÍA DIGITAL

En tiempos recientes se ha correlacionado a la sociedad civil organizada, la ciudadanía digital y los movimientos sociales como una nueva tendencia de los tiempos en los que vivimos, que parte de distintos campos y que se interconectan en nodos digitales. En buena medida estos fenómenos de movilización física (organizada en la red) y digital son el resultado del déficit participativo, político, económico y democrático que se percibe en las distintas sociedades en el orbe entero.

> Pese a que existen diversos contrapesos para contrarrestar estos desequilibrios, como la rendición de cuentas, la contraloría social, la transparencia de información, los informes (globales y locales de las actividades de los servidores públicos y privados)

y los observatorios ciudadanos, entre otras figuras y procesos compensatorios, estos no han sido suficientes para resolver el creciente problema de la desconfianza en las instituciones públicas" (Natal *et al.*, 2014: 22).

Es así como surgen comunidades transnacionales ciudadanas digitales que se identifican frente a los actos o discursos del poder político y económico que contraviene el sentido de bienestar de la ciudadanía: "Para ello se sobreentiende que la participación ciudadana depende de la toma de una serie de acciones e iniciativas que impulsen el bienestar social, fomentan la ciudadanía y convoquen a la democracia" (Estupiñan *et al.*, 2016: 3); con ello se ha elevado el debate de la *res publica* a distintas plataformas que buscan evidenciar tales déficits o bien elevar propuestas más cercanas a quienes la necesitan según las identidades y generaciones de las que son parte.

Lo que habría comenzado en la década de los noventa en Seattle frente a la Organización Mundial del Comercio (OMC) como manifestaciones antisistémicas, organizadas a través de la web 0.1, se han vuelto incursiones desde la esfera de lo privado a lo público digital, generando cada vez movimientos autónomos, autogestivos, horizontales, cooperativos, espontáneos, para exigir la apertura y democratización de los espacios y contra la alta concentración del poder y la riqueza. En ese sentido, la ciudadanía digital y sus distintas manifestaciones en buena medida se relacionan con el disgusto de los ciudadanos frente a las fuerzas de la globalización materializadas a través de los mercados internacionales y la mutación de la naturaleza del Estado benefactor. Por lo tanto, la ciudadanía civil en sus diferentes dimensiones y vocaciones se relaciona con la necesidad prácticamente generalizada de encontrar espacios de diálogo para alcanzar la justicia, equidad, desarrollo, fraternidad y fortalecer las diversas identidades de las comunidades. "Esto quiere decir que la sociedad del riesgo mundial surge, en virtud de la percepción pública de los riesgos, una sociedad autocrítica bien preparada, al menos en la manera como habla de acciones o ideas alternativas [...]" (Beck, 2019: 142).

Las plataformas digitales y redes sociales han jugado un papel primordial en la nueva construcción de los espacios civiles, al evidenciar desde el déficit democrático, de gobierno, falta equidad e

inclusión, niveles de subdesarrollo, corrupción, racismo, clasismo, cultural, voracidad económica, lucha medioambiental y de género, entre otros, la inacción o la acción poco solidaria:

> Ya no hay grandes decisiones de las que puedan derivar pequeñas decisiones, ni fronteras de las que emanan reglamentaciones específicas. Así como las comunidades ya no están contenidas en la región, ni la región en el estado nacional, la pequeña decisión ya no deriva de la grande. La crisis del concepto del poder determinado espacialmente encuentra de este modo su expresión en la búsqueda de decisiones. Las decisiones ya no se toman de modo lineal, en el sentido de que cada corporación posee una competencia bien perfilada; más bien, se descomponen en distintos fragmentos, y el tradicional de debate político, las disputas sobre principios y directrices, ideologías o el ordenamiento social, se destiñe, o, mejor dicho se descompone (Beck, 2019: 153).

Frente a lo unidireccional de la acción del estado y su pensamiento dualista y lineal, el uso de Internet se ha vuelto una especie de rizoma que descentraliza los poderes político (incluso el económico) y sociocultural, para dotarlos de nuevas características sociales complejas:

> Una de esas posibilidades que ha abonado a la conformación de la ciudadanía digital contemporánea es precisamente la tecnopolítica, que va desde la conexión de acciones colectivas donde convergen identidades transgresivas de vanguardia, el desarrollo de formas de innovación en el diseño de la política pública surgida de públicos participativos en ambientes digitales, hasta la coordinación *glocal* para preservación y defensa de procomunes y espacios públicos, exigencias de transparencia y rendición de cuentas, organización de manifestaciones y foros alternos, entre muchas posibilidades (Leetoy *et al.*, 2019: 4).

Los movimientos sociales que reflejan la ciudadanía digital buscan principalmente elevar la acción por sobre los discursos oficiales, las injusticias raciales o de género, o el uso maniqueo del mercantilismo de las corporaciones internacionales, incluyendo la de las propias plataformas y redes sociales digitales. El intercambio dia-

lógico no se limita a la exposición de ideas o de información, por el contrario: "permiten colaboraciones remotas y asíncronas en la construcción de una esfera pública más diversa, y si bien los movimientos sociales son efímeros, las luchas constantemente mutan con otros actores, pero con las mismas circunstancias que les han dado origen" (Leetoy *et al.*, 2019: 5), de ahí que la ciudadanía digital tenga un carácter transnacional y transestatal. Para lograrlo, las comunidades digitales fortalecen e impulsan su base de conocimiento, sus estrategias de comunicación (retórica digital), así como los objetos de protesta (viralización de contenidos), al resto de la nación o de la cosmópolis digital. Se trata de la construcción del espacio público desde el ciberespacio constituido por distintas narrativas, ciberculturas, generaciones, pluralidad que presiona desde ese ámbito no material hacia el material, mediante la acción colectiva física o digital; justamente lo transnacional-transestatal ha perdido un lugar primordial, porque el espacio de lo público ha sido reconstruido desde la colectividad cívico-digital.

Si bien la discusión se puede pensar desde lo cívico-democrático, la realidad es que la mayor parte de los debates se llevan a cabo en espacios digitales de grandes capitales enfocados en la tecnología; razón por la cual el espacio público-digital se compone de ciudadanos e integra a estas grandes corporaciones y sus diferentes repercusiones para la acción sociopolítica que no necesariamente se enfocan en el bienestar, sino que, bajo manipulación del consumo digital, tendencias sociales (civiles o de industrias culturales) se orientan en pro de las ganancias (McChesney, 2013). Por ello se plantea la necesidad de que sea la propia población la que desarrolle estrategias para que, fenómenos como las intenciones de censura o el periodismo independiente, mantengan una posición frente al poder del Estado y de estas corporaciones tecnodigitales:

> Las coyunturas críticas en los medios y las comunicaciones tienden a ocurrir cuando se cumplen dos o tres de las siguientes condiciones:
> – Hay una nueva tecnología de comunicación revolucionaria que socava el sistema existente;
> – El contenido del sistema de medios, especialmente el periodismo, está cada vez más desacreditado o visto como ilegítimo; y/o
> – Hay una gran crisis política –severo desequilibrio social– en la que el orden existente ya no funciona, las instituciones dominantes son cada vez más desafiadas y hay grandes movimientos de reforma social (McChesney, 2013: 67).

En 2017, Zuckerman estableció una teoría a partir de su observación del manejo de las plataformas digitales por parte de los movimientos sociales y la ciudadanía digital, la teoría de los gatos lindos (*Cute cats Theory)* en la que señalaba:

> Las herramientas digitales para que los consumidores normales publicaran contenidos no políticos, eran a menudo muy útiles para el activismo político, precisamente porque es difícil censurarlas por los gobiernos, sin con ello censurar también contenidos inocuos, porque la censura de contenidos inocuos puede alertar a los usuarios no activistas de las maniobras de censura, y porque el activismo que usa las herramientas de los consumidores puede activar la 'capacidad latente' de los usuarios no activistas para crear y diseminar contenidos de activismo. [...] vemos que la resistencia a la censura puede ser un beneficio menos significativo que la capacidad para suscitar la participación, para la recreación y para el humor, que distribuyen los contenidos activistas a muy amplias audiencias. Al mismo tiempo, un examen detallado de las circunstancias que permiten a los activistas extenderse usando herramientas de usuario de este estilo revela un conjunto de amenazas para este tipo de discurso digital. En particular, la confianza en las plataformas comerciales para el discurso público puede someter a los activistas a la "censura del intermediario", o a censuras privadas a la libertad de expresión, por parte de los propietarios de las plataformas digitales (Zuckerman, 2017: 28-29).

Lo que se puede desprender de la teoría de Zuckerman (2017) es que la ciudadanía digital ha tratado de trabajar en plataformas comerciales no sólo porque la mayor parte de las personas cuentan en sus dispositivos o acceden a tales espacios de manera regular, sino porque el poder político, para socavar los intentos de visibilización y el intento de crear espacios de diálogo, por fuerza tendría que censurar espacios (plataformas comerciales) que contienen diversos

contenidos que no necesariamente tienen que ver con las peticiones y/o demandas de la ciudadanía. Esto es percibido por la población como censura y como un ataque personal a su espacio digital subjetivo. De ahí que existan gobiernos que han intentado cerrar las opciones de información, intercambio de ideas o protesta de grandes corporaciones mediáticas. Por eso la importancia de que las plataformas web 2.0 sean transaccionales y el acceso a Internet un derecho humano, que permite el ejercicio de las libertades y la participación política.

> Un ciudadano digital que hace uso constante y recurrente de lo dispuesto por Internet tiene derecho a usar las nuevas tecnologías de información y comunicación en la medida que desarrolle habilidades digitales, desplazamientos y acceso al información en línea de forma segura, transparente y privada, así como participar en diferentes medios tecnológicos que hoy en su mayoría son públicos y cada vez más baratos [...] esta ciudadanía digital surge de las nuevas formas de socializar a través de los nuevos contactos (Estupiñan *et al.*, 2016: 5).

De este modo, la ciudadanía digital puede entenderse también como una estrategia y una nueva forma de de organización en cuanto a lo que Rosanvallon (citado por Natal *et al.*, 2014) denomina contrademocracia, no en contraposición a la democracia, "[...] sino más bien como formas alternativas de representación y de legitimación que pueden incluso superar a la democracia institucional al construir un sistema de poderes indirectos en la sociedad para vigilar, controlar y enjuiciar la actuación de los gobernantes" (Natal *et al.*, 2014: 29). Hay que considerar que en algunos países el activismo político-digital constituye una especie de desobediencia civil, pero en una forma ahora virulenta que cobra mayor rapidez frente a las concepciones de La Boétie, Thoreau, Gandhi o Martin Luther King, Malcom X, entre otros. Las tecnologías de la información y el conocimiento tienen un impacto no sólo en la información *per se*, sino en el debate de lo público desde el nivel local, pasando por el regional, el nacional, hasta el global, en la que los costos sociopolíticos se reducen notablemente aunque aumenten los de la clase política, pero genera una ciudadanía cada vez más activa, dinámica y empoderada.

CULTURA DIGITAL Y LITERACIDAD DIGITAL COMO FUNDAMENTOS DE LA CIUDADANÍA DIGITAL

Inminentemente la ciudadanía digital se relaciona con la cultura digital. No obstante, de manera casi generalizada, se piensa en este concepto a partir de una serie de nociones o de cualificaciones que tienden a invisibilizar, nulificar y excluir a buena parte de la población en el nivel global. En ese sentido, se suele confundir la cultura digital con una serie de habilidades y competencias que en realidad se refieren a la llamada alfabetización en la materia, negando la posibilidad de aprehender distintos fenómenos y ecosistemas digitales que conviven sin que haya una escala de capacidades homologada. Dicho de otro modo, la cultura digital se relaciona de manera amplia con las prácticas, identidades, ecosistemas digitales, valores, lectura e interpretación de la realidad, más que con una serie de competencias verificables tan sólo en una parte de la población. En ese sentido, cabe retomar una primera aproximación a este concepto al entender que:

> La cultura digital abarca más allá de los sistemas, prácticas, entornos y medios culturales simbólicos (como los directamente relacionados con la información, la comunicación, el conocimiento o la educación) y se extiende prácticamente por todos los ámbitos de la sociedad digital, los rápidos procesos de innovación desencadenados por las TIC digitales han transformado radicalmente, junto con los sistemas, los colectivos y las dinámicas de la información y la comunicación, también las formas de conocimiento e investigación tecno-científica (Lèvy, 2007: 129).

Habría que entender entonces: "lo digital" nos cruza como humanidad a todos en distintas formas y ámbitos. Nuestra relación con la tecnología no sólo es variada, sino que responde a diversos contextos socioculturales, socioeconómicos e incluso sociopolíticos y geográficos; pero todo ser humano tiene una cultura digital, que en principio no vale más que la de otra persona; sino que se debe reflexionar sobre la base de la diversidad, la creación de comunidades (incluyendo justamente la ciudadanía digital), los intereses, la brecha digital, las divisiones sociales, la edad, el género, entre otros. De ahí que la

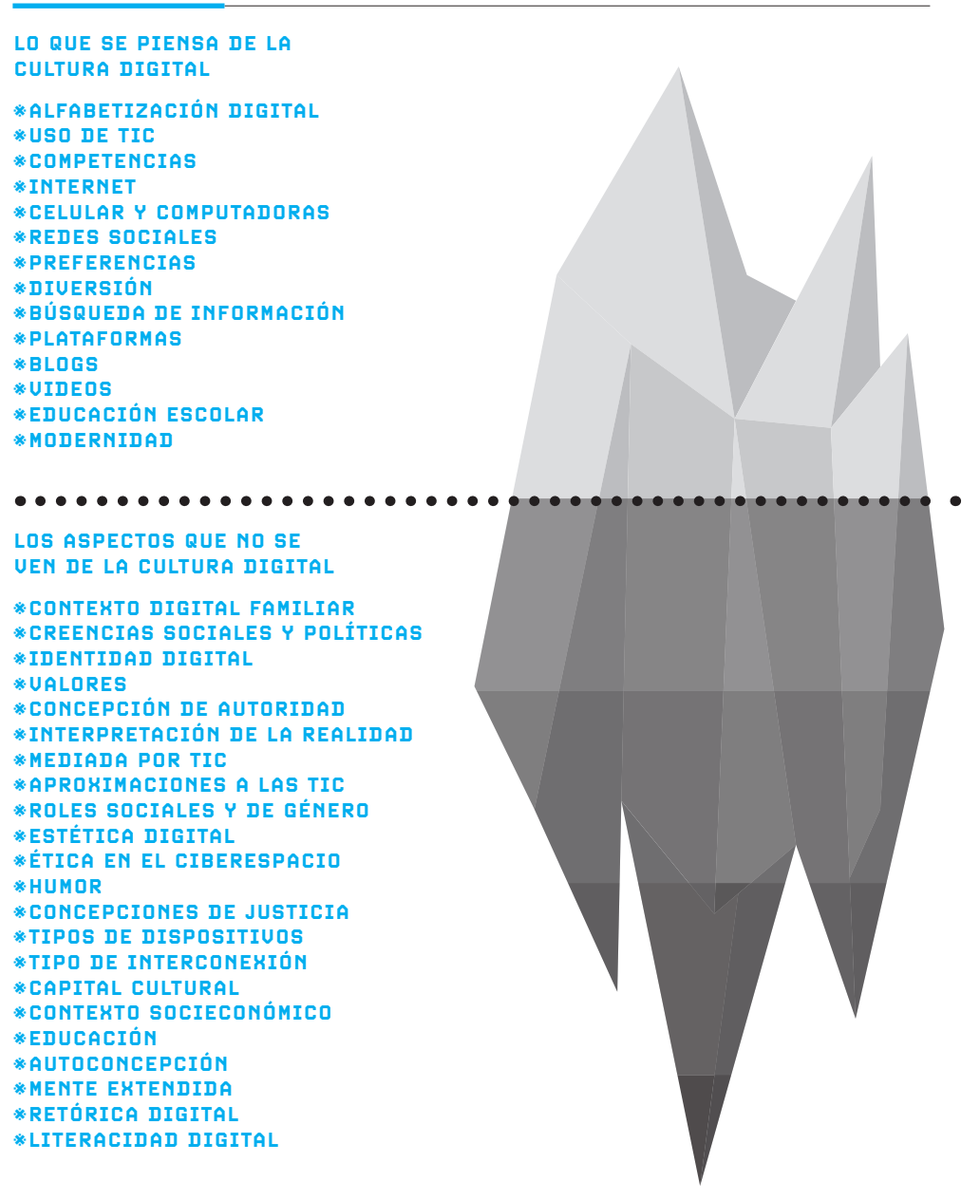
cultura digital en realidad sea un fenómeno bastante complejo que no se limita al ciberespacio, sino que tiene una narrativa que es extensión de nuestro mundo real. Lo que construimos en el ciberespacio como comunidades e identidades no es distinto de lo que sucede en la realidad. Por el contrario, forman una unidad. La ciudadanía digital es uno de estos nuevos espacios, ecosistemas, ambientes, que permite construir y reconstruir a las personas a partir de la necesidad de expresión y organización frente a la biopolítica, las injusticias, la necesidad de pertenecer a comunidades o bien, encontrar formas alternas al bienestar humano.

Entender las identidades que la ciudadanía diseña, crea, desarrolla, organiza, a través de la tecnología digital, implica entender que la cultura digital es como un iceberg (véase figura 01) en la que la sección superior es tan sólo una mínima parte del trasfondo de lo que implica en toda su complejidad, de ahí que no podamos reducirla sólo a la alfabetización digital.

De hecho, en la cultura digital hay divisiones sociales (Shweta Barupal, 2017) muy claras, las cuales han generado que las brechas digitales sean cada vez más manifiestas. Aspectos como la edad, género, geolocalización, idioma, educación, grupo étnico, entre otros, ciertamente generan habilidades distintas en relación con diversos tipos de acceso y el ejercicio de tales, y en ese sentido se puede establecer que hay poblaciones que se ven más o menos beneficiadas por las nuevas tecnologías (Shweta Barupal, 2017) y que, por lo tanto, haya grupos que ante diversas restricciones tengan una cultura digital diferente.

Lo que solemos llamar cultura digital ha coexistido con buena parte de las sociedades occidentales desde por lo menos la década de los 80 del siglo pasado; no obstante, la ampliación de su uso, principalmente de Internet, ha hecho una notable diferencia entre zonas económicas y edades (y, por supuesto, género) alrededor del mundo, e incluso al interior de los propios países. Esas habilidades que se van desarrollando al entrar en contacto con diferentes tecnologías digitales permiten a las personas tener una comprensión y lectura del mundo de acuerdo con sus condiciones, conexiones y contextos, esto es a lo que llamaremos literacidad digital. Esta se compone por una lectura subjetiva rizomática, es decir, interactiva, hipertextual e interconectada de la realidad que nos rodea. Todos los seres humanos leemos el mundo de diversos modos, pero al comenzar a interactuar

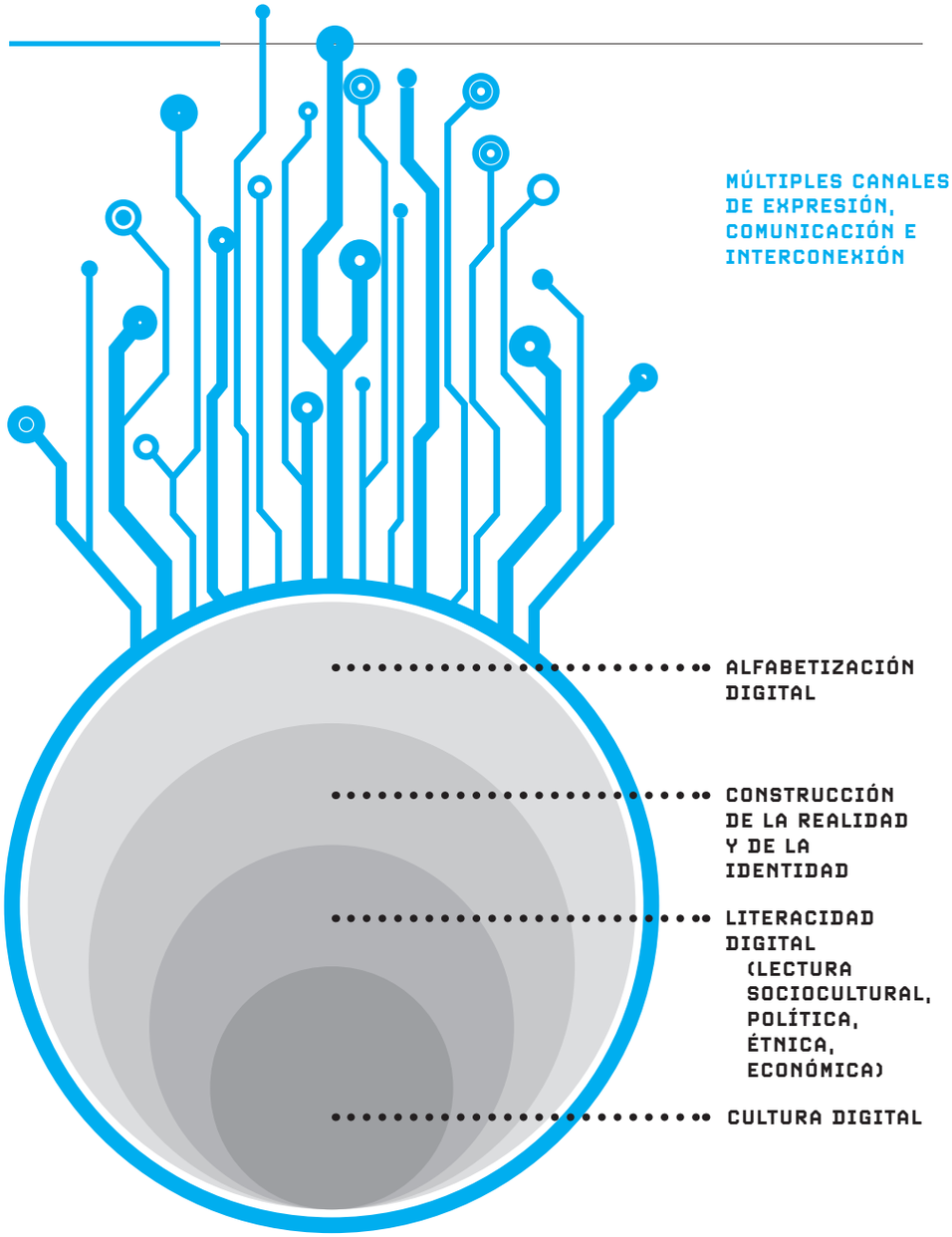
FIGURA 01. ICEBERG DE LA CULTURA DIGITAL



FUENTE: elaboración propia.

SISTEMAS-SUBSISTEMAS DE LA CULTURA DIGITAL Y VISIÓN RIZOMÁTICA DE INTERCONEXIONES

FIGURA 02.



FUENTE: elaboración propia.

con los dispositivos digitales, sea que hayamos evolucionado en su uso, por ejemplo, de la videocasetera al *streaming*, o de las enciclopedias a los buscadores y Wikipedia (o incluso la *Deep Web*), saltamos de una información a otra, la conectamos y tenemos interacción con el resto de las personas de diversa forma. Lo que no se puede negar es esta lectura y comprensión en un único canal, sino en múltiples (véase figura 02). Ahora bien, justamente esa división social a la que ya se hacía alusión y que crea distintos tipos de brechas, se relaciona con la alfabetización digital en tanto que desarrollamos las competencias no sólo para el manejo de la información, sino para su búsqueda, creación, transmisión, entre otros, con un sentido crítico y pensamiento computacional (lógico). En ese marco es que hablamos de una serie de competencias digitales de lecto-escritura, que no sólo pueden ser medibles, sino que se diferencian enormemente entre generaciones, regiones socioeconómicas y socioculturales.

No obstante, para los fines de este texto y en contraposición a los autores que suponen que la cultura digital es una serie de competencias digitales (parece que cada vez más refinadas), habría que señalar que respecto de la ciudadanía digital –si bien se relaciona evidentemente con los grados de alfabetización de sus constituyentes–, lo importante es cómo una comunidad lee, entiende y prioriza sus valores e ideas de manera conjunta y busca, por algunos de cientos de medios digitales, expresar su situación, propuestas o una serie de injusticias en su contexto próximo.[2] A partir de que la esfera de lo privado y lo público cada vez se desdibuja más por la exposición pública de lo privado de las personas, así como aquel déficit democrático, debemos prestar más atención a las distintas culturas digitales que generan distintos movimientos digitales.

Y es que recordemos que la teoría de los nativos digitales (Prensky, 2001), no consideró que las empresas relacionadas con el mundo digital se hayan empeñado cada vez más en hacer sus servicios y dispositivos en un ambiente (*affordance*) (Gibson, 1979) cada vez más amigable: "En los espacios digitales, los *affordances* pueden

2 En ese sentido, una comunidad en un área remota que se organiza y toma un video que alguno de sus agremiados sube a la Red por alguna red social, tiene tanto valor como las organizaciones de áreas urbanas o de grandes urbes, que pueden moverse en varios canales (redes, plataformas, foros, por mencionar algunos).

parecer naturales, pero están diseñados por los creadores del sitio para dirigir específicamente al usuario a navegar la tecnología de una manera particular" (Davisson y Leone, 2018: 87). De ahí que un celular o una tablet puedan ser usados por infantes, como por una persona con una menor competencia en lectoescritura.

Las redes sociales y los foros de debate han permitido que la ciudadanía fortalezca sus lazos de cooperación horizontal, creación de información, participación con valores, creencias e ideas compartidas que generan la circulación de reflexiones, críticas, expresiones propias, entre otros, es decir, una colaboración creativa (Zappen, 2005: 321).

CIUDADANÍA DIGITAL, MOVIMIENTOS SOCIALES Y RECOPILACIÓN-ALMACENAMIENTO DATOS

Parece que hemos dejado claro que la aparición de la integración de la tecnología digital a nuestras vidas ha puesto de manifiesto un cambio radical en la discusión de lo público, principalmente de la política. La participación ciudadana, de manera particular la digital, en la esfera de lo público ha permitido ampliar el plano de discusión a prácticamente cualquier persona que pueda disponer de un dispositivo y acceso a la Red. Sin embargo, esto no es así de sencillo, dado que, como hemos visto, existe una división social que fragmenta las distintas comunidades al crear brechas que hacen que tal participación ciudadana, desde los contextos locales, y con una lectura del mundo propia llena de subjetividades y consumo digital, difiera de un caso a otro.

> Las redes sociales son altamente efectivas en expandir la voz de los ciudadanos, que hoy pueden expresar libremente sus propios mensajes de manera virtual. Así, la producción de la información ha cambiado de tener un solo emisor que transmita a múltiples receptores a múltiples emisores y múltiples receptores. Además, ya no son las grandes corporaciones y el gobierno los que controlan, sino que cualquier usuario que tenga acceso a las TIC adecuadas puede compartir y publicar información de manera sencilla e inmediata (Lara Caballero, 2014: 76).

Si bien México ha aumentado la penetración de Internet a los hogares en los últimos años, la brecha digital aún se encuentra muy por debajo de lo requerido como para permitirle a la población un mayor contacto con el gobierno y ser ciudadanos más participativos. A ello debemos sumar que las condiciones socioeconómicas de buena parte de la ciudadanía, a lo largo del país, son cada vez más precarias, por lo que pagar la renta de Internet y, además, lograr costear un equipo de gama baja, es apenas posible en zonas urbanas y áreas aledañas a las megaciudades. Por otra parte, existe una condición de infraestructura que aún requiere ampliar la cobertura del país.[3] Estas circunstancias desincentivan a la ciudadanía digital en tanto que, si bien se pueden organizar de manera tradicional exponer sus casos, preocupaciones y necesidades, muchas veces queda fuera de sus manos. Aún así hemos visto cómo se han creado movimientos a lo largo del país en zonas remotas que buscan mejores condiciones de existencia.

En México, la ciudadanía digital ha hecho uso principalmente de dos redes sociales, Facebook y Twitter, si bien es cierto que el buscador más importante, no sólo en México, sino en todo el mundo, ya es YouTube. No obstante, nuevas generaciones están haciendo uso de otras redes sociales como Instagram, Reddit, Twich, 8chan (ahora 8kun), 4chan, y TikTok, entre otras. Aunque relativamente guarda ciertos patrones el perfil de usuarios de Twitter, hay marcadas diferencias, pero se trata de un espacio en el cual de modo general se dirimen temas de coyuntura por la propia estructura de la red y su tipo de lectoescritura. Según el informe de la plataforma *We Are Social* (2020) (apoyada por *Statista*, entre otros), poco más de 70% de la población mexicana hace uso de redes sociales, pero solamente 10% emplea Twitter aún cuando la propagación de la información podría alcanzar los 11 millones, principalmente por la velocidad con la que se pueden poner temas de manera prioritaria, gracias a los *hashtags*; pero además poco más de 60% son hombres y el resto, mujeres, de edades arriba de los 13 años. Esto nos indica que la repercusión de las comunicaciones de orden político por esta red es muy escasa en comparación con el total de la información que

[3] Buena parte de los celulares, que es el dispositivo más usado en México, aún se maneja en la banda 2.4 ghz, porque es la que reconocen los equipos de gama baja y media. Mientras que los equipos de alta gama pueden trabajar en la banda 5 ghz, pero evidentemente estos son más caros.

consume la población por otros medios, principalmente Facebook, YouTube o Instagram. Entonces, la plataforma de Twitter representa una brecha en términos de cultura digital, para la participación política, dado que es un círculo relativamente pequeño quienes participan en esta, a diferencia de las que ya se han señalado.

Aquí es donde lo que hemos expuesto sobre literacidad digital –como una forma de leer e interpretar la realidad– nos permite reflexionar sobre el papel que están cumpliendo otro tipo de lenguajes además del textual. La diferencia se encuentra en que siendo YouTube el buscador de más consumo junto con Google, maneja un lenguaje audiovisual, que puede generar interpretaciones distintas para hacer eco de la participación de la ciudadanía en la esfera pública y la política. En buena medida la mercadotecnia política, principalmente el tiempo de elecciones, se ha situado justamente entre Facebook y YouTube, generando condiciones nuevas para la participación política, la gobernanza y la comunicación.

En su conjunto, las principales redes sociales ya señaladas forman el ecosistema en el cual la ciudadanía digital en México suele establecer sus canales de comunicación y de organización. Encontramos así que los distintos movimientos de la ciudadanía digital más importantes que se han planteado en México tienen como particularidad formarse o darse digitalmente hablando en zonas urbanas y grandes urbes. Por ejemplo, desde la desaparición de los 43 estudiantes de Ayotzinapa, la guardería ABC, Soy 132, Vivas nos queremos, se formaron como ecosistemas digitales que conjuntan tanto el uso de redes sociales vinculadas al texto, como a la imagen (fotografía y video). Si bien el fenómeno social principal pudo haberse dado fuera de una zona urbana, es en el centro (áreas urbanas) donde se genera la discusión y expansión digital.

Por otra parte, tenemos otros fenómenos aún más locales que se relacionan con el cuidado del medio ambiente o zonas en peligro por el calentamiento global, desaparición de mujeres y menores de edad, situaciones de seguridad respecto del narcotráfico, entre otros, que al ser locales, depende en buena medida de saber aprovechar la velocidad de los mensajes, el tipo de plataforma y la cantidad de personas afectadas, para que los mensajes, y expresiones puedan volverse tendencia nacional en cualquiera de estas plataformas. Este es un fenómeno de gran ayuda para, por ejemplo, la localización de personas o para condenar y pedir justicia en el caso de los feminicidios o las situaciones de corrupción.

Como bien indican Natal e Ibarra (2014), Twitter es una red social altamente dependiente de la coyuntura político-social y es una referencia por el tipo de mensajes que se pueden dar para los medios de comunicación masiva, además de generar tendencias. Sin embargo, Facebook ha sido utilizado por otras organizaciones sociales haciendo uso de la ciudadanía digital para fenómenos más específicos, como pueden ser el trato a los migrantes centroamericanos, las madres de hijos desaparecidos por el narcotráfico, la violencia en ciertos estados, la preservación de zonas con ecosistemas en peligro, la protección de animales, la trata de personas con distintos fines; mientras que YouTube, al ser un espacio audiovisual, tiende a una discusión más amplia, no necesariamente argumentada, pero más cercana a un tipo de perfil que prefiere tener información en un formato distinto.

Si bien hemos dicho que las diferentes culturas digitales que tenemos a lo largo y ancho de nuestro país han creado un ecosistema de redes y plataformas de participación en el que claramente se observan las divisiones sociales y las brechas digitales, la ciudadanía se ha organizado y expresado, pero esto no es muy diferente que en otros países. Por ejemplo, el uso que hicieron los presidentes Obama y Trump para sus campañas electorales, el movimiento feminista *Me Too*, la relación entre jóvenes combatientes por medio de redes sociales en la *primavera árabe*, el movimiento de mujeres latinoamericanas Ni una más/ Vivas nos queremos, la revolución de los paraguas en Hong Kong, la operación *Lava Jeto* en Brasil, *Black Lives Matter*, los chalecos amarillos en Francia, el M-15 en España, las manifestaciones en Chile y en Colombia, son sólo algunos de los casos que podemos rastrear alrededor del mundo, y que acompañan a otros que son aún más locales. Pero en este mismo nivel de actividad también encontramos otros movimientos sociales que deben ser tratados con mucha cautela, como las campañas en redes sociales del Estado islámico de Iraq y Siria (ISIS, por sus siglas en inglés) para sumar soldados a sus filas, los llamados al racismo, a la xenofobia y los discursos antimigrantes, los movimientos de personas antivacunas, los terraplanistas, incluso el fenómeno de *QAnon* en Estados Unidos, que generó la toma del Capitolio en 2021. Otros

casos que se han dado es la política del tuit, la diplomacia digital, la twiplomacy, por mencionar algunos.

Por esta tendencia que se ha señalado es que el tema de la recopilación, almacenamiento, tratamiento y uso de los datos personales, principalmente en las redes sociales, foros y otras plataformas, se vuelve un asunto delicado que puede atentar contra los derechos humanos, los derechos civiles y la propia libertad de expresión. En la mayor parte de los países existe legislación sobre la protección de datos personales. Sin embargo, el uso que se hace con fines monetarios por parte de las grandes corporaciones digitales, haciendo uso de la inteligencia artificial, es una asignatura pendiente en todo el mundo. La creación de perfiles psicológicos, de estado, de humor, situación financiera, reconocimiento facial, datos biométricos, gustos y preferencias, son aspectos que la IA trabaja cotidianamente y que no está debidamente normado.

Recordemos que la inteligencia artificial ya se ha comenzado a usar no sólo con fines de generación de perfiles para la mercadotecnia, sino para las campañas electorales, crear tendencias o manipulación de información con intenciones políticas. Aunque esta tecnología permite grandes beneficios a la humanidad como en el caso de la salud, los sistemas meteorológicos o los de tránsito, también ha sido usada para armamento autónomo (como drones), seguimiento y búsqueda de personas en diferentes países a partir de su reconocimiento facial, la manipulación de mercados y de inversiones, por mencionar algunos. Varias empresas de tecnología digital son muy opacas y poco transparentes en el uso de la información que recopilan, y en el objetivo de su tratamiento. De los diversos datos que proporcionamos, ya sea porque los generamos y entregamos a las empresas, o bien porque dejamos huella digital, prácticamente no volvemos a saber nada, ni siquiera si siguen siendo almacenados y por cuánto tiempo o si ya han sido destruidos. La propia reputación digital, incluyendo la empleabilidad de una persona, depende de esa información, siendo una máquina quien toma una decisión de vida.

Hay que recordar que existen datos que no son de contenido individual o personal y que, por lo tanto, no hay consecuencias en el ámbito de la privacidad; un ejemplo de ello es el seguimiento de huracanes, tsunamis, temblores y otros fenómenos meteorológicos, además de aviones, barcos, movimientos cíclicos de animales, tránsito urbano; sin embargo, los datos que en realidad más preocupan son aquellos de tipo privado-personal que se procesan para distintas tomas de decisiones o generación de perfiles económicos, financieros, educativos, políticos, o incluso migratorios y de salud. En este aspecto, las mayores preocupaciones de la ciudadanía digital respecto de la inteligencia artificial se han centrado no sólo en esta recolección de datos, sino en la opacidad del diseño y creación de algoritmos y, en especial, su operación, en la cual las máquinas toman decisiones.

NORMATIVAS SOBRE INTELIGENCIA ARTIFICIAL

Las *Directrices de privacidad de información y datos* de la OCDE se publicaron por primera vez en 1980, fue uno de los primeros instrumentos normativos. Sin embargo, Cukier (2017) advierte que este marco regulatorio se planteó en un contexto diferente; si bien la inteligencia artificial ya estaba generando tecnología comercial, se ponía en tela de duda acotar la recolección de información y la necesidad de especificar los propósitos así como la limitación de uso. En ese sentido, este acuerdo no beneficiaba el desarrollo de la inteligencia artificial, principalmente por el cuestionamiento al uso de datos privados. Para Cukier no sólo han cambiado los métodos y formas de recolección de datos sino que los usuarios son diferentes: por ejemplo, anteriormente los datos se generaban de una manera pasiva, hoy en día los usuarios no solamente los crean, sino que los consumen, ya sea a través de aplicaciones, *streaming,* información en general, y todos los elementos que se han señalado de la evolución social a través de las TIC. Otro caso era la obtención de datos de las personas, empresas u otras entidades con un sólo fin, mientras que hoy en día se pueden intercalar, interconectar, o asociar grandes cantidades de datos información con varios propósitos; incluso los métodos de tratamiento de datos se basaban en una estadística tradicional frente a la que emplea la inteligencia artificial, como los árboles de decisión o las redes neuronales.

Una versión considerablemente más evolucionada es el *Reglamento General de protección de datos de la Unión Europea* (GDPR, por

sus siglas en inglés), que tiene entre algunos de sus propósitos apoyar a la sociedad cuando se requiere recolectar datos por terceros actores comerciales (Facebook, Amazon, Google); pues al tiempo que se necesita mantener la protección de los datos, principalmente los de tipo personal, respecto del propósito, se debe hacer el menor uso de estos y su limitación para usos específicos con fines comerciales. Este reglamento, si bien data de 2016, entró en vigor completamente en 2018. Se trata de una normativa que unificó derechos y obligaciones de los países pertenecientes a la Unión Europea, dado que anteriormente las distintas empresas tecnológicas tenían que hacer adecuaciones operativas sobre la normativa de 28 países .

La novedad de este reglamento es que afecta a cualquier empresa que quiera recoger, guardar, tratar, usar o gestionar los datos y la información de los ciudadanos de la Unión Europea. Un aspecto que inaugura es no sólo la posibilidad del derecho al olvido y a la portabilidad, sino a que los datos personales sean eliminados una vez que han sido usados para su propósito, un aspecto sustancial que se verá poco más adelante, pues, de hecho, los ciudadanos europeos pueden solicitar a las empresas que confirmen si sus datos están siendo usados, por cuáles mecanismos y con qué finalidades. No obstante, existen algunas inquietudes en aspectos vitales en torno a la ciudadanía digital, como el hecho de que en el caso de las redes sociales, las empresas están obligadas a regresar los datos que las personas hayan entregado.

En el caso del uso de sistemas de gestión y servicios de datos, los contratos deben de dejar en claro, por ejemplo, de qué trata el servicio y cuáles son las condiciones, y también se debe señalar el tratamiento de la información. Técnicamente, en la Unión Europea este tipo de procesamiento debe ser claro para el ciudadano promedio. Finalmente, las empresas que prestan servicios en los que se manejen datos, tienen 72 horas para dar parte tanto a las autoridades de un país, de la Unión así como los clientes o usuarios, si hubieran tenido fallas en la seguridad. Al igual que en otros casos, siempre debe existir una persona responsable de los datos personales-privados, pero más específicamente respecto de su uso con fines publicitarios o de seguimiento del comportamiento de las personas.

No obstante, Cellarious (2019) advierte que, dado que la industria comercial requiere de enormes cantidades de datos, es

complicado lograr homologar los principios de protección de datos, dado que son heterogéneos, en cuyo caso se ha planteado que la Unión Europea debería proveer pautas que le permitan a sus ciudadanos el derecho de determinar el modo en cómo se usarán tales datos, principalmente respecto de la privacidad. También implica que el diseño del uso de los datos deberá ser similar en su arquitectura para todas los las empresas, por el tema de portabilidad, que es un derecho de los ciudadanos. Sin embargo, se ha encontrado que, mientras las grandes empresas sí pueden establecer este tipo de estructuras, las medianas y pequeñas pueden tener problemas para generar esos mismos modelos. Si bien podría parecer una normativa con incorporaciones novedosas, por ejemplo, en relación con distintos fenómenos que se han dado en la ciudadanía digital, incluso este reglamento requiere rectificaciones en especial, porque la evolución de la inteligencia artificial ha ido avanzando rápidamente, así como el uso de las tecnologías por parte de la ciudadanía organizada; pero aquí tan sólo hablamos del uso de datos, no de recolección y tratamiento con inteligencia artificial.

En 2021, la Comisión Europea finalmente presentó la legislación sobre inteligencia artificial, el cual se considera el primer marco legal formal de este tipo (Parlamento Europeo, 2020-2021), al que se suma una normativa sobre la maquinaria autónoma y los robots. En principio se busca aumentar la seguridad y definirla frente a los consumidores (ciudadanos), a la vez que genere certeza para la inversión en inteligencia artificial en el territorio de la UE. Dado los riesgos y retos del uso de la inteligencia artificial, principalmente enfocada en la recolección y procesamiento de datos personales, en esta normativa la UE estableció cuatro niveles de riesgo: mínimo, limitado, alto e inaceptable. Solamente quedó excluido de esta tipología el uso militar de la inteligencia artificial. Respecto de esta contingencia, es evidente que ambas regulaciones (de datos e IA), tendrán que trabajar de la mano, puesto que, por ejemplo, un riesgo inaceptable es considerado una amenaza para la seguridad, los medios de vida y los derechos de las personas. Un caso podría ser que se manipule el comportamiento humano o se incite a la violencia mediante las redes sociales, lo cual justamente ya se ha dado; o bien, un gobierno puede argumentar que un movimiento social o una organización

incitan a la violencia o quiere manipular a la ciudadanía. Llama la atención que, en el caso del riesgo limitado, la normativa sobre inteligencia artificial señala que los ciudadanos deben ser informados cuando están hablando o interactuando con máquinas, como con *bots*; este es un ejemplo completamente diferente al que se dio en su momento con el bot Watson en educación, que era una máquina de apoyo a los estudiantes en la revisión de sus trabajos escolares, quienes muchas veces asumieron que trabajaban con personas reales; o bien, como sucede en el caso de México, donde se han investigado granjas de *bots*, que funcionan no solamente en periodos electorales, sino para crear tendencias o discusiones sobre temas que civilmente son importantes.

Para finalizar, un tema espinoso es la identificación facial, considerando que existen otros países su uso se ha hecho frecuente, principalmente en zonas públicas, con finalidades asociadas a la seguridad nacional. En el caso de la Unión Europea se prohíbe su uso en estas áreas, pero se podría emplear en algunas situaciones "especiales" o para detectar a una persona desaparecida, como un menor de edad o buscar a un delincuente o terrorista. Si bien es cierto que esto es un avance, también preocupa, pues su uso, aunque se tiene que dar bajo la autorización judicial, se puede emplear tanto en movimientos sociales, manifestaciones, como en detectar a migrantes a partir de sus características étnicas y de género, u opositores a un gobierno. En este tema, la UE ha puesto aparentes excepciones al reconocimiento facial, así como a la recolección de datos biométricos de los ciudadanos, sobre todo cuando sean usados drones con fines de seguridad, pero que lleven la intención de hacer el reconocimiento, por ejemplo, de manifestantes, lo cual supondría atentar contra diversos derechos civiles.

Ahora bien, queda pendiente la situación de dos países y su legislación interna respecto de la inteligencia artificial: Estados Unidos y Reino Unido. Para estos dos territorios debemos de considerar que la IA y su posible regulación parten de un enfoque completamente diferente al de la Unión Europea, o al que veremos más adelante, en otras instancias internacionales. La IA está relacionada directamente con dos aspectos básicos para estos dos Estados: la tecnología, que está conectada con la seguridad nacional y los negocios. No es casualidad que la mayor cantidad de inversión en IA privada y usada con fines gubernamentales se dé en Estados Unidos y en una menor proporción en Reino Unido. En ambos casos, la IA está relacionada con el aparato militar, así como la vigilancia, el uso de drones, por ejemplo, para reconocimiento facial se había ya usado en Estados Unidos anteriormente, su uso en el campo militar también se había estado dando, los riesgos y amenazas a la estructura crítica, seguimiento meteorológico, estudios de salud, entre otros. La National Security Agency (NSA) en su momento permitió el uso de la IA para dar seguimiento y reconocimiento a personas dentro del territorio estadounidense con fines de vigilancia contra el terrorismo, basados en perfiles de cuentas de correo, análisis de lenguaje natural, movimiento de cuentas bancarias, y perfiles en redes sociales. Todo esto con permisos de tribunales específicos con mucha opacidad, que no se manejaban de manera regular en el ámbito de lo público.

Podemos, entonces, concluir que ambos países no cuentan con una legislación específica en inteligencia artificial, y posiblemente no contarán con una jamás, dado que esta tecnología en realidad está normada en varios instrumentos internos, muchos de ellos, como se había señalado, en relación con la seguridad nacional; además de que el manejo de datos personales está regulado de un modo distinto y por separado a la IA (tal como lo estaba la UE), al igual que sobre *big data* y algoritmos. En ese sentido, el enfoque del Estado no se centra en los ciudadanos y sus derechos civiles y bienestar, sino en su uso de manera industrial, enfocado en los negocios o bien, para uso militar.

En el caso de los negocios, una legislación centrada en los ciudadanos y sus derechos probablemente generaría el efecto no deseado en la Unión Europea, que es menoscabar la oportunidad y libertad de las empresas en investigación en inteligencia artificial. De ahí que, empresas como Microsoft, Amazon, Facebook, Twitter, Google, Tesla, entre algunas de las más importantes, sí hayan logrado desarrollar esta tecnología sin un freno normativo. Incluso empresas como Netflix lograron contar con proveedores de ia más sofisticados, lo cual ha permitido su rápido crecimiento y expansión. Lo mismo podríamos señalar de los bancos del sistema financiero. La generación de patrones y perfiles para dar créditos se basa, en buena medida, en cruzar datos con información que las personas proveen. En consecuencia, los gobiernos estadounidense y del Reino Unido han

dejado en las manos de las propias empresas la creación de códigos de conducta y principios éticos acordes con los objetivos y propósitos de las empresas, incluyendo, evidentemente, el uso de los datos con fines de ganancias monetarias.

Esto explicaría en buena medida por qué cuando se dio el caso de Cambridge Analytica, Mark Zuckerberg tuvo que pasar ante el Congreso y ser cuestionado respecto de la responsabilidad de la recolección y tratamiento de datos, pero particularmente la facilidad del uso de terceros sin permiso. En ese sentido distintas organizaciones civiles en Estados Unidos, así como del Reino Unido han seguido luchando para que se regulen; pero este tema no parece estar en la agenda inmediata y evidentemente no fue considerado de forma sustancial, específica y profunda en el T-MEC. Lo que se tiene en ambas naciones son comités que analizan directamente –como en Estados Unidos– o bien, consultan a una serie de expertos –o a entidades como el Select Committee on Artificial Intelligence, del Reino Unido (House of Lords, 2018) y la National Security Commission on Artificial Intelligence (NSCAI) de Estados Unidos (2021)– las consecuencias del uso de IA sobre los ciudadanos. En ambos casos sólo se generó una serie de recomendaciones en múltiples áreas, con principal énfasis en el desarrollo de la IA y los negocios, así como otras aplicaciones. De modo evidente, aspectos como el reconocimiento facial son temas que posiblemente no se toquen del todo, porque, como se mencionó antes, están en algún sentido regulados en otros documentos. En un momento en que en Estados Unidos las luchas civiles y movimientos ciudadanos digitales justamente han encontrado eco tanto dentro, como fuera de ese país, el reconocimiento facial a grupos específicos como los afroamericanos o los latinos, en áreas públicas, crearía aún más revuelo.

PRINCIPIOS ÉTICOS Y POLÍTICOS INTERNACIONALES

Por otra parte, el Instituto de Ingenieros Eléctricos y Electrónicos (IEEE, por sus siglas en inglés) es una de las organizaciones que ya han comenzado a trabajar sobre una serie de pautas, principalmente enfocadas en la IA: "Asegurar que todos los interesados e involucrados en el diseño y desarrollo de sistemas autónomos e inteligentes estén educados, capacitados y capacitados para priorizar consideraciones éticas de modo que estas tecnologías avancen en beneficio de la humanidad" (IEEE, 2019). Llama la atención que el documento titulado *Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems* (2019), generado como parte del IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems, cuenta con una base axiológica y ética que proviene de varias tradiciones de valores de alrededor del mundo (Occidente, Oriente, África, entre otros). Su propósito es ético, legal y técnico, dirigido tanto al gobierno, ciudadanos, como al mundo de los negocios.

Sus principios generales son ocho, entre los que pueden destacar, para las finalidades de este texto, poner en primer lugar los derechos humanos, en el sentido de que todo diseño de IA debe ser creado y operado para respetar, promover y proteger este marco; también destaca el bienestar como el principal criterio de creación; la importancia de la relación entre la agencia de las personas y sus datos, en tanto que la IA debe empoderar a los ciudadanos para que puedan compartir su información privada no sólo de manera segura, sino que tengan las bases para controlarlo; tanto diseñadores, como operadores deben prestar evidencia del uso de que este tipo de tecnología está siendo efectiva para su propósito; en ese tenor, la decisión de las máquinas debe ser transparente; ese mismo principio debe ser extensivo al tema de la responsabilidad con base en decisiones bien fundamentadas; de ahí que creadores y operadores tengan consciencia de los riesgos que se pueden dar o de usos indebidos; y finalmente, la necesidad de que quien opere tal IA tenga la información y formación suficiente para hacerlo (IEEE, 2019: 10-12). También la propuesta cuenta con otras secciones en áreas como educación, impacto al medio ambiente, marcos legales y métodos de aplicación.

En el caso del Future for Life Institute, que se dedica a la investigación y divulgación sobre temas que generan riesgos y amenazas para la humanidad (cambio climático, armas de destrucción masiva, biotecnología e IA), ha desempeñado un papel fundamental para analizar el potencial de la IA, no sólo en el nivel tecnológico, con los posibles beneficios de diverso orden que pueda traer al desarrollo humano o la salud, sino especialmente en los planos ético y político: "[La inteligencia artificial] también

podría permitir una desigualdad sin precedentes, la pérdida de la privacidad y las libertades civiles, concentraciones excesivas de poder y un riesgo extremo de daños personales y en toda la civilización" (Future for Life Institute, s/f). En esta materia el Instituto ha trabajado seis áreas de información: *1)* beneficios y riesgos de la IA, *2)* armas letales autónomas, *3)* reconocimiento superinteligente, *4)* políticas (programas y estrategias alrededor del mundo sobre IA), *5)* alineación de valores accionados con la IA, *6)* los principios éticos para IA de Asilomar.

Por otra parte, el Instituto considera que existen varios desafíos políticos y éticos de la IA que están altamente relacionados con riesgos que se conectan de modo directo con el día a día de las personas, que van desde aspectos relacionados con la investigación, la gobernanza global, el empleo, la economía, los derechos y libertades civiles, pasando por las máquinas autónomas, hasta el panorama de la inteligencia general artificial. De los puntos relacionados con la ciudadanía digital, porque evidentemente se han observado en la última década diversos fenómenos que, como advertimos líneas arriba, se asocian con el déficit democrático, la infodemia y desinformación, la vigilancia y autovigilancia, las demandas sociales, movimientos sociales, por mencionar algunos.

En esta misma línea, el Future for Life Institute ha generado un modelo, a manera de panorama, sobre la interconexión de diversas áreas prioritarias para políticas respecto de la IA; es importante destacar que la relación entre la gobernanza y la ética, en la que justamente se observan los retos y desafíos de esta tecnología, por ejemplo, sobre consideraciones que los gobiernos deberían tener sobre políticas domésticas, normas sociales, políticas aplicadas y, evidentemente, el marco regulatorio de la inteligencia artificial.

Por otra parte, la OCDE cuenta con un Observatorio de Políticas de Inteligencia Artificial en la que también trabaja principios, así como recomendaciones sobre políticas acerca de la IA. Respecto de los principios, la valoración general es que si bien se basan en colocar en el centro del diseño y operación de la IA a las personas, los temas son más limitados y menos específicos, en virtud de que la organización ha decidido que sean lo más flexibles para que un mayor número de países se pudieran adherir a ellos.

A diferencia del IEEE y del Future for Life Institute, en el caso de la OCDE, los temas sobre privacidad, vigilancia, derechos civiles, entre otros, no se encuentran contemplados como principios en sí mismos entre distintos agentes de manera interconectada, sino que están orientados hacia los gobiernos, mercados y finanzas. No obstante lo anterior, el Observatorio tiene entre sus áreas de investigación sobre políticas públicas, aspectos de la gestión del gobierno digital y del empoderamiento de los ciudadanos mediante la IA.

La diferencia entre los principios que sostiene el IEEE y el Future for Life Institute, es que se basan principalmente en la conexión entre ética, política e ingeniería; mientras que los de OCDE se refieren sobre aplicabilidad pero no tienen un cometido ético-cívico claro para fines de este texto.

Consideraciones éticas y jurídicas regionales para América del Norte en el marco de la relación trinacional sobre la relación ciudadanía digital e inteligencia artificial

Nos encontramos en una fase importante, viendo hacia el futuro la reflexión y regularización de la inteligencia artificial. Se comienzan a dar los primeros trabajos globales y regionales que permitan considerar marcos de referencia, principalmente, sobre el manejo de los datos personales, en relación con la definición de perfiles y patrones éticamente aceptables y legalmente viables, además de la responsabilidad jurídica de quien los diseña. La reflexión desde las humanidades y las ciencias sociales en relación con los tecnólogos y la autonomía de las máquinas para tomar decisiones, es que solamente ellas deban realizar las que cumplan con principios éticos que no violenten los derechos fundamentales de cualquier ser humano. Hay otros temas pendientes, como la corrección de algoritmos, la curaduría de datos, la integración de bases, cuidado al acceso y elección, propósitos de la limitación y su confidencialidad entre otros (Fleischer, 2017).

Adicionalmente, habría que considerar que también es necesario reflexionar desde la ética, la tecnopolítica y la infraestructura de datos sobre la gobernanza digital. Uno de estos aspectos tiene que ver con la administración de la infraestructura digital: sabemos muy bien que en el caso de la IA, la recolección de datos es vital para el trabajo de esta tecnología; en el caso de la ciudadanía

digital, dado que la mayor parte de las organizaciones buscan trabajar por medio de redes sociales comerciales, los agentes externos utilizan estos para crear perfiles lo más detallado posible de los diferentes usuarios, los cuales tienen que ver con preferencias, gustos, contenidos creados, ánimos de las personas e incluso con los sesgos cognitivos. El fruto de la aplicación de algoritmos le permite a las grandes empresas no sólo tener mayor conocimiento sobre sus usuarios, sino la monetización de la información, por una parte, así como la venta de espacios para anuncios de todo tipo. En ese sentido, como bien señala Owen (2017), existen algunos elementos de la gobernanza de la Internet relacionados con los espacios públicos digitales, dado que estos están siendo dominados, de manera principal, por empresas privadas, cuyos intereses no necesariamente van de la mano de la ciudadanía digital o de los gobiernos, por lo que el uso de los datos privados quiere decir que se van a usar por el bien común. Aunado a esto, la compleja y rápida evolución de la inteligencia artificial, principalmente en redes sociales y otros servicios, como el *streaming*, pero también la inteligencia de las cosas (IoT), el mundo financiero, la salud, nos permiten concluir que los distintos gobiernos alrededor del mundo todavía no cuentan con la suficiente capacidad técnica, profesional, tecnológica, jurídica, sociopolítica, para regular a estas grandes empresas digitales. Uno de estos temas es, por ejemplo, la irrupción del *marketing* político en las redes sociales, esencialmente en los periodos de elecciones y la aparición de las *Fake News*.

La ética es la gran paradoja entre privacidad *versus* beneficio. Por ejemplo, es claro que recolectar datos sobre el tráfico en las ciudades más congestionadas y utilizar IA para una mejor gestión de esta, traería un beneficio. Sistemas como Google Maps o Waze, justamente recolectan los datos a partir de usuarios individuales, cuyo derecho a la privacidad y derecho constitucional de libertad de tránsito se pueden ver comprometidos en tanto vigilancia. Es claro que las personas que cuentan con uno de estos dos sistemas, cuando descargaron la aplicación aceptaron los términos y condiciones de ambas empresas, aunque ello no supuso una reflexión profunda jurídica, ética y civil de lo que implicaba dar sus datos de manera "gratuita".

Otro caso podría ser para el el sector de la salud: la recopilación de varias imágenes sobre diversos tumores y enseñarles a las máquinas a reconocer cuáles son de tipo benigno y cuáles malignos, reporta un enorme beneficio, el cual permitirá contar *a posteriori* con tecnología que detecte posibles enfermedades en los puntos más tempranos de gestación.

No obstante, en el caso de la ciudadanía digital, la recolección de datos puede afectar las formas de organización, en la medida en que no haya una protección real de los algoritmos una vez que se han recopilado los datos. Si bien México cuenta con marcos regulatorios sobre la protección de información, no se ha determinado si esta va a generar un uso provechoso al momento de su recolección y si, por lo tanto, los ciudadanos deberían ser advertidos, incluyendo la opción de que sea destruida o reutilizada. En ese sentido, las empresas que controlan las redes comerciales deberían contar o adaptarse a diversas estrategias nacionales de privacidad y, en el caso de América del Norte, principalmente con unas de corte regional; de manera que los tres países no vean vulnerados los derechos políticos cívicos de la ciudadanía. Ya que, desde el punto de la ciudadanía digital los nacionales quedan bajo la vigilancia de dos entes: por un lado las empresas y, por otro, los gobiernos.

Dado que, como se ha expresado líneas más arriba, las esferas de lo privado y lo público en la era digital han comenzado a disolverse, el derecho a la organización digital de la ciudadanía implica generar gran cantidad de datos que las empresas pueden comercializar y que no necesariamente están en la línea del bien común, o de diversas causas sociales políticas, culturales o económicas. La necesidad de expresión a través de redes sociales implica o tiene como consecuencia las ganancias financieras y la vigilancia de los grandes consorcios, con bajo o nulo control de los datos de los ciudadanos.

El problema radica en que pensamos en IA como una sola, cuando sus aplicaciones son diversas, por lo que la regulación y las estrategias deberían considerarse según sus usos, así como beneficios y posibles riesgos sobre el manejo de información, principalmente privada. Como comenta Freeman (2017), la necesidad de reglamentación y el marco para la aplicación de IA requiere pensar los beneficios junto con el tema de los riesgos en el largo plazo. En los entornos digitales,

mucha de la responsabilidad se deja sobre los hombros del usuario al aceptar largos contratos en la web o en aplicaciones, en tanto que los proveedores de los servicios dicen testificar mediante tan largo y poco entendible convenio, que su sistema es seguro; aunque en la práctica no contamos con mecanismos de defensa jurídica, porque muchas de las plataformas se encuentran en terceros países o sin representación en México. Esto se ajusta no sólo a las empresas de redes digitales, sino para cualquier plataforma, incluyendo el comercio electrónico. De manera regional, tampoco contamos con mecanismos de salvaguarda del uso de datos personales con fines de tratamiento con inteligencia artificial.

La responsabilidad jurídica, ética y moral debería de recaer tanto en los productores de los distintos dispositivos (*hardware*), como de los sistemas de servicios que emplean inteligencia artificial (*software*), de modo que la responsabilidad sea común.

Entonces el tema de la regulación de la inteligencia artificial no se limita a la recolección ni al tipo de datos que son, los métodos, los algoritmos, la pasividad, el tema de privacidad, evidentemente, sino a la responsabilidad. Pongamos algunos ejemplos: en los eventos de la *primavera árabe*: ¿se debería de culpar a las redes sociales comerciales por las manifestaciones en las calles de Túnez o Egipto o al gobierno o la ciudadanía organizada o a los productores de dispositivos? ¿Por qué sí hubo una responsabilidad para Cambridge Analytics y Facebook en la generación de perfiles de los usuarios de este último, principalmente, para crear tendencias en las elecciones Trump *versus* Clinton? Borges (2017) señala precisamente que el tema de las obligaciones y el sistema o los sistemas jurídicos tendrían que estar evolucionando en relación con la propia evolución de la IA. Para ello, el autor pone el caso en la conducción de automóviles, en el cual son las personas las responsables de los daños causados al haber un choque o algún imperfecto contra un tercero, es lo que llamamos responsabilidad civil. Pero qué es lo que debería de suceder, pensando en el mediano y largo plazos, cuando el dueño de un automóvil autónomo acaso tuviera un accidente. La obligación, entonces, se modifica completamente si bien el dueño de dicho automóvil es responsable por haber adquirido un bien de esta naturaleza, posiblemente también la

empresa constructora, así como la que diseñó y la que creó el sistema de navegación y el de conducción tengan incumbencia. El tema da para pensar cuál es la responsabilidad de las máquinas cuando toman decisiones autónomas, a diferencia de las que siguen órdenes. El riesgo, entonces, así como la responsabilidad, toman un tinte diferente. En los próximos años, las legislaturas deberían comenzar a pensar no solamente en automóviles autónomos, sino en toda máquina que tome decisiones por sí misma, considerando que aún cuando ya puedan tener esta acción propia, detrás de ellas existen humanos.

CONCLUSIONES

Una de las necesidades que debe de considerar el marco regulatorio para la región de América del Norte, de manera conjunta y no separada, es que los ciudadanos estén informados no sólo de la protección de datos, sino de qué pasa y cómo han sido obtenidos y el tratamiento que se les va a dar. Las máquinas y los algoritmos deben de quedar en resguardo jurídico de seres humanos, aun cuando existen decisiones que estas máquinas tomen de manera autónoma. Se requiere una protección no solamente para el resguardo de la información personal en la red, sino que, al ser empleada por las corporaciones digitales, estos datos se manejen, en todo caso, de manera anónima y se defina qué se va a hacer con ellos una vez empleados (¿almacenaje o destrucción?), y que cada ciudadano u organización social pueda exigir a las empresas información sobre el modo que han sido usados tales datos y con cuál algoritmo, es decir, evitar la opacidad.

En el marco de la relación trilateral en América del Norte, particularmente porque una buena parte de las empresas que desarrollan IA se encuentra en Estados Unidos, es necesario comenzar a reflexionar y abrir la discusión no sólo intergubernamental, sino con la sociedad civil digital organizada de los tres países, para regular el trabajo de las máquinas autónomas. La reglamentación, al igual que la gobernanza de la IA, debe crear un balance equilibrado que permita a las empresas seguir innovando y trayendo beneficios a las personas, pero con mecanismos de protección para los gobiernos y los ciudadanos, especialmente para que los espacios

públicos digitales ganados y esta observancia ciudadana se mantenga y se desarrolle como un contrapeso a los poderes fácticos. En ese sentido, se requiere pensar la ciudadanía digital y asegurar que siga funcionando para fortalecer a los distintos gobiernos y alcanzar el bienestar común, pensando que es necesario garantizar su desarrollo integral, lo que implica ampliar el enfoque de manera regional, dado que la ciudadania digital no sólo está creciendo cada día más, sino que se expande, y que siempre existe la posibilidad de las organizaciones civiles regionales (por ejemplo, de defensa de los migrantes indocumentados o de mujeres en situación de violencia o la trata de personas) y que cualquier ciudadano de los tres países, cuente con reglas claras sobre cómo se relacionan sus datos en la operación de la inteligencia artificial.

Si bien la naturaleza de la relación regional de América del Norte es muy distinta a la de la Unión Europea, sí se requiere pensar desde la ética, la cultura digital y los derechos civiles la correlación entre datos, operación de la IA y responsabilidad.

BIBLIOGRAFÍA

Barupa, S. (2017). Digital Divide: A critical analysis. Recuperado de https://bit.ly/3ITSyjR

Beck, U. (2019). ¿Qué es la globalización? Falacias del globalismo, respuestas a la globalización. España, Barcelona: Paidós.

Borges, G. (2017). Liability for machine-made decisions: Gaps and potential solutions. En *AI: Intelligent machines, smart policies,* OCDE. Recuperado de https://bit.ly/3HImoxt

Cellarious, M. (2019). IA: retos y oportunidades para la protección de datos. En *IA: Máquinas inteligentes, políticas inteligentes,* OCDE. Recuperado de https://bit.ly/3geRkDl

Cukier, K. (2017). Do privacy laws obstruct beneficial uses of data?, en *IA: Intelligent machines, smart policies*, OCDE. Recuperado de https://bit.ly/3ogFFZc

Davisson, A. y Leone, A. (2018). From coercion to community building. En Hess, A. y De Silva, A.D.S. y Frith, J. (2012). *Mobile interfaces in public spaces: Locational privacy, control, and urban sociability*: Routledge. Recuperado de https://bit.ly/3s9E48H

Estupiñán Villanueva, A., Molina Carmona, E., Flores Guevara, S. y Martínez Bermeo, J.R. (2016). Participação Digital na construção de e-democracia e cidadania digital. *ride. Revista Iberoamericana para la Investigación y el Desarrollo Educativo*, *7*(13), 126-146.

Fleischer, P. (2017). Data Protection and Ethics in the Age of Machine Learning. En *AI: Intelligent machines, smart policies,* OCDE. Recuperado de https://bit.ly/3giLLUt

Freeman, R. (2017). Evolution or revolution? The future of regulation and liability for AI. En *AI: Intelligent machines, smart policies,* OCDE. Recuperado de https://bit.ly/3rjO9kb

Future for Life Institute (s/f). Artificial Intelligence. Recuperado de https://bit.ly/3ssMnwL

Gibson, J. (1979). *The Ecological Approach to Visual Perception.* Houghton Mifflin.

House of Lords (2018). AI in the uk: ready, willing and able? Select Committee on Artificial Intelligence, Report of Session 2017-19. Recuperado de https://bit.ly/3rmoffT y https://bit.ly/3geRkDl

IEEE (2019). Ethically Aligned Design: A Vision for Prioritizing Human Well-being with Autonomous and Intelligent Systems. Recuperado de https://bit.ly/3ANCyNy

IEEE (2019). The IEEE Global Initiative on Ethics of Autonomous and Intelligent Systems. Recuperado de https://bit.ly/3ujGfcH

Lara Caballero, M. (2014). La brecha digital en un contexto. En Natal, A. *et al.* (eds.). *Ciudadanía digital.* Universidad Autónoma Metropolitana, Unidad Iztapalapa/Unidad Lerma.

Leetoy, S., Zavala-Scherer, D., y Sierra, F. (2019). Tecnopolítica y ciudadanía digital. Comunicación y Sociedad, 16, 1-8. Recuperado de https://bit.ly/34rFHpY

Lévy, P. (2007). Cibercultura: informe al Consejo de Europa. *Cibercultura*, Antropos/UAM-I, 1-254.

McChesney, R. (2013). *Digital Disconnect: How capitalism is turning the Internet against democracy*, The New Press.

Natal, A. e Ibarra, M. (2014). Movimientos virtuales: Twitter y la acción colectiva en México. En Natal, A. *et al.* (eds.). *Ciudadanía digital.* Universidad Autónoma Metropolitana, Unidad Iztapalapa/Unidad Lerma.

Natal, A., Ortega, W. y Martínez, Ma. G. (2014). Ciudadanía digital: desconfianza política y uso de internet para el ejercicio de la ciudadanía. En Natal, A. *et al.* (eds.). *Ciudadanía digital.* Universidad Autónoma Metropolitana, Unidad Iztapalapa/Unidad Lerma.

National Security Commission on Artificial Intelligence (2021). Final Report, Congreso de Estados Unidos. Recuperado de https://bit.ly/3rlXV5e

OCDE (2019). IA: Máquinas inteligentes, políticas inteligentes, núm. 270, ocde Publishing, Paris/Asociación Mexicana de Internet. Recuperado de https://bit.ly/3scSBR9

OCDE (2019). Recommendation of the Council on Artificial Intelligence, Legal Instruments. Recuperado de https://bit.ly/3ogFiOc

OCDE (2021). AI Policy Observatory. Recuperado de https://oecd.ai/

Owen, T. (2017). Governing Digital Infrastructure. En *AI: Intelligent machines, smart policies*, ocde. Recuperado de https://bit.ly/34rIKyy

Petrizzo Páez, M.Á. (2005). Participación ciudadana y tecnologías de la información y la comunicación: Hacia una administración pública relacional. *Nueva sociedad*, *195*, 88. Recuperado de https://bit.ly/345ZT17

Parlamento Europeo (2020-2021). Resolución del Parlamento Europeo, de 20 de octubre de 2020, con recomendaciones destinadas a la Comisión sobre un marco de los aspectos éticos de la inteligencia artificial, la robótica y las tecnologías conexas (2020/2012(INL)). Recuperado de https://bit.ly/3ukm0eW

Prensky, M. (2001). Digital Natives, Digital Immigrants Part 1, *On the Horizon*, *9*(5), 1-6. Recuperado de https://bit.ly/3J0MDJX

Shweta Barupal (2017). Digital Divide - A critical analysis. Recuperado de https://bit.ly/3ITSyjR

Unión Europea (2016). Reglamento 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). Recuperado de https://bit.ly/3B55hxD

We are social (2021). Global digital overview, reporte de México 2021. Recuperado de https://bit.ly/3scGMu2

Wolfie, Ch. (2017). Corporate Surveillance In Everyday Life: How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions, Institute for Critical Culture, Cracked Labs. Recuperado de https://bit.ly/3LeSZr9

Zappen, J.P. (2005). Digital rhetoric: Toward an integrated theory. En *Technical Communication Quarterly*, *14*(3), 319-325. Recuperado de https://bit.ly/3rmd6f6

Zuckerman, E. (2017). ¿Los gatos monos al rescate? Redes sociales y expresión política. En *Cuadernos de Información y Comunicación*, 22, 27-42. Recuperado de https://bit.ly/35I1j2d

CAPÍTULO 05

CIUDADANÍA DIGITAL EN MÉXICO: DERECHOS DE ACCESO, HABILIDADES Y PARTICIPACIÓN POLÍTICA

ITZKUAUHTLI ZAMORA SAENZ*

* Instituto Belisario Domínguez. Una versión previa a este capítulo se publicó como cuaderno de investigación de la Dirección General de Análisis Legislativo. Agradezco los valiosos comentarios de Israel Palazuelos Covarrubias para mejorar este trabajo.

El surgimiento y la extensión masiva del uso de las tecnologías de la información y la comunicación (TIC), a finales de la década de los noventa constituyó un hito en la historia de la humanidad, el cual fue conceptualizado de diferentes maneras: sociedad red, sociedad de la información y sociedad del conocimiento, entre las más reconocidas. En el año 2005 la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) se decantó por el término de sociedad de conocimiento, debido al vínculo que estableció entre el nuevo entorno digital y los retos que representa para el aprendizaje, el fortalecimiento de los derechos humanos y la necesaria relación con los problemas de sostenibilidad ambiental de la sociedad contemporánea (Mansell y Tremblay, 2015).

El entorno digital puede definirse como el ámbito de la realidad social que se caracteriza por la presencia de las TIC, las cuales constituyen la oportunidad de funcionar como herramientas que permiten generar y compartir conocimiento de una manera más rápida y con un alcance de audiencia más amplio. En la medida en que una persona está capacitada para participar de este nuevo entorno digital, se potencia su actividad en la sociedad del conocimiento.

Esta también ha sido el marco contextual más adecuado para analizar el tema de la ciudadanía digital, ya que colocó sobre el tapete de la discusión la importancia de generar mecanismos de inclusión para que la emergencia del nuevo entorno digital no incidiera en la ampliación de las desigualdades socieconómicas existentes; por el contrario, se espera que sea un catalizador para aminorarlas. Sin embargo, investigaciones en la materia han señalado que la tecnologización de la vida cotidiana ha favorecido a la población que ya ocupaba una posición privilegiada en el entramado social en términos de ingreso económico y nivel educativo, debido a que este sector es el que más fácilmente ha logrado adquirir los dispositivos y las habilidades digitales que se requieren para aprovechar las oportunidades laborales y educativas (por mencionar algunas esferas sociales) que representan las TIC (van Dijk, 2009).

La sociedad del conocimiento no se reduce a que las personas tengan acceso a las TIC; no obstante, este aspecto es fundamental para brindarles la oportunidad de incorporarse a redes de aprendizaje que les permitan mejorar sus competencias y capacidades, así

como su posición en el entramado social. Además de este acceso a las TIC, es importante que la persona tenga la capacidad de buscar, seleccionar y analizar información disponible en el entorno digital. Sin embargo, resulta muy evidente que estas capacidades no están igualmente distribuidas en la población por diferentes razones, entre las más frecuentes se encuentran las condiciones socioeconómicas, mismas que repercuten en la falta de oportunidades educativas y culturales para poder utilizar las herramientas digitales como Internet de manera autónoma, así como para producir contenidos comunicativos que circulen en dicha red (Castells, 2012: 307).

El presente capítulo aborda la cuestión de la ciudadanía digital en nuestro país. En el primer apartado se define este concepto y se propone un abordaje a partir de tres variables que se desarrollan en secciones específicas: la accesibilidad, las habilidades digitales y la participación en entornos digitales. Esta última se desarrolla como una competencia propiamente política que permite aproximarnos analíticamente a las nuevas formas de expresión que están aconteciendo en las redes sociodigitales.[1] La incorporación de dicha dimensión permite reiterar que el entorno digital no se reduce a un aspecto tecnológico, sino que tiene implicaciones relevantes como medio de comunicación que aspira a tener una organización más horizontal e interactiva, de manera que las personas tengan la posibilidad de expresar su opinión, solicitar información y establecer un vínculo con sus representantes políticos.

A partir de la revisión de estas variables queda de manifiesto el hecho de que la brecha digital persistente en nuestro país es multiforme. Si bien es muy importante no dejar de mencionar la relación que tiene este concepto con la falta de acceso a las TIC, también lo es vincularlo a la falta de habilidades digitales para aprovechar estas herramientas en la generación de conocimiento y la resolución de problemas. Igualmente, es fundamental no dejar de señalar que

1 Se opta por la expresión redes sociodigitales para referirse a las plataformas que permiten la comunicación en el entorno digital. Normalmente se les ha llamado redes sociales, pero este concepto de fuerte tradición sociológica tiene que ver con enfoques mesoestructurales para identificar la manera en que las personas de un grupo han establecido sus relaciones sociales, de manera que tiene alcances teóricos y empíricos más amplios que no se abordan en el presente estudio.

esas brechas tienen expresiones territoriales (particularmente en asentamientos rurales), socieconómicas y etarias.

En las conclusiones se enfatiza la necesidad de impulsar una política estatal que permita disminuir sensiblemente la brecha digital, no solamente con el acceso a las TIC, sino en articulación con el fortalecimiento de la currícula en la educación formal para que las personas puedan desarrollar adecuadamente las competencias generales de aprendizaje y generación de conocimiento para la resolución de problemas. En ese sentido, la construcción y expansión de la ciudadanía digital contribuye a ampliar los canales de participación en una democracia.

¿QUÉ ES LA CIUDADANÍA DIGITAL?

La ciudadanía ha constituido un concepto de mucha utilidad para identificar la posición que tiene un grupo social al interior de un Estado a partir de la obtención de un conjunto de derechos y obligaciones en el campo civil, político, social o cultural. Dicha posición no es fija, fluctúa de acuerdo con la participación colectiva de un sector social determinado que aspira a conseguir ciertos derechos o el mejoramiento de las condiciones necesarias para ejercerlos plenamente. En otras palabras, la ciudadanía no constituye un estatus fijo en una comunidad política; por el contrario, tiene un comportamiento dinámico de manera que se contrae o se dilata a partir del surgimiento de nuevos derechos y la presión que ejercen diferentes grupos para que el Estado implemente las políticas públicas necesarias que garanticen su pleno ejercicio en condiciones de igualdad (Isin y Wood, 1999). En ese sentido, es posible afirmar que la ciudadanía constituye un marco analítico para conocer avances o retrocesos en la inclusión social en una comunidad política determinada para que todas las personas puedan ejercer un conjunto de derechos y obligaciones que se consideran universalizables.

Los derechos y obligaciones a los que alude el concepto de ciudadanía tienen un desarrollo histórico. De esta manera, a la tipología clásica de derechos civiles, políticos y sociales, acuñada por Thomas H. Marshall (1992), se han agregado otro tipo de derechos que las sociedades contemporáneas han reconocido como importantes para adaptarse a las nuevas exigencias del entorno.

Precisamente, el concepto de ciudadanía digital trata de responder a esta transformación de la realidad social a raíz del surgimiento y la globalización de las tecnologías de la información (TIC) como el Internet, las computadoras y los teléfonos inteligentes (smartphones), por mencionar algunos ejemplos.

La ciudadanía digital se puede definir como un conjunto de derechos y obligaciones que permiten la participación libre y responsable en una sociedad en línea, esto es, en una caracterizada por la mediación de las TIC. En este sentido, se propone abordar la ciudadanía digital como un concepto multidimensional en el cual se identifican al menos tres ejes analíticos: la accesibilidad, las habilidades y la participación política. La tríada se encuentra interrelacionada jerárquicamente, de manera que, si no hay acceso, se truncan los avances en el desarrollo de habilidades y sin estas dos (acceso y habilidades), se dificulta la posibilidad de participar políticamente en el entorno digital. De este modo, no basta tener acceso regular a Internet; también se requiere haber desarrollado habilidades para aprovecharlo en aras de la construcción de capacidades personales en los ámbitos educativo, laboral, político y cultural, por mencionar algunos (Mossberger, 2009). Dicho con otras palabras, el acceso a las TIC amplía las oportunidades que una persona tiene en diferentes ámbitos de su vida cotidiana: puede conseguir información de calidad que sea de utilidad para su desarrollo laboral, puede convertirse en una opción para ejercer su derecho a la educación (modalidad a distancia) y para disfrutar de una oferta cultural vinculada a la lectura (libros digitales) o el entretenimiento.

En suma, este nuevo entorno ha modificado la manera de establecer vínculos sociales por la intermediación de la tecnología. Hay una creciente literatura que busca analizar dichos cambios (Christakis y Fowler, 2010; Fernández Vicente, 2019); no obstante, este documento se limitará a ciertos alcances que puede tener en la esfera política a partir del crecimiento de la participación en las redes sociodigitales.[2] Tampoco se abordan otras dimensiones emergentes de la ciudadanía digital mucho más relacionadas con la cultura y la identidad.

2 Esta delimitación a la esfera de la participación política obedece a la importancia que representa para una institución legislativa como el Senado de la República.

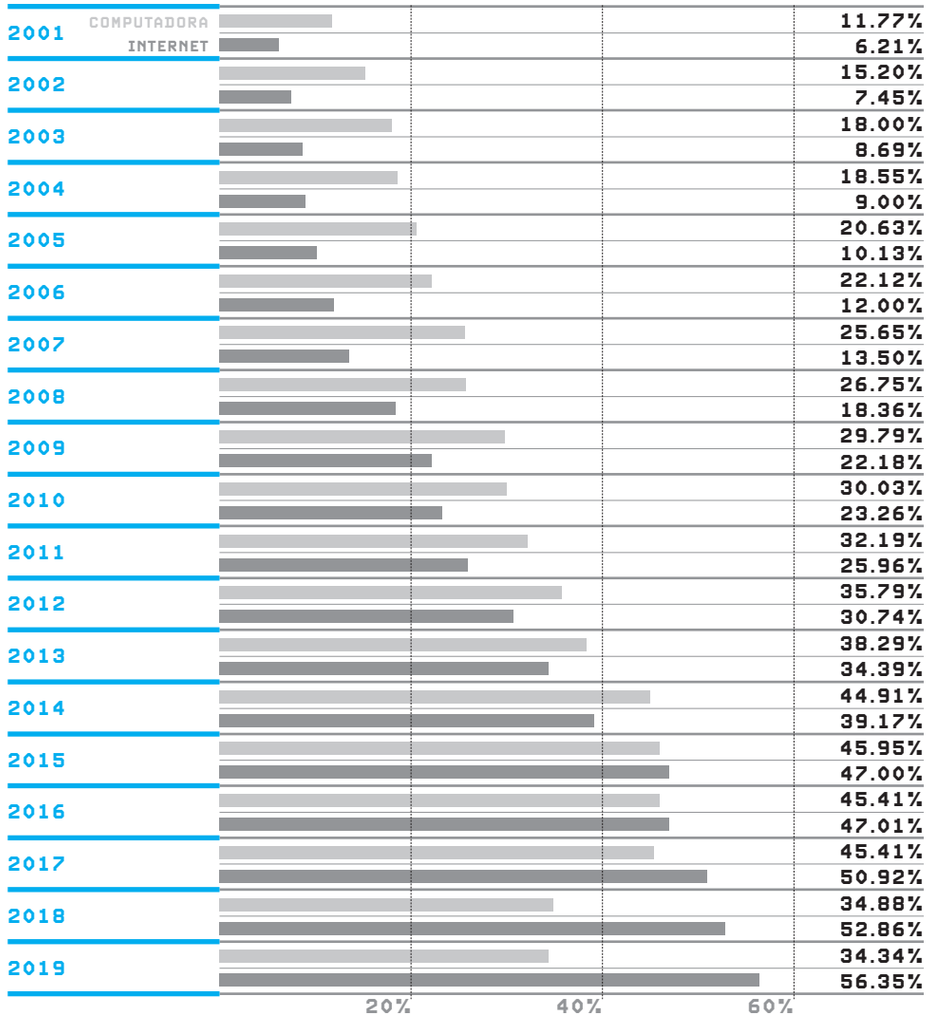
Precisamente, la emergencia de más y nuevas dimensiones es indicador del dinamismo y la constante transformación del entorno digital, aspectos que forman parte de sus características distintivas. Nótese la regularidad con la que surgen dispositivos con nuevas y más funcionalidades, la exigencia de actualización permanente para hacer posible la compatibilidad interna del ecosistema digital del cual se ha provisto una persona, así como la innovación y creación de nuevas plataformas que permiten nuevas formas de expresión, por mencionar algunas. El dinamismo y la transformación constante del entorno tienen una incidencia directa en la ciudadanía digital, ya que las habilidades adquiridas en el presente pueden resultar insuficientes u obsoletas en el futuro inmediato. Este hecho constituye una amenaza para la propia construcción de la ciudadanía digital, ya que acelera el establecimiento de posibles brechas generacionales en cuanto al uso y conocimiento de las TIC. Por lo tanto, conforme avanza la expansión del entorno digital, aumenta la urgencia de que el Estado implemente políticas públicas que permitan la inclusión de los diferentes grupos sociales en el pleno reconocimiento y ejercicio tanto de los derechos como de las obligaciones que representa la ciudadanía digital. De lo contrario, la ampliación de la desigualdad entre aquellos que forman parte de la sociedad del conocimiento y los que se quedaron a la zaga, es más difícil de revertir.

EL EJE DE ACCESIBILIDAD

El indicador más utilizado para analizar el grado de inclusión en la ciudadanía digital es el acceso a las TIC, particularmente a computadoras y a Internet. Medir la ciudadanía digital únicamente por la accesibilidad es una visión limitada, pero cualquier aproximación multidimensional la tiene como punto de partida, ya que constituye el elemento *sine qua non* para desarrollar habilidades y capacidades digitales. En ese sentido, garantizar el acceso a las TIC es básico para el ejercicio de la ciudadanía digital.

La exclusión en el acceso a las TIC establece la brecha digital al interior de un Estado, es decir, un sector de la población está marginado de estas tecnologías por su condición socioeconómica, su ubicación territorial o incluso por su edad. El concepto de brecha

GRÁFICA 01. PORCENTAJE DE HOGARES EQUIPADOS CON COMPUTADORA E INTERNET, 2001-2019



FUENTE:

elaboración propia con base en ENDUTIH, 2019.[3]

[3] El propio Instituto Nacional de Estadística y Geografía (Inegi) hace una advertencia sobre la comparabilidad de estas cifras. Al respecto, señala que de 2001 a 2014 el levantamiento que hacía el Módulo sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (MODUTIH) cuestionaba a un informante que respondía sobre el uso de las TIC que hacían todos los miembros del hogar. A partir del año 2015, en coincidencia con el surgimiento de la ENDUTIH, se modificó la metodología para seleccionar un informante de manera aleatoria, que responde únicamente al uso que él mismo hace de las tecnologías. En ese sentido, no es del todo preciso comparar las cifras de estos dos bloques de tiempo (2001-2014 y 2015-2019); sin embargo, se muestran en esta gráfica con el objetivo de tener una idea aproximada de la evolución de este indicador.

digital es fundamental para incluir el tema de la desigualdad en la sociedad del conocimiento, ya que revela cómo un sector de la población no tiene la posibilidad de ejercer este derecho.

El indicador más frecuente para medir la brecha digital ha sido la cantidad de hogares que tienen una computadora conectada a Internet, aunque hay otras propuestas que han planteado que la unidad de medida sea la persona con acceso a un dispositivo electrónico conectado a Internet, o bien la posibilidad de conectarse en otros espacios como escuelas y bibliotecas, por mencionar algunos. Para nuestros fines expositivos se utilizará el porcentaje de hogares con conexión a Internet. Como se puede apreciar en la gráfica 1, en los últimos 18 años se aprecia un crecimiento sostenido en el porcentaje de hogares que tienen conexión a Internet en nuestro país, ya sea mediante una conexión fija o móvil. De esta manera, del 6.2% que se tenía en 2001, se incrementaron 50.2 puntos porcentuales para alcanzar el valor de 56.4% en la medición de 2019. En la misma gráfica sobresale que, contrario a la tendencia en la conexión a Internet, en los últimos tres años se aprecia una ligera disminución de los hogares equipados con computadora.

La disminución de las computadoras está sumamente relacionada con la diversificación de los dispositivos electrónicos con los cuales la población se puede conectar a Internet. La expansión de teléfonos móviles inteligentes ha sido particularmente relevante, al grado de constituir el principal equipo para conectarse a la red. Al respecto, 95.3% de la población usuaria de Internet declaró que el smartphone es el principal equipo con el que se conecta; en segundo lugar, se encuentran las personas que lo hacen mediante una computadora portátil (33.2%) y en tercero, quien lo realiza mediante una computadora de escritorio (28.9%). El resto de los dispositivos tiene una frecuencia más baja: la televisión inteligente (*smart TV*) o algún dispositivo conectado a ella concentraron 23.4% de las respuestas, la tableta (*tablet*) el 17.8% y la consola de videojuegos 8.4% (ENDUTIH, 2019). De esta manera, seis de cada 10 personas en México afirman conectarse a Internet principalmente mediante la computadora de escritorio o portátil (62.1%). Sin embargo, la propia ENDUTIH señala que solamente 43% de la población de seis años o más es usuaria de computadora, lo que representa

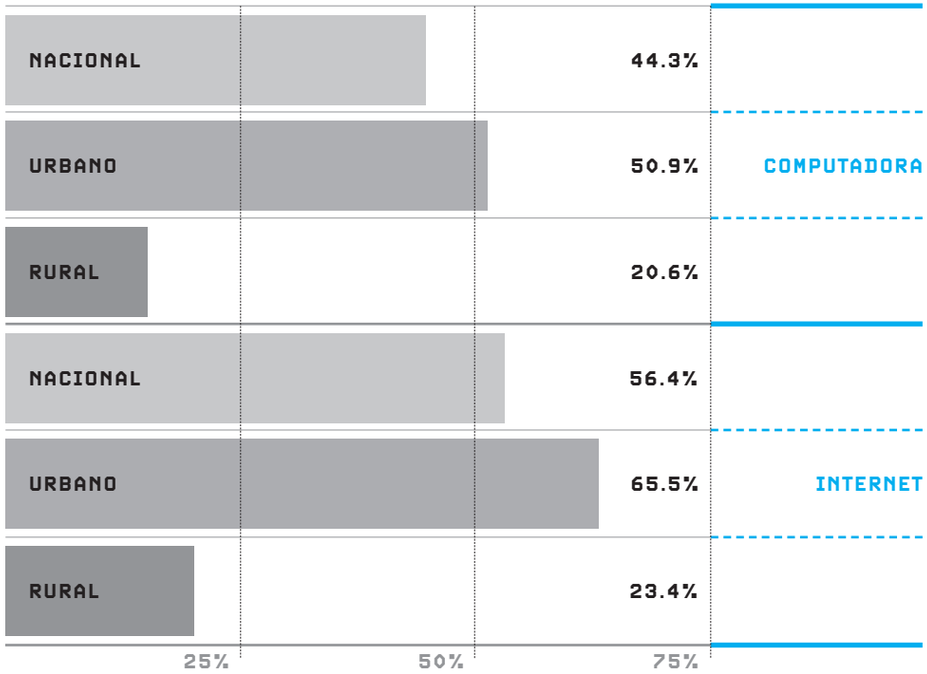
una disminución de 8.3 puntos porcentuales con respecto al valor que tenía el indicador en el año 2015. Esta falta de correspondencia entre los porcentajes requería de mayor precisión para saber por qué hay una mayor cantidad de población que afirma conectarse por computadora de escritorio o laptop con respecto a la que es usuaria de este tipo de dispositivos. Se podría conjeturar que, si bien se utiliza la computadora para conectarse a Internet, se reconoce el desconocimiento de otro tipo de habilidades para utilizarla de manera más amplia.

La accesibilidad de Internet en el hogar es una condición deseable para el desarrollo de la ciudadanía digital, ya que favorece la posibilidad de obtener información que pueda ser de utilidad para fortalecer las competencias cívicas, laborales y educativas. Ahora bien, aunque se apreció este crecimiento permanente en el porcentaje de hogares conectados a Internet en la gráfica anterior, hay tres tipos de brechas que es importante subrayar. La primera de ellas radica en los hogares ubicados en los asentamientos rurales. En la gráfica 2 se muestra que solamente dos de cada 10 hogares rurales tienen computadora de escritorio e Internet en casa (20.6% y 23.4%, respectivamente). La cifra está considerablemente lejos de los valores que se tienen para los hogares urbanos, los cuales también resultan superiores al promedio nacional.[4]

[4] Si se tiene como unidad de análisis a la población de seis años o más, también es notoria la brecha digital en cuanto al uso de Internet. Al respecto, 76.6% de la población urbana afirmó ser usuaria de Internet, mientras que solamente 47.7% de la población rural respondió en ese sentido (ENDUTIH, 2019). De esta manera, si bien es cierto que la población rural aumenta en proporción con respecto a los hogares en cuanto uso de Internet por la posibilidad de hacerlo en espacios laborales, educativos, privados (café Internet) o por datos móviles del smartphone, el porcentaje es inferior a la mitad de la población total en condición de ruralidad y sigue siendo un valor lejano al obtenido para el espacio urbano.

GRÁFICA 02.

INTERNET EN PORCENTAJE DE HOGARES CON COMPUTADORA O INTERNET, SEGÚN EL ÁMBITO TERRITORIAL (URBANO-RURAL): PORCENTAJE DE HOGARES CONECTADOS Y DIFERENCIAS EN FRECUENCIA DE USO EN GRUPOS DE EDAD, 2018



FUENTE:
elaboración propia con base en ENDUTIH, 2019.

El segundo tipo de brecha es la socioeconómica. Numerosos estudios en el nivel internacional han acumulado evidencia para afirmar que la condición socioeconómica es un factor relevante para el acceso a las TIC, de manera que vivir en situación de pobreza disminuye significativamente esta accesibilidad (Mossberger, 2009). Aunque la brecha digital en términos socioeconómicos está relacionada con la condición de ruralidad, no se pueden fusionar, ya que esto implicaría invisibilizar la pobreza urbana como un factor importante de exclusión en la ciudadanía digital. La ENDUTIH revela que, al ocupar un estrato socioeconómico más bajo, disminuye notoriamente la cantidad de personas usuarias de Internet, de una computadora y de teléfono celular (véase cuadro 01). La mayor brecha digital se encuentra entre los usuarios de computadora y los de Internet, justo las TIC en las que se ha enfocado esta investigación. En el primer caso, solamente 20.1% de las personas que se encuentran en el estrato socioeconómico "bajo" son usuarias de computadora, a diferencia del 76.6% de las personas que se encuentran en el estrato económico "alto" (diferencia de 56.5 puntos porcentuales). En segundo lugar, mientras que 45% de las personas que se encuentran en el estrato socioeconómico "bajo" son usuarias de Internet, lo son 92% de las personas del estrato socioeconómico "alto" (diferencia de 47 puntos porcentuales).

Dentro de las principales razones que señala la población que se encuentra en el estrato socioeconómico "bajo" para no tener conexión a Internet en el hogar se encuentran la falta de recursos económicos (60.2% de quienes carecen de dicha conexión), la falta del servicio en la localidad (26.1%) y la falta de interés o por no considerarlo necesario (10.1%). El orden de estas razones cambia para el estrato socioeconómico "alto", de manera que la principal razón para este grupo es la falta de interés o por no considerarlo necesario (35.2% de las respuestas), seguido de la falta de recursos económicos (34.8%) y la falta de servicios en la localidad (3.9%). Es muy probable que las personas que se encuentran en un estrato socioeconómico "bajo" y señalan la falta de servicio en la localidad como la principal razón para carecer de servicio de Internet, radiquen en asentamientos rurales, ya que la cobertura en zonas rurales en nuestro país es muy precaria.

CUADRO 01. USUARIOS DE TECNOLOGÍAS DE LA INFORMACIÓN POR ESTRATO SOCIOECONÓMICO, 2019

Estrato socioeconómico	Usuarios de computadora	Usuarios de Internet	Usuarios de teléfono celular
Nacional	43.0	70.1	75.1
Bajo	20.1	45.0	55.2
Medio bajo	40.4	71.8	77.1
Medio alto	58.1	83.3	85.1
Alto	76.6	92.0	90.9

FUENTE:
elaboración propia con base en ENDUTIH, 2019.[5]

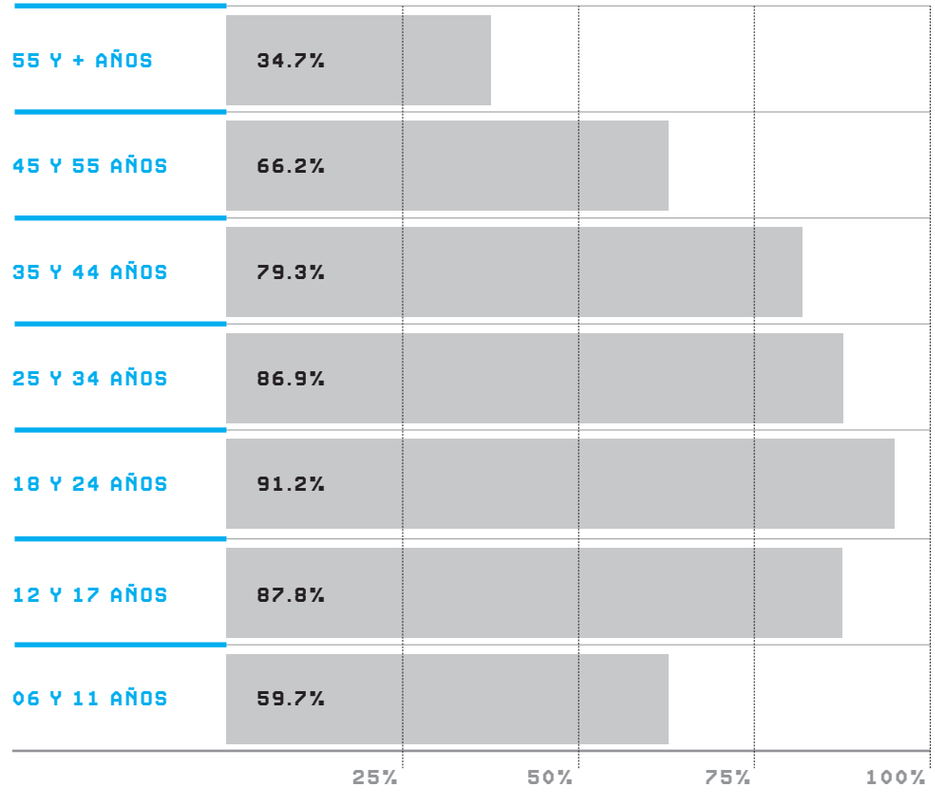
5 Esta estratificación realizada por el Inegi está construida a partir de 34 indicadores que recuperan información de las características socioeconómicas de los habitantes de las viviendas, así como información referente a las características y el equipamiento de estas.

Lara Caballero (2014) señaló en una investigación que la brecha digital por razón socieconómica es interseccional con la de género. En dicho estudio concluyó que los hogares cuya jefatura es una mujer, tenían un acceso menor en comparación con los que contaban con un hombre. La hipótesis detrás de esta brecha de género es que las mujeres suelen tener niveles educativos e ingresos más bajos, lo que influye en una menor accesibilidad a las TIC en este tipo de hogares monoparentales. La principal fuente de información que se utilizó fueron los resultados del Módulo de Condiciones Socioeconómicas de la Encuesta Nacional de Ingresos y Gastos de los Hogares del año 2010, de manera que se requiere un trabajo que utilice información más reciente para saber si se mantiene este comportamiento o de qué manera ha variado.

En el apartado anterior se señaló que la ciudadanía digital ha tenido su principal desarrollo en el presente siglo. Además, se caracteriza por un entorno que se transforma rápidamente. No hay resultados concluyentes para aseverar que los "nativos digitales" (aquella población que nació con este tipo de entorno) tenga mayores habilidades digitales en comparación a las generaciones previas al surgimiento y la expansión masiva de las TIC, denominados "migrantes digitales" (van Deursen y van Dijk, 2010). Sin embargo, en el caso mexicano se destaca que la población adulta mayor tiene menos accesibilidad a Internet. En ese sentido, la tercera brecha digital por señalar es la etaria, ya que el acceso y la construcción de habilidades digitales (saber-hacer con las TIC) tienen niveles muy bajos en la población mayor. En la gráfica 3 se destaca que solamente 34.7% de la población de 55 años y más en nuestro país es usuaria de Internet. Esta cifra es inferior a la de la población de menor edad incluida en el levantamiento de la ENDUTIH, como es la de 6 a 11 años, ya que 59.7% de este sector es usuario de Internet.

Otro indicador que señala una brecha digital de tipo etario, aunque más en clave de habilidades digitales se encuentra en la encuesta del Instituto Federal de Telecomunicaciones (IFT). En ella se pregunta el principal motivo por el cual una persona no tiene teléfono móvil con acceso a Internet o redes sociales. La principal respuesta que dio la población de 50 y más años fue que no sabe utilizar Internet (32.4%).[6] Ningún otro grupo etario tiene esta respuesta como principal motivo (IFT 2019).

GRÁFICA 03. PORCENTAJE DE POBLACIÓN USUARIA DE INTERNET POR GRUPOS DE EDAD, 2019



FUENTE:
elaboración propia con base en ENDUTIH, 2019.

Se ha argumentado la posibilidad de que el principal problema para la población adulta mayor en cuanto al indicador de accesibilidad no se restrinja al aspecto físico, sino que incida un aspecto de carácter psicológico denominado "acceso motivacional", por el cual se prefiere estar desconectado debido a la ansiedad que pueda representar la dificultad para familiarizarse y utilizar el entorno digital o incluso la desconfianza hacia los desarrollos tecnológicos (van Dijk, 2009).

6 El resto de las respuestas ofrecidas por este grupo etario sobre el principal motivo para no tener un teléfono móvil con acceso Internet fueron: 27.6% señaló que no le interesa adquirir uno / no lo necesita; 16.8% que su equipo es obsoleto; 9.9% que el precio del equipo es elevado; 2.9% indicó que no hay Internet en donde vive / no hay Internet; 0.5% no ha tenido tiempo de ver equipos; y 2.4% no sabe / no contestó.

EL EJE DE LAS HABILIDADES DTIGITALES

La exclusión en la conformación de una ciudadanía digital no se puede medir únicamente en términos de la accesibilidad física a las TIC, ya que ese eje no permite observar otras desigualdades relacionadas con la brecha digital. Hay matices importantes que trascienden la accesibilidad y para abordarlos es preciso identificar el desarrollo de habilidades digitales, es decir, el *saber-hacer* con las TIC. Sobre ello se han propuesto varios modelos que resultan muy interesantes (Eshet-Alkalai y Amichai-Hamburger, 2004), pero para tener una estimación estadística en el nivel nacional hace falta generar más información base. Para los fines de este capítulo se utilizarán tres tipos de habilidades sobre las cuales hay datos asequibles en el nivel nacional: el uso de Internet, la distinción de riesgos de Internet y las habilidades computacionales.

El uso de Internet implica un conocimiento y el manejo de aplicaciones, así como de los propios dispositivos electrónicos. En la sección anterior se identificó que la principal conectividad de Internet se lleva a cabo fundamentalmente con el smartphone. Este cambio de dispositivo prioritario está relacionado con los principales usos que tiene la red. En ese sentido, los usos predilectos que hace la población con acceso a Internet son el entretenimiento (91.5% de la población usuaria), la obtención de información (90.7%), la comunicación (90.6%), el acceso a las redes sociales (87.8%), como apoyo a la educación o la capacitación laboral (83.8%) y para acceder a contenidos audiovisuales (80.5%) (ENDUTIH, 2019).[7] La encuesta realizada por el IFT permite apreciar con mayor detalle cómo se modifica el uso de Internet a partir del dispositivo empleado. Esta información se muestra en el cuadro 02.

Como se puede apreciar en este, las principales actividades que se realizan con el teléfono móvil están relacionadas con aspectos de comunicación (enviar mensajes instantáneos y hacer llamadas o videollamadas) y de entretenimiento (redes sociales).

7 Esta estratificación realizada por el Inegi está construida a partir de 34 indicadores que recuperan información de las características socioeconómicas de los habitantes de las viviendas, así como información referente a las características y el equipamiento de estas.

CUADRO 02. PRINCIPALES ACTIVIDADES REALIZADAS MEDIANTE INTERNET FIJO DE ACUERDO CON EL EQUIPO UTILIZADO

Dispositivo	Primera actividad	Segunda actividad	Tercera actividad
Teléfono móvil (smartphone)	Enviar mensajes instantáneos (WhatsApp, Skype, etcétera.): 96.1%	Hacer llamadas o videollamadas (Skype, WhatsApp, Facetime): 92.3%	Redes sociales: 80.5%
Laptop	Uso de e-mail o correo electrónico: 21.0%	Compras por Internet: 18.6%	Transacciones bancarias: 12.5%
Computadora de escritorio	Uso de e-mail o correo electrónico: 19.60%	Transacciones bancarias:14.9%	Compras por Internet: 14.9%
Tableta	Ver noticias: 6.6%	Entretenimiento (ver películas, series, deportes): 6.4%	Ver videos cortos (YouTube): 6.2%
Smart Tv	Entretenimiento (ver películas, series, deportes): 39.1%	Ver noticias: 25.0%	Ver videos cortos (YouTube): 9.3%
Consola de videojuegos	Jugar (juegos de video de Internet): 12.0%	Entretenimiento (ver películas, series, deportes): 1.1%	Ver noticias: 0.8%

FUENTE: elaboración propia con base en IFT, 2019.

Tanto en la computadora portátil como en la de escritorio se realizan principalmente actividades de comunicación asincrónica (uso de *e-mail*), así como actividades financieras (compras por Internet y transacciones bancarias). La principal actividad en la tableta consiste en revisar noticias y después actividades vinculadas con el entretenimiento (ver películas, series o deportes y ver videos cortos). En cuanto a la denominada televisión inteligente (*smart TV*)

destaca como principal actividad el entretenimiento (ver películas, series, deportes), seguido de aspectos informativos (ver noticias) y ver videos cortos en Youtube. Finalmente, la actividad preponderante en la consola de videojuegos es la actividad lúdica (juegos de video de Internet).

Navegar por Internet implica una serie de riesgos ligados a la vulneración de nuestra privacidad y al mal uso de datos personales por parte de terceros. Al respecto, las personas usuarias de la red requieren ciertas habilidades para bajar información y acceder a sitios confiables, con la finalidad de realizar cualquier actividad bajo una mayor certidumbre de seguridad, legalidad y ética. La ENDUTIH 2019 ofrece información sobre los principales problemas que las personas usuarias de Internet han tenido al navegar por la red. Es importante señalar que esta información no está planteada en términos propiamente de habilidades digitales para distinguir riesgos, sino justo en los problemas que se han tenido, aunque podría afirmarse que, en la medida en que un problema se reconoce, ya implica un cierto conocimiento sobre la habilidad para afrontarlo.

Los principales problemas identificados están relacionados con la prestación del servicio, como la lentitud en la transferencia de la información, las interrupciones de la señal o el exceso de información no deseada en los sitios web. Los problemas más frecuentes en términos de riesgos al mal uso de datos personales o de fraude cibernéticos que señalaron las personas en los tres meses previos al momento de ser encuestadas fueron la recepción de mensajes de personas desconocidas (20.3% de las personas usuarias de Internet), la infección de los equipos por algún virus informático (13.1%), haber sido víctimas de fraudes con información financiera o personal (4%) y la violación a la privacidad (3.1%). Es importante advertir que la encuesta no permite precisar a qué se refiere la población cuando menciona que un tercero violó su privacidad, pero se puede inferir que en este rubro se incluyen prácticas como el *bullying*, el *sexting* y otras formas en las que se expone imágenes e información personal sin consentimiento de la persona afectada.

El tercer indicador de las habilidades digitales es el referente a las destrezas computacionales, las cuales se definen como aquellas

CUADRO 03. ANÁLISIS DE CONTINGENCIA EN DONDE SE DESTACA QUE LOS ESTRATOS SOCIOECONÓMICOS SON LOS QUE TIENEN MENOS HABILIDADES COMPUTACIONALES

	ESTRATO SOCIOECONÓMICO			
Habilidad computacional	**Bajo**	**Medio bajo**	**Medio alto**	**Alto**
Enviar y recibir correo electrónico	12.4%	30.3%	26.4%	30.9%
Descargar contenidos de Internet (música, videos, documentos, etcétera)	14.4%	31.6%	25.1%	28.9%
Copiar archivos entre directorios (carpetas)	13.2%	30.7%	25.7%	30.3%
Crear archivos de texto	14.0%	30.8%	25.5%	29.7%
Crear hojas de cálculo	11.8%	29.1%	26.7%	32.4%
Crear presentaciones	13.1%	30.3%	25.7%	30.8%
Instalar dispositivos periféricos (impresora, proyector, etcétera)	11.1%	28.1%	27.2%	33.6%
Crear o usar base de datos	11.5%	27.8%	26.9%	33.9%
Programar en lenguaje especializado	12.8%	29.1%	28.5%	29.7%

FUENTE:
elaboración propia con base en ENDUTIH, 2019.

capacidades operacionales que permiten realizar actividades básicas con hardware y software de equipos de cómputo. En muchas ocasiones se utiliza como base aquellas habilidades que permiten trabajar con programas de la paquetería Office, ya que son las más utilizadas en actividades laborales y educativas. La transformación constante del ambiente digital requiere de un proceso de actualización continua de este tipo de habilidades, así como del desarrollo de nuevas por el surgimiento de innovaciones digitales.

Los resultados de la ENDUTIH 2019 indican que 39.48% de la población encuestada actualmente es usuaria de computadora (escritorio o portátil) o de tablet. Las principales habilidades computacionales de esta población consisten en saber descargar contenidos de Internet como música, videos y documentos (86.8%), crear archivos de texto (82.6%), enviar y recibir correo electrónico (79.0%) y copiar archivos entre directorios (76.9%). Sólo hay dos habilidades que se encuentran en menos de la mitad de la población usuaria de computadoras o tablets, las cuales exigen cierto conocimiento matemático de base. De esta manera, solamente 45.7% señaló crear o usar base de datos y 17.5% programar en lenguaje especializado.[8]

EL EJE DE LA PARTICIPACIÓN POLÍTICA

Los medios electrónicos han permitido un nuevo tipo de involucramiento político en la sociedad del conocimiento. La posibilidad de obtener información en Internet y la existencia de plataformas que permiten realizar trámites gubernamentales, así como formar parte de una conversación generalizada sobre temas de actualidad, han creado nuevas formas de participación para la ciudadanía digital. Las plataformas y herramientas digitales se caracterizan porque permiten expresar la voz de manera inmediata, descentralizada, interactiva y en libertad en comparación a los medios de comunicación tradicionales como la radio o la televisión (Natal, Benítez y Ortiz, 2014).

El eje de la participación política podría considerarse como una habilidad digital de tipo estratégico, ya que, con su ejercicio, se desea alcanzar un fin determinado en la esfera pública, como puede ser realizar algún trámite o algún tipo de activismo en las redes sociodigitales para plantear problemas, así como alternativas de solución. Es importante subrayar que la participación digital no se reduce a consultar información en la red, como a expresar y realizar acciones en el campo político. Para ello, es necesario reconocer que el ejercicio libre de esta forma de participación requiere de un contexto político favorable para la libertad de expresión y que la democracia de un país esté abierta a mejorar la interacción entre la ciudadanía y las autoridades de gobierno mediante las herramientas existentes y emergentes del entorno digital.

Hay una polémica abierta sobre el papel que tienen las redes sociodigitales en la sociedad contemporánea, la cual abarca una gama amplia de interpretaciones que van desde considerarlas el nuevo ágora en el que se debaten los asuntos públicos más relevantes, una nueva herramienta para aproximarse a ciertos sectores de la población o un espacio en el que prolifera la banalidad e interacciones basadas en la violencia verbal y la descalificación.[9]

La UNESCO valora positivamente el papel que pueden tener las redes sociodigitales en la sociedad del conocimiento. Se ha mencionado que son fundamentales para compartir información que permite generar y aplicar conocimiento (Mansell y Tremblay, 2015) y que facilitan la articulación de una comunidad de intereses dispersa geográficamente (Natal, Ortega y Martínez, 2014). Por esta razón, se ha convertido en un elemento más del repertorio de acción colectiva en la dimensión política. Es verdad que no siempre circula información veraz, útil y relevante en términos de una sociedad de conocimiento, para eso también será importante que la persona pueda tener la capacidad para filtrar, verificar y emitir comunicaciones de manera responsable. En las redes abunda información, de manera que se requiere cierta educación digital para utilizarla de manera efectiva en la construcción de conocimiento.

Cabe señalar que las redes sociodigitales implican un sesgo importante con respecto a la población que las usa. En primer lugar, se encuentra la existencia de la brecha digital en los tres

8 El resto de las habilidades computacionales fueron: crear presentaciones (70.6%), crear hojas de cálculo (63.8%) e instalar dispositivos periféricos como impresoras o proyectores a la computadora (56.0%).

9 Sobre esta última posibilidad resulta muy ilustrativo el proyecto que Microsoft realizó en el año 2016, el cual se trataba de un programa informático que denominó "Tay" para que interactuara automáticamente con personas usuarias de Twitter a partir del reconocimiento del tipo de mensajes predominantes de la red y de sus interlocutores. En menos de 24 horas de haber dado de alta al perfil artificial del bot, "Tay" comenzó a emitir mensajes racistas, xenófobos y sexistas, de manera que la compañía decidió cerrar la cuenta.

rubros señalados anteriormente: estrato socioeconómico, tipo de asentamiento y edad. El reconocimiento de esta brecha permite identificar el sesgo que tiene este tipo de participación, ya que hay una mayor representación de personas jóvenes, residentes de ciudades y de niveles socioeconómicos medios y altos. En principio, este sería el sector que normalmente se expresa en las redes sociodigitales y que desde ahí busca incidir en la conformación de una opinión pública. Por lo tanto, la discusión política en redes, aunque copiosa, no es representativa de la heterogenidad social de nuestro país. Además, hay que señalar que en este ambiente digital existen formas distorsionadas para crear temas de discusión a partir de la creación y la administración de cuentas con perfiles falsos, cuyo único objetivo es aumentar la resonancia a favor o en contra de un determinado problema o persona. Esta falta de confiabilidad en la información que circula en las redes sociodigitales se ha constituido en uno de los problemas principales de la expresión política de la ciudadanía digital: el hecho de que proliferen cuentas con perfiles apócrifos con el único objetivo de generar tendencias políticas en esa esfera de discusión crea un nuevo sesgo sobre esta forma de participación.

Derivada de estas distorsiones que ha tenido la participación política en redes sociodigitales se ha remarcado la importancia de las habilidades digitales, ya que es deseable que las personas tengan capacidades para distinguir cuentas y noticias falsas (*bots* y *Fake News*, respectivamente), a partir de ciertas condiciones que permitan evaluar la confiabilidad de la fuente emisora de cualquier mensaje para evitar la propagación de aquella que resulta dudosa.[10] La ciudadanía digital requiere de habilidades específicas para distinguir información veraz y de calidad para evitar sumarse a la circulación de la que no cuenta con estas características. A su vez, resulta fundamental mejorar la calidad de la participación política en el medio virtual a partir de fortalecer una educación cívica democrática que favorezca una interacción basada en argumentos, la tolerancia y la búsqueda de consensos.

A pesar de estos giros inesperados de la participación y la discusión política en las redes (*Fake News*, el discurso de odio, etcétera) es fundamental reconocer que se ha constituido en una herramienta más del repertorio de acción colectiva que tiene mucha repercusión para plantear ciertas demandas de carácter político como puede ser la vulneración de derechos o la falla en la prestación de servicios públicos, por mencionar algunos. Sobresalen los casos emblemáticos de los movimientos políticos por una mayor apertura democrática en el Medio Oriente (conocida como "Primavera árabe") y de las acciones de colectivos feministas que transfieren sus reclamos en las redes sociodigitales a expresiones en el espacio público derivadas de una síntesis de reclamos políticos en clave de hashtags como #MiPrimerAcoso, #Metoo y #Niunamás, por mencionar algunos. Sin lugar a duda, la dimensión política ha sido uno de los aspectos más explorados en la investigación reciente sobre ciudadanía digital, gracias a la potencialidad que tienen las redes sociodigitales como un nuevo espacio de expresión en el que se puede denunciar, opinar, mostrar simpatías por ciertos hechos políticos y hacer un llamado a una movilización colectiva (Tilly y Wood, 2010; Natal, Benítez y Ortiz, 2014).

Para aproximarnos al estudio de esta dimensión, se utilizará como indicador el uso de las redes sociodigitales en México. En el apartado anterior se identificó que su uso constituye la tercera actividad más frecuente de la población mediante el uso de su teléfono móvil y que tiene Internet fijo. En el cuadro 04 se aprecia que la red sociodigital con mayor penetración en la población mexicana es Facebook (94.9% de las personas usuarias de redes), seguido de Messenger (79.7%) e Instagram (39.9%). La red sociodigital de Twitter, que suele asociarse más con una conversación de carácter político, ocupa la cuarta posición con 21.4% de los usuarios de redes. Salvo el caso de Facebook, que es más utilizado en el grupo etario de 25 a 34 años, destaca que el grupo etario de los jóvenes (18 a 24 años) es el principal usuario del resto de las redes.

10 Sin entrar a detalle, una noticia falsa o *Fake News* es aquella que tiene la intención deliberada de engañar y cuyo éxito se mide en función de la propagación que tiene en Internet, esto es, de su "viralización". A la propagación excesiva de noticias falsas en las redes digitales e Internet se le ha denominado infodemia.

CUADRO 04. REDES DIGITALES QUE SE NAVEGAN MÁS EN INTERNET FIJO, POR GRUPOS DE EDAD

18-24 años	25-34 años	35-49 años	50 años y más	Total	Redes Sociales
96.5%	97.4%	93.8%	90.3%	94.9%	**Facebook**
87.0%	83.8%	78.2%	63.9%	79.7%	**Messenger**
60.7%	38.2%	34.0%	22.9%	39.9%	**Instagram**
26.8%	23.4%	18.7%	14.8%	21.4%	**Twitter**
28.0%	17.1%	14.5%	4.6%	17.0%	**Snapchat**

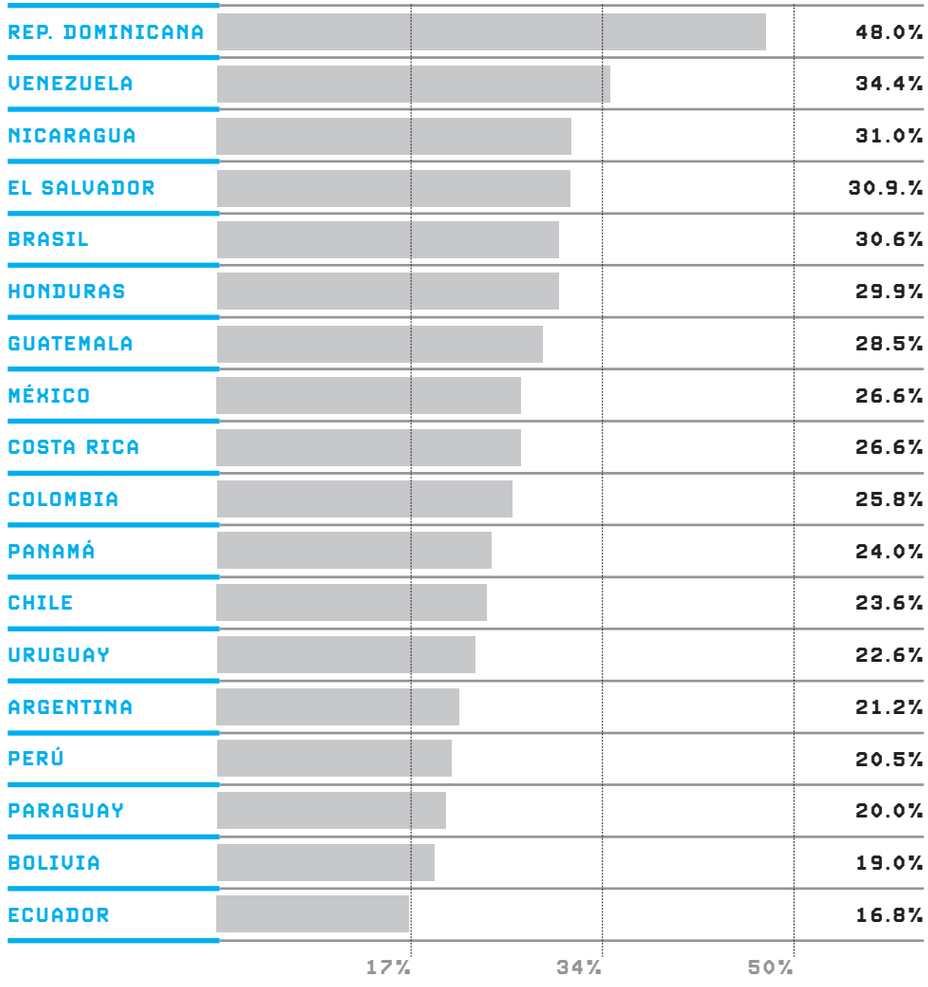
FUENTE: elaboración propia con base en ift (2019). No suma 100% porque la pregunta permite seleccionar respuestas múltiples.

En la misma encuesta del IFT se destaca que lo más compartido en redes sociodigitales mediante el teléfono móvil son videos (66.5%), memes o imágenes graciosas (62.6%), fotos que pueden ser autorretratos (*selfies*), de amigos o familiares (59%), artículos de noticias y deportes (50.9%) y fotos de comida y bebida (34.3%) (IFT, 2019).

Ahora bien, ¿qué tanto consideran las personas que las redes sociodigitales pueden tener una incidencia en temas políticos? Hasta el momento la única encuesta identificada que ofrece información sobre este indicador fue el Latinobarómetro en su levantamiento del año 2015. Los resultados para México fueron los siguientes: 26.6% respondió que las redes permiten la participación en política, 28.2% mencionó que solamente crean la ilusión de que uno está participando y 32.8% señalaron que las redes no sirven para participar en política.[11] Visto en perspectiva regional podemos ver que en nuestro país la creencia de que las redes sociodigitales permiten la participación en política ocupa una posición intermedia en los países de América Latina, alejado de los países punteros como son la República Dominicana (48%) y Venezuela (34.4%), pero también distante de los países que ocupan los últimos lugares como Ecuador (16.8%) y Bolivia (19%).

[11] El porcentaje se completa con 12% que no sabe y 0.4% que no respondió.

GRÁFICA 04. LAS REDES SOCIALES PERMITEN QUE UNO PARTICIPE EN POLÍTICA



FUENTE: elaboración propia con base en Latinobarómetro, 2015.

Como se puede apreciar en dicha gráfica, en general, la ciudadanía es muy cauta al evaluar la efectividad política de la participación en redes. A falta de mayores estudios que permitan profundizar estos resultados, se identifica un escepticismo sobre el ciberactivismo, considerándolo mayoritariamente como una ilusión o como algo de escasa utilidad. A manera de hipótesis, se podría adelantar que, si bien las redes sociodigitales han abierto una nueva forma

de participación y expresión de una opinión política, no necesariamente esto se ha visto reflejado en una mayor democratización de este tipo de comunicación. No todas las personas activas políticamente en las redes logran el mismo nivel de influencia y protagonismo en dichas plataformas y, además, quienes lo logran suelen ser las mismas que ya tienen una relevancia en las formas convencionales de participación. Ahora bien, ante dicha situación hay que recordar lo que se comentó anteriormente, referente al aumento en la cantidad de perfiles falsos, *Fake News* y en el grado de virulencia y descalificación que suelen adquirir las discusiones políticas en dicha red. Seguramente estas características en algo han influido en un cierto desencanto sobre el impacto político en plataformas digitales.

CONCLUSIONES

En este capítulo se abordó el tema de la ciudadanía digital desde tres dimensiones interrelacionadas: la accesibilidad, las habilidades digitales y la participación política. Desde luego, hay otras que también podrían haberse incluido, por ejemplo, la identidad digital. En los últimos años el gobierno mexicano ha venido extendiendo sus políticas públicas para garantizar el derecho humano a la identidad mediante el uso de las TIC. De esta manera, además de la Clave Única de Registro de Población (CURP), que desde muchos años se tramita por Internet, se ha planteado el proyecto de una cédula de identidad única mediante mecanismos de registro digitales. En caso de prosperar dicho proyecto, será necesario realizar la regulación y las leyes necesarias para salvaguardar la privacidad y buen uso de los datos personales. Esta es solamente una arista más de la ciudadanía digital. En la medida en que el entorno digital siga transformándose, seguramente habrá otras esferas novedosas que tendrán repercusiones en la manera en que se aborda y analiza este tipo de ciudadanía.

Podría considerarse que el resultado más relevante en las tres dimensiones analíticas seleccionadas está relacionado con el hecho de subrayar cómo las desventajas estructurales (educativas y económicas) tienen incidencia en la desigualdad tecnológica. La brecha digital en términos de accesibilidad y habilidades es tan marcada, que las personas que se encuentran en un estrato socioeconómico bajo y viven en asentamientos rurales, se están quedando rezagadas en la conformación de una sociedad del conocimiento. A este fenómeno hay que agregar la brecha digital por cuestiones etarias. Por razones que necesitan explorarse con mayor profunidad, las generaciones que nacieron mucho antes de la revolución digital han tenido dificultades para realizar esta transición. En ese sentido, no es casualidad que en las encuestas los grupos de adultos mayores sean quienes tengan menores habilidades digitales para utilizar las TIC. En cambio, las y los jóvenes son quienes utilizan de manera frecuente una gran cantidad de dispositivos digitales en su vida cotidiana, incluso muestran una mayor apertura a participar políticamente en las redes sociodigitales. La brecha digital se ha constituido en un nuevo mecanismo de exclusión en varios campos: económico, cultural, educativo, político, etc. Por eso es importante tener políticas que regulen y permitan resolver esta desigualdad. Dicho con otras palabras, el Estado tiene un papel fundamental para disminuir las brechas digitales existentes. Esta responsabilidad no solamente radica en su papel de entidad reguladora, sino también como impulsor de políticas públicas que garanticen el acceso a las TIC.

El cambio permanente del entorno digital constituye una amenaza constante en términos de ampliar la brecha digital. A lo largo del documento se indicó que una de las características de las TIC es su permanente transformación. Por esta razón, constantemente se ven nuevos dispositivos, plataformas y paqueterías que generan incompatibilidades en el nicho digital que una persona ha ido construyendo a su alrededor. Para quienes no han tenido acceso, familiarizarse con un entorno digital resulta más complicado, ya que después de aprender una habilidad digital, el hardware y el software se transforman, sin que necesariamente esta persona pueda actualizar su microentorno a la misma velocidad en la que acontece la innovación. En su momento, Castells (2001) afirmó que la velocidad con la que se transforma el entorno digital es prácticamente la de Internet, por eso menciona que uno de los aspectos más importantes del *e-learning* consiste en “aprender a aprender”, ya que esto permitirá que la persona pueda estar actualizada y tenga las habilidades para convertir la información obtenida en conocimiento y habilidad aplicados.

México no es el único país que presenta una brecha digital en sus asentamientos rurales. La infraestructura inadecuada y la dificultad para acceder a este tipo de lugares incrementan los costos que representa la instalación de las TIC en zonas rurales, por lo que a las empresas no les ha parecido atractivo este negocio. La Unión Internacional de Telecomunicaciones (ITU, por sus siglas en inglés) menciona que para mejorar la accesibilidad y conectividad de Internet en áreas rurales y remotas, se requiere de una política estatal robusta que se caracterice por: *1)* Facilitar los requerimientos regulatorios para operadores de redes en estas comunidades, *2)* Crear facilidades en impuestos locales y aduanales, *3)* Impulsar incentivos para la inversión mediante un clima de negocios caracterizado por la transparencia y la certidumbre; y *4)* Centrarse en redes de acceso complementario que atiendan a mercados desatendidos (ITU, 2020). Otros planteamientos que se han propuesto para resolver esta problemática han consistido en colocar infraestructura que pueda ser compartida por varios operadores y favorecer el desarrollo de habilidades y competencias digitales (alfabetización digital) para estimular la demanda de este servicio.

Otra política relevante para la construcción de la ciudadanía digital consiste en el fortalecimiento de la educación cívica que favorezca una participación democrática en el medio virtual. La regulación de la participación política en redes sociodigitales es una discusión que ha cobrado bastante relevancia en los últimos años. Al respecto, se ha señalado la necesidad de controlar la propagación de noticias falsas que pueden tener efectos indeseados en la toma de decisiones tanto individuales, como colectivas; aunque también se ha mencionado el riesgo que implicaría este tipo de regulación, ya que podría atentar en contra del derecho a la libertad de expresión. Mientras se definen mejor los contornos de esta discusión, se puede comenzar con fortalecer las habilidades digitales y la educación cívica de la población, ya que estas tendrían efectos positivos en la participación política en el entorno digital en un marco de libertades y respeto a los derechos humanos. Trabajar en esas esferas mejorará las capacidades para buscar, evaluar y utilizar información confiable que esté disponible en Internet. Asimismo, se esperaría que esto contribuya a mejorar el nivel de

discusión política para privilegiar el planteamiento de argumentos sobre comentarios lesivos que sólo atentan contra la dignidad de los interlocutores. Dicho con otras palabras, el Estado tiene una responsabilidad muy importante en implementar políticas públicas que favorezcan la educación formal en todos los niveles, ya que ésta es un medio central para que la ciudadanía tenga mayores capacidades de participar y tomar decisiones informadas en el uso, aprovechamiento y aprendizaje que les permite el nuevo entorno digital. La UNESCO plantea la misma idea con la premisa de que la población requiere tener capacidades necesarias para evaluar la información digital. Para ello se requieren procesos de aprendizaje formales e informales que combinen recursos en línea y fuera de ella, y con una prioridad en aspectos multiculturales (multilingüismo) para fomentar entornos de aprendizaje diversificados e incluyentes (Mansell y Tremblay, 2015). Ello implica tener especial atención a los factores contextuales específicos y la circunstancia de grupos poblacionales que se encuentran en una situación marginal (población adulta mayor, población indígena, con alguna discapacidad, etcétera).

Una política encaminada a la "alfabetización digital" podría estar encaminada a desarrollar habilidades y competencias relacionadas con el entorno digital a fin de resolver las problemáticas que cada sociedad defina como relevantes. Es importante enmarcar esta alfabetización como parte de un esfuerzo público mayor de mejorar la educación formal que imparte el Estado, ya que las carencias digitales están vinculadas a otra falta de capacidades en el aprendizaje que dificulta que las personas utilicen las herramientas del entorno digital para contribuir en la construcción de conocimiento y en la participación activa de la comunidad, es decir, se requiere fortalecer las capacidades de las personas para dotar de sentido y procesar la información para resolver problemas (Barroso, 2013). Dicho con otras palabras, el desarrollo de habilidades digitales para aprovechar el potencial que representan las TIC depende en gran medida de las competencias previas que ha desarrollado la persona en términos de aprendizaje y generación de conocimiento, ya que estas son básicas para identificar, discriminar y comparar información que circula en Internet. A lo largo del capítulo se mencionó que la participación en

redes sociodigitales o en otros ambientes tecnológicos que se desarrollen como medios de comunicación, no solamente requiere un andamiaje jurídico que garantice la libertad de expresión, la libertad de información y el derecho a la privacidad, por mencionar algunos aspectos normativos; también es importante que haya una educación cívica que oriente a la ciudadanía para que esta privilegie la argumentación sobre la descalificación o el insulto y tenga las herramientas para analizar críticamente la información que recibe para distinguir aquella que sea falsa de la que emiten fuentes confiables. Esto implica no sólo centrarse en el uso de las TIC, sino en las condiciones institucionales y socioculturales que favorecen determinadas formas de aprendizaje, el uso y la interacción en el entorno digital.

Ampliar y mejorar las condiciones de acceso para ejercer la ciudadanía digital es un mecanismo de inclusión social que puede marcar una diferencia en las condiciones de vida de las personas. A este respecto, la reducción de la brecha digital representa un aspecto ético para la sociedad del conocimiento, ya que implica igualar oportunidades para el desarrollo en la medida en que se convierta en una herramienta para mitigar las desigualdades estructurales que persisten en las dimensiones económica, social y cultural (Norris 2001; Pineda, 2009). De no reducirla, se correrá el riesgo de potencializar la desigualdad que ha afectado a sectores de la población, normalmente de bajos ingresos y nivel educativo, que han carecido de espacios y canales de participación en los que puedan expresar su voz para la toma de decisiones colectivas.

BIBLIOGRAFÍA

Barroso Jerez, C. (2013). Sociedad del conocimiento y entorno digital. *Teoría de la educación. Educación y cultura en la sociedad de la información*, 14(3), 61-86.

Castells, M. (2001). *La Galaxia Internet: reflexiones sobre Internet, empresa y sociedad*. Barcelona, España: Plaza & Janés.

Christakis, N. A., y Fowler, J.H. (2010). *Conectados. El sorprendente poder de las redes sociales y cómo nos afectan*. Madrid, España: Santillana.

Deursen, A. J. A. M van, y van Dijk, J..A.G.M (2010). Measuring Internet Skills. *International Journal of Human-Computer Interaction*, (26), 891-916.

Dijk, Jan A. G. M. van (2009). One Europe, digitally divided. En A. Chadwick y Howard, P.H. (ed.), *Routledge Handbook of Internet Politics* (288-304). Londres, Inglaterra: Routledge.

Eshet-Alkalai, Y. y Amichai-Hamburger, Y. (2009). Experiments in Digital Literacy. *Ciberpsychology & Behavior*, (7), 421-29.

Fernández Vicente, A. (2019). Caminar en la era del smartphone. *Revista Mexicana de Sociología, 81* (4), 855-80.

Isin, E., y Wood, P. (1999). *Citizenship and Identity*. Londres, Inglaterra: Sage.

Lara Caballero, M. (2014). La brecha digital en un contexto de participación ciudadana. En Natal, A., Benítez, M. y Ortiz, G. (ed.), *Ciudadanía digital* (75-100). Ciudad de México, México: UAM, Unidad Iztapalapa y Unidad Lerma; Juan Pablos Editor.

Mansell, R., y Tremblay, G. (2015). *La renovación de la visión de las sociedades del conocimiento para la paz y el desarrollo sostenible*. São Paulo, Brasil: UNESCO.

Marshall, T.H., y Bottomore, T. (1992). *Ciudadanía y clase social*. Madrid, España: Alianza Editorial.

Mossberger, K. (2009). Toward digital citizenship: addressing inequality in the information age. En A. Chadwick y Howard, P.H. (ed.), *Routledge Handbook of Internet Politics* (173–85). Londres, Inglaterra: Routledge.

Natal, A., Benítez, M. y Ortiz, G. (2014). Introducción. En .A. Natal, M. Benítez. y G. Ortiz (ed.), *Ciudadanía digital* (9-20). Ciudad de México, México: UAM, Unidad Iztapalapa y Unidad Lerma; Juan Pablos Editor.

Natal, A., Ortega, W. y Martínez, G. (2014). Ciudadanía digital: desconfianza política y uso de Internet para el ejercicio de la ciudadanía. En A. Natal, M. Benítez. y G. Ortiz (ed.), *Ciudadanía digital*, (21-47). Ciudad de México, México: UAM, Unidad Iztapalapa y Unidad Lerma; Juan Pablos Editor.

Norris, P. (2001). *Digital Divide. Civic Engagement, Information Poverty, and The Internet Worldwide*. Cambridge, Inglaterra: Cambridge University Press.

Pineda, M. (2009). Desafíos actuales de la sociedad del conocimiento para la inclusión digital en América Latina. *Disertaciones. Anuario electrónico de estudios en comunicación social*, 2 (1), 10–25.

Tilly, C., y. Wood, L.J. (2010). *Los movimientos sociales, 1768-2008. Desde sus orígenes a Facebook*. Segunda edición. Barcelona, Madrid: Crítica.

Unión Internacional de Telecomunicaciones (ITU) (2020). ITU launches new study paper on broadband and connectivity solutions for rural and remote áreas. *ITU News*. Recuperado de https://bit.ly/36UabQq

ENCUESTAS CONSULTADAS

Corporación Latinobarómetro. *Latinobarómetro 2015*. Instituto Federal de Telecomunicaciones. *Primera Encuesta 2019. Usuarios de servicios de telecomunicaciones.*

Instituto Nacional de Estadística y Geografía, Secretaría de Comunicaciones y Transportes e Instituto Federal de Telecomunicaciones. *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en Hogares (ENDUTIH), 2019.*

CAPÍTULO 06

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD EN LATINOAMÉRICA Y EL CARIBE

ALEJANDRO PISANTY BARUCH*

* Departamento de Física y Química Teórica, Facultad de Química, unam, Ciudad Universitaria, Av. Universidad 3000, Ciudad de México, y Centro Latam digital. El presente documento representa la etapa final, en 2020, de la línea de trabajo sobre ciberseguridad del proyecto Latam Digital que fuera comisionado al autor. Presento una visión de conjunto orientada a la estrategia a futuro centrada en un caso de estudio, México, en el contexto regional y mediante un análisis retrospectivo para la extracción de lecciones aprendidas.

Desde la expansión inicial del cómputo electrónico en la década de los cincuenta, la información clave de entidades vitales para la humanidad se ha almacenado en formatos digitales y se ha considerado necesario protegerla de diversos tipos de ataques e intrusiones. La extensión del cómputo a hogares, oficinas y toda clase de negocios y entidades gubernamentales (a través de la computadora personal en la década de los ochenta y el crecimiento explosivo de Internet en los decenios más recientes) han hecho indispensables las consideraciones de seguridad.

Con distintos nombres, que sólo parcialmente indican distintas entidades, en los ochenta y noventa lo llamamos seguridad en cómputo. Priorizaban los grandes centros de datos y la computadora personal comenzaba a despegar, los problemas que se presentaban eran más fallas en los programas de los sistemas operativos, mismos que eran usados por grandes *hackers* del momento para proporcionar esos descubrimientos y hacer aportaciones que marcaron una evolución en los sistemas usados en la época. Hacia finales de los noventa aparecieron los primeros virus conocidos con una intención principalmente de diversión (ping pong, cascada, etcétera), comenzaron a infectar equipos con capacidades mucho más (Disterer, 2013) maliciosas (borrado de información, reinicio de equipos). Con la primera década del presente milenio llegaron los estándares británicos (BS 7799-1, que se convertirían en el internacional ISO/IEC 27000, y serie consecuente) que marcaron una evolución y calidad en el procesamiento de datos. Se pasó de poner la atención en proteger la seguridad física en primer plano a priorizar los datos, así como su procesamiento en las compañías, bancos y gobiernos; entonces el concepto se llamó seguridad de la información. En esta época vimos un notable despegue de los problemas en seguridad que, aunado a la masificación de la computadora personal, el dispositivo móvil y el aumento de velocidades de transmisión, no hemos podido erradicar, pues aún hoy son un problema latente, ya que surgen ataques masivos que usan diversas tipologías como *spam*, *phishing*, DDoS, *malware*.

La evolución de los datos e información y, a la vez, de su procesamiento (velocidad, memoria, transmisión de módem a banda ancha) nos llevó a encontrarnos con grandes cúmulos de información, por lo que a inicios de 2012 comenzó a acuñarse el término ciberseguridad, donde la computadora se volvió básica en los hogares y oficinas; y el teléfono móvil se convirtió rápidamente en otro instrumento con el que el quehacer del ser humano pudo desenvolverse con grandes velocidades de transmisión y las redes sociales ocuparon un amplio espectro de la ecuación. Es en este punto donde comenzó la integración de la seguridad física con la seguridad lógica. Esa evolución nos llevó a ver la seguridad del dato y la información como un todo, presente en la seguridad física (cámaras, dispositivos, IoT) y en la lógica (programas, software, sistemas operativos) para así acuñar el término ciberseguridad. Lo anterior trajo nuevos retos y paradigmas en materia de ciberseguridad, ataques a gran escala, ataques de negación de servicio o DDoS masivos, secuestro de datos e información, redes sociales, etcétera. En esos años pudimos ver claramente cómo los gobiernos empezaron a interesarse más en el valor del dato y comenzaron a invertir para crear centros de respuesta, y algunos de ataque, reclutando personal experto para proteger infraestructuras de seguridad pública y nacional.

Es importante mencionar que hoy la ciberseguridad está sumamente relacionada con la inteligencia, que ha sido vital para las sociedades modernas. En el ecosistema de la ciberseguridad, actualmente la inteligencia tiene presencia electrónica y es usada de manera importante en lo que conocemos como ciberinteligencia. Esto no es más que el uso de herramientas especialmente diseñadas para hacer inteligencia llevada a los medios electrónicos. Esto ha derivado en conceptos como guerras híbridas, que existen en la actualidad y son empleadas como arma para poder desestabilizar gobiernos y diversas entidades de todas las escalas.

La seguridad informática, la ciberseguridad y la seguridad de la información han pasado a ser parte de la agenda pública de manera constante y extendida. La crisis derivada de la pandemia de Covid-19 en 2020 ha traído nuevos problemas y discusiones más amplias que años anteriores, debido a la súbita migración de actividades al ciberespacio por parte de cientos de millones de personas, así como la consecuente ampliación de la superficie de ataque a estas y a organizaciones.

Desde hace por lo menos sesenta años la protección de algunos activos y operaciones informacionales digitales ha sido considerada

parte de la seguridad nacional en los países industrializados. Esta preocupación se ha extendido y vuelto más compleja conforme los activos y las operaciones, así como los medios de intrusión, se han vuelto accesibles a actores cada vez más dispersos y diversos.

La ciberseguridad representa un problema particularmente complejo en la frontera entre seguridad personal, pública y nacional por la facilidad con la que un ataque a un activo informático personal puede permitir el acceso a ataques a la seguridad pública y estos pueden representar un problema de seguridad nacional. Un ejemplo para ilustrar esta afirmación es un ataque de *phishing* o de *ransomware* que compromete a cuentahabientes de la banca y se puede extender hasta desestabilizar el sistema financiero de un país u obligarlo a dejar de operar, así sea temporalmente. La ciberseguridad es un problema complejo y *wicked* ("perverso") en el que múltiples partes casi independientes interactúan de maneras imprevisibles e imposibles de regular.

El reconocimiento de la ciberseguridad como un componente de la seguridad nacional se da de diversas formas. En algunos casos los actores destacados de la seguridad informática han logrado atraer la atención de las autoridades de su país y estas progresivamente van incorporando la ciberseguridad a la estrategia de seguridad nacional, quizás inicialmente enfocándose en la protección de las operaciones de las fuerzas de seguridad, después con una visión sistémica de la sociedad. Países industrializados con un fuerte desarrollo informático propio incluyen los ataques a terceros como parte de sus estrategias de defensa nacional y progresivamente las extienden a sectores críticos de la nación, como las redes de producción y distribución de energía y agua, de ahí a sistemas principalmente privados como el financiero.

En América Latina y el Caribe (en lo sucesivo LAC) el panorama de ciberseguridad nacional es tan diverso como cabe esperarlo de la propia diversidad cultural, política y económica de la región. En años recientes, organismos como el Comité Interamericano contra el Terrorismo (CICTE), de la Organización de Estados Americanos (OEA), han observado que el continente entero debe pasar a la acción coordinada para defender la región, al tiempo que han impulsado una conjunción de esfuerzos nacionales para que cada país cuente con una Estrategia Nacional de Ciberseguridad (en lo sucesivo ENCS) competente y eficaz.

Una de las líneas de trabajo más activas de la OEA ha sido la colaboración con la Universidad de Oxford para crear un modelo de madurez en ciberseguridad nacional, estudiar país por país el estado del arte y calificarlo en función de dicho modelo de madurez, así como utilizar la evaluación para que cada gobierno, con los actores pertinentes, convoque, formule y aplique una ENCS. Con base en el modelo de madurez, cada país evaluaría de manera periódica los resultados de aplicar la ENCS y formularía un nuevo ciclo de la misma.

El trabajo realizado por la comunidad de Internet, durante décadas, sobre ciberseguridad fue incluido parcialmente, pero también se dejaron fuera contribuciones importantes. Los avances y logros de los distintos países son muy diversos. De eso trata también el presente trabajo, de identificar algunas aportaciones pendientes de recoger en las ENCS.

En un conjunto de investigaciones precedentes, diversos autores se han ocupado del tema ciberseguridad desde puntos de vista relevantes para el presente texto. Moreno Albornoz y Maqueo (2019) revisaron el estado de la ciberseguridad en América Latina y el Caribe, sobre todo desde la perspectiva del marco legislativo. Mario Vignettes (2019) analizó la esfera ética del ciberconflicto. María José Rodríguez Rodríguez (2019) exploró la relación de la ciberseguridad nacional con la inteligencia, tema que se retomará más adelante en este texto. Anahiby Becerril (2019) explora las dimensiones más amplias del ciberespacio, los orígenes y cálculos del riesgo y su impacto sobre la seguridad nacional.

En el mismo volumen, atendiendo la importancia de la formación de capacidades, Espinosa y Morales (2019) investigan el estado de la seguridad informática en las universidades y otras instituciones de educación superior en México. Salvador Camacho (2019) y Salvador Venegas-Andraca (2019) muestran aspectos tecnológicos que deben ser atendidos con visión estratégica de largo plazo (evolución del sistema de nombres de dominio de Internet y computación cuántica, respectivamente).

Carlos Estrada Nava (2021) provee un insumo fundamental para una potencial ENCS, un atlas de riesgos para la ciberseguridad, para el caso de México. Fátima Cambronero (2019) expande el horizonte de la gobernabilidad para la ENCS para considerar la naturaleza multisectorial, multipartita o *multistakeholder* de la gobernanza de

Internet (Gleckman, 2018; Harcourt *et al.*, 2020; DeNardis *et al.*, 2020) como un factor que las estrategias deben preservar y utilizar. Finalmente, en este volumen Alejandro Pisanty (2019) describe los diversos regímenes entre los cuales se desenvuelve la gobernanza de Internet y del ciberespacio, así como su efecto sobre la gestión de la ciberseguridad; además de un conjunto de variables fundamentales para el diseño de una ENCS realista, con visión de futuro, sustentable a largo plazo en el espacio internacional.

METODOLOGÍA

Para la elaboración del presente trabajo se consideraron los siguientes elementos:

1. Participación en los procesos consultivos de la Agenda Digital en México desde el año 2000 (Proyecto e-México, Programa para la Sociedad de la Información y el Conocimiento, Agenda Digital, Estrategia Digital Nacional).
2. Asistencia a reuniones de trabajo de la ENCS de México en el proceso impulsado por la OEA, 2017-18.
3. Estudio de documentos de las ENCS de diversos países de Latinoamérica y el Caribe, así como de países externos a la región.
4. Estudio de documentos adicionales a los de ENCS nacionales.
   - **a)** Informe Ciberseguridad 2016 (OEA-BID, 2016)
   - **b)** Informe Ciberseguridad 2020 (OEA-BID, 2020)
   - **c)** Informe Anual. Estrategia Nacional de Seguridad Pública (Durazo y SSyPC 2020)
   - **d)** Informes sobre ciberseguridad de la Unión Internacional de Telecomunicaciones (ITU, 2019; 2021)
   - **e)** Avances en revistas especializadas, noticias, y comunicados oficiales
5. Entrevistas con especialistas.
6. Iteraciones del proceso de análisis documental y entrevistas
7. Selección y adaptación de un marco de análisis para el estudio comparativo.
8. Realización del análisis y obtención de conclusiones y propuestas.

ANÁLISIS

Que un país disponga de una ENCS es actualmente una necesidad imperiosa. Los activos más importantes de la sociedad son digitales, o dependen del ciberespacio para su gestión, aprovechamiento y defensa.

Este hecho se ha ido imponiendo gradualmente entre los gobiernos de la mayoría de los países, en diversos grados de reconocimiento. Algunos han integrado una ENCS a sus estrategias tanto de seguridad nacional como de desarrollo digital; otros lo hacen de palabra, aunque no atienden la ciberseguridad a niveles jerárquicos suficientemente altos ni le otorgan presupuestos y capacidad de intervención suficiente; y muchos todavía están en etapas iniciales o superficiales de asimilación de esta idea.

Una ENCS, idealmente, debe estar conformada cuando menos por un documento maestro y un conjunto de mecanismos para llevarla a cabo; sin ejecución, el documento se vuelve irrelevante. Como toda estrategia, debe tener claridad en sus objetivos, metas, acciones, políticas, recursos requeridos, factores críticos de éxito y mecanismos de evaluación, retroalimentación y formulación de un nuevo ciclo. Como toda acción de planeación, estará constreñida por el "triángulo de hierro", formado por alcance, costo y tiempo; además de las variables usuales de la gestión de proyectos, como recursos humanos, comunicación y gestión del cambio. Además, estará sujeta a los mismos factores de presión que toda política pública y los de todo fenómenos de seguridad, plagados de incentivos perversos de actores, muchas veces, deliberadamente ocultos y que actuarán de manera indirecta.

Un importante tema de debate se refiere a las estructuras y mecanismos necesarios para que una ENCS sea efectiva. En países de Latinoamérica, ¿deberá estar aprobada desde la línea superior y ejecutarse por un órgano responsable que reporte de manera directa al poder Ejecutivo? En documentos relacionados con la Agenda Digital (Estrategia Digital Nacional, EDT) de México, de 2017, se produjeron estructuras con reporte directo a la oficina de EDN de presidencia o a la de tecnologías de información de la misma presidencia de la República, y pudieron al menos agruparse organizaciones de gobierno Para algunos autores, entre ellos Guel (comunicación personal, 2020-2021) la clave del relativo éxito en ciberseguridad de la Comunidad Europea y de España, en particular, fue crear el organismo que se

encargue de ella, fortalecerlo y dotarlo de herramientas y autoridad para evolucionar su economía, su transformación digital. El organismo a cargo conduce la ejecución de la estrategia, audita a diversos actores, propone iniciativas. Se trata del organismo que fue en sus orígenes conocido como Instituto Nacional de Tecnologías de la Comunicación (INTECO), hoy Instituto Nacional de Ciberseguridad (INCIBE) (con responsabilidad también sobre pymes y gobierno digital), y la seguridad nacional recae en la Agencia de Inteligencia Española (CNI). Muchos países europeos aplican hoy día este modelo.

Por otra parte, una ENCS debe estar alineada con la Estrategia Digital Nacional y acompasar su desarrollo con el de esta, valiéndose del desarrollo digital para contar con recursos y sirviendo a dicho desarrollo mediante la protección de sus actores y los activos que generan.

La formulación de una ENCS será más eficaz si reúne a todos los actores relevantes, se produce a través de procesos de consulta efectivos, logra acuerdos entre los actores clave y concita voluntades de todos los actores.

Para este estudio hemos considerado que uno de los marcos de referencia ideales de una ENCS modelo es el que está contenido en el modelo de madurez de Oxford. Para la Estrategia Digital Nacional elegimos los marcos de referencia formulados por Nagy K. Hanna. Para el análisis de las ENCS existentes adoptamos además el marco de referencia de Eduardo Alfredo Leiva y añadimos algunas variables que se expondrán más adelante.

El Modelo de Madurez de Capacidad de Seguridad Cibernética de Oxford (GCSCC, 2016) es producto de un trabajo acucioso que ya ha sido sometido a prueba y reformulado con base en la retroalimentación, producto de sus primeros resultados. El modelo se refiere específicamente a las capacidades para la ciberseguridad y evalúa cinco campos, a saber:

1. Política y estrategia de ciberseguridad
2. Cibercultura en la sociedad
3. Educación, capacitación/entrenamiento y competencias de ciberseguridad
4. Marcos legales y regulatorios
5. Estándares, organizaciones y tecnologías.

A partir de estos campos, el GCSCC construye un cuestionario que puede ser aplicado a actores relevantes en cada país y con ello construye calificaciones diferenciadas en cada rubro, las que al final se convierten en un estado de madurez calificado del 1 (menor) al 5 (mayor). Si bien esta metodología adolece de algunas imperfecciones (incentivos perversos de algunos actores, selección de participantes, subjetividad, información incompleta), permite un seguimiento longitudinal en cada país y una comparación transversal entre países que pueden ser productivas –sería deseable un mecanismo que incluya explícitamente a más actores (en la actualidad disponemos de este). Los indicadores de otras evaluaciones, como las de la ITU (2020), adolecen también de opacidad y de que son alimentados exclusivamente por gobiernos, para los cuales existen diversos incentivos que pueden llevar a distorsiones.

El marco de análisis de madurez de GCSCC ha sido aplicado en dos ciclos por la OEA, uno en 2016 y otro en 2020. En el segundo se hicieron algunas modificaciones mediante trabajos del grupo de Oxford.

El marco de referencia de Nagy Hanna (2016) se aplica a las estrategias nacionales o subnacionales que en distintos momentos se han conocido como programas e-<país> (por ejemplo e-México), Agenda Digital, programas de desarrollo de la sociedad de la información o del conocimiento, estrategia digital (nacional en su caso), o más recientemente transformación digital. Para el mejor desarrollo de estas estrategias Hanna recomienda los siguientes diez factores:

1. Visión y compromiso compartidos
2. Sinergias y escala
3. Infraestructura *soft* y capacidad local
4. Transformación integral en estrategia nacional
5. Alianzas público/privado
6. Difusión e inclusión para la equidad
7. Fondeo estratégico y adaptable
8. Balance estratégico nacional/local
9. Descentralización y gestión del cambio
10. Monitoreo y evaluación ágil desde el inicio.

Puede observarse fácilmente que estos mismos factores se pueden aplicar al desarrollo e implantación de una ENCS.

Leiva (2015) hace un minucioso análisis de las ENCS de varios países latinoamericanos (Colombia, Brasil, Chile y Argentina) y de otras regiones, mismos que agrupa en el bloque anglosajón (Canadá, Reino Unido, Estados Unidos de América) y de la Unión Europea (Alemania, Francia, España y Estonia), más Japón y Rusia. De su extenso y cuidadoso trabajo extrae para calificar (con una calificación binaria sí/no) los rubros siguientes:

1 Protección de
- **a)** Infraestructuras críticas
- **b)** Economía
- **c)** Seguridad nacional
- **d)** Bienestar social

2 Enfoque
- **a)** Concientización
- **b)** Conocimiento
- **c)** Educación
- **d)** Capacidades cibernéticas militares

3 Sector público
- **a)** Liderazgo/coordinación
- **b)** Marco jurídico

4 Sector privado
- **a)** Participación en la estrategia

5 Cooperación internacional
- **a)** Cooperación en su grupo
- **b)** Cooperación con otros países (se entiende que fuera de su grupo)

Además de los documentos de ENCS consultados por Leiva, se acudió a versiones más actualizadas en aquellos países de la región en donde existen y, en casos selectos, de los de otras regiones, así como al conciso resumen de CCI de España (García, 2018; Kosévich, 2019; CCI, 2021; CONPES 2020; (Andrés R. Almanza, 2020), 2020; Pisanty, 2020).

En conjunto, estos tres marcos de referencia nos permiten analizar, comprender y evaluar las ENCS desde varios puntos de vista complementarios y proponer algunos pasos hacia adelante, especialmente para el caso de México.

Adicionalmente, el ciberespacio y la ciberseguridad son conceptos polisémicos cuya definición varía a lo largo del tiempo, de geografías y sectores. En todos los casos, las consideraciones acerca del ciberespacio están íntimamente ligadas a Internet y, por ello, a su gobernanza. La gobernanza de Internet no puede reducirse a la acción de los gobiernos ni a su colaboración a través de organismos intergubernamentales ni a la acción conjunta de los gobiernos con la industria, como se ha demostrado y lo sigue probando el sistema construido a propósito en las décadas recientes. Los marcos de referencia descritos, excepto quizás el de Hanna, no toman en cuenta algunas propiedades básicas de Internet, los efectos específicos de Internet sobre la conducta humana y organizacional y las características fundamentales de la gobernanza de Internet. Por ello hemos complementado estos marcos de referencia con criterios derivados de estas líneas de trabajo.

En las propiedades de Internet consideramos la arquitectura de capas, la conmutación por paquetes, el principio de mejor esfuerzo, la interoperabilidad, la apertura, el principio de robustez, la descentralización, la escalabilidad, y la innovación sin pedir permiso.

Analizamos los efectos de Internet sobre las conductas a través del marco de referencia 6F, de nuestra autoría, en el que se mapean los fenómenos y conductas entre Internet y el mundo fuera de línea (predecesor o externo a Internet) mediante los factores de masificación (incluyendo efectos de red), identidad y anonimato, transjurisdiccionales, abatimiento de barreras, reducción de fricción, y efectos de memoria y olvido (Pisanty, 2020).

La gobernanza de Internet ha sido un campo contencioso; sin embargo, cuenta ya con elementos relativamente estables a partir de los principios de la Cumbre Mundial sobre la Sociedad de la Información (CMSI), de los cuales destacamos que debe ser democrática, orientada a las personas, a los grupos en situaciones de desventaja y basada en la participación de todas las partes interesadas. Además, los mecanismos de gobernanza de Internet que han probado su efectividad están orientados a la solución de problemas específicos, razonablemente bien identificados; reúnen a todas las partes interesadas mediante representantes adecuados; cuentan con un diseño institucional proporcional al problema que resuelven, se basan en la racionalidad técnica de Internet, están construidos con

capacidad para evolucionar y adaptarse a realidades cambiantes y de ser necesario cuentan con mecanismos explícitos para desarrollar políticas y aplicarlas transparencia, rendición de cuentas y formas de reclamación, reversión y compensación de decisiones impugnadas.

La gobernanza por múltiples partes interesadas o *multistakeholder* (en lo sucesivo MSH) ha sido probada en muchos campos de acción fuera de Internet y el ciberespacio, y es un complemento a la acción gubernamental y multilateral cuando esta no es suficientemente ágil o de grano fino para responder a los cambios producidos por la tecnología. En el caso particular de Internet se ha probado hasta la saciedad la importancia de reunir actores gubernamentales, del sector privado (entiéndase también industria, de negocios o lucrativo), sociedad civil (o tercer sector), y de manera bien específica a la comunidad técnica de Internet, que puede ser transversal a los otros sectores y participa guiada, ante todo, por el conocimiento técnico, las posibilidades y limitaciones de la tecnología.

Si bien la seguridad no aparece explícitamente en la lista de principios de Internet aquí enunciada, es incorrecta la apreciación de que no fue considerada desde el inicio en el diseño de los protocolos que le dieron lugar. Lo que sucede con la seguridad está contenido especialmente en el principio de robustez de Postel, que deja en la orilla tareas como las de protección de la información, mientras que la responsabilidad de la red se restringe al paso eficaz y eficiente de paquetes IP. En los años en que se desarrolló esta investigación y sus primeras aplicaciones a la interconexión de redes, la criptografía estaba en una etapa de rápida evolución tanto en su aspecto matemático (desarrollo de algoritmos como el RSA y los de Diffie y Hellman) como en el computacional con una aceleración en la capacidad de proceso que permitía desafiar de manera constantemente creciente a las implementaciones de los algoritmos criptográficos, incluso los más avanzados.

Por ello el diseño de Internet deja al emisor y el receptor de los mensajes el cuidado de la integridad, autenticación, confidencialidad, disponibilidad y no refutación de la información y sus operaciones. Más tarde ha sido necesario dedicar esfuerzos adicionales a la protección de la infraestructura de red, ya que los equipos activos que la conforman también son computadoras; sus sistemas operativos y software están sujetos a fallas, vulnerabilidades, riesgos y ataques similares a los de la orilla y la intercepción de mensajes es posible, incluso en fibra óptica. No obstante esta protección a la red, el principio de subsidiaridad implícito en la formulación "inteligencia en la orilla" descarga la responsabilidad en los emisores y receptores para las propiedades de la información citadas al principio del párrafo.

La comunidad técnica y de las primeras aplicaciones sociales de Internet adaptó rápidamente conductas defensivas y preventivas cuando, en un rudo despertar, aparecieron los primeros ataques, desde el *spam* hasta los gusanos, troyanos y virus informáticos basados en Internet o capaces de propagarse usando la red. Observamos así tanto el diseño de medidas técnicas, entre las que figuran las listas de control de acceso en los ruteadores, como las medidas organizacionales, destacando la conformación de Computer Emergency Response Team o Equipo de Respuesta a Emergencias Computacionales (CERT) y, posteriormente, Computer Security Incident Response Team o Equipo de Respuesta a Incidentes de Seguridad en Cómputo (CSIRT) y la red Forum of Incident Response and Security Teams o Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST) que los reúne, el intercambio de información, la creación de ambientes de confianza, la capacitación a especialistas, usuarios, funcionarios y población en general, la concientización, la intervención en políticas públicas y legislación. Los CERT y CSIRT se formaron inicialmente, sobre todo, en universidades. El éxito de este modelo llevó después a conformar unidades similares en sectores como el financiero, en algunos países, y en los gobiernos, dotando a las unidades de capacidad legal de iniciar la persecución de delitos, colaborar con fuerzas policiales o militares del propio país y del extranjero, e intervenir en seguridad pública y nacional.

Para contar con información al día, realista y a detalle necesaria en dicha evaluación, adicionalmente al análisis documental y otros trabajos de gabinete, entrevisté a cuatro expertos de diferente formación, origen y actividad profesional. Todos ellos cuentan con más de 20 años de experiencia en el campo en varios países de la región a partir de las responsabilidades y cargos en que se han desempeñado. Las entrevistas se llevaron a cabo durante los meses de junio y julio de 2020 por vía telefónica. A partir de las primeras tres se elaboró un cuestionario más ela-

borado para preparar la cuarta, misma que se complementó con preguntas y exploraciones no estructuradas.

Con base en los análisis realizados, se puede hacer un primer conjunto de calificaciones para la ENCS de México, al usar la tabla de variables de Leiva y complementarla con los criterios derivados de los otros marcos de referencia y la información obtenida en las entrevistas. A los criterios de Leiva he añadido algunos de elaboración propia.

CUADRO 01. CONTINÚA

Variable Leiva	Estado actual en México (resumen)	Propuesta (resumen)
Ausencia de órgano de dirección en ciberseguridad.	Mandato disperso, sin autoridad suficiente.	Crear un organismo o mecanismo de coordinación, definir y reorganizar mandos y estructuras con participación de todas las partes interesadas.
Gestión desconcentrada.	Falta visión macro, más desconcentrada que gestionada. Ausencia de estándares.	Cadena de mando en el ámbito, por sectores. Estructurar. Normalizar.
Insuficientes recursos humanos, técnicos y económicos en organismos de gestión.	Carencia de modelo de formación. Recursos insuficientes en número, calidad, alcance y eficacia.	Presupuestos públicos e incentivos para los privados. Sueldos, reclutamiento, estabilidad e incentivos. Adquisición de recursos técnicos (hardware y software). Dispersión y estructura del presupuesto en el nivel federal y subnacional, con alcance a los sectores privado, social, técnico y académico.
Conocimiento parcial e insuficiente de la situación nacional mediante estado fiable y actualizado de información.	Al no haber mando centralizado ni estructuras de coordinación, no se levantan estadísticas ni hay tablero de mando, la autoridad del CERT "central" es insuficiente.	Debe crearse un organismo con autoridad y acciones definidas. Estructuras y, sobre todo, mecanismos funcionales y sustentables. Construcción de confianza y comunicaciones abiertas.

CUADRO 01. CONTINÚA

Ausencia de marco compartido, estable y abierto en ciberseguridad. Insuficiente comunicación pública-privada.	Falta de coordinación. Interfiere el cabildeo de empresas interesadas en proveer equipo y servicios o en un marco regulatorio específico. En el sector financiero, apenas hay un tibio avance por respuesta a ataques significativos. Sector energético y otras infraestructuras críticas mal protegidas.	Organismos o mecanismos de coordinación. Estructurar líneas de confianza, comunicación y coordinación. Construir canales confiables. Estabilidad de estructuras, normas, procesos y personas.
Escasa colaboración de sectores privados.	Incentivos perversos para ocultar información. Falta confianza.	Incentivar los mecanismos de colaboración intersectorial que den confianza a actores de los sectores privado, social, técnico y académico. Crear un sistema estructurado de incentivos (ley y normas de *data breaches*, seguros y aseguradoras, responsabilidad civil, responsabilidades de funcionarios públicos, ambientes de mediación con academia y sociedad civil.
Ausencia de normativa específica y completa en ciberseguridad, así como de legislación	Leyes inaplicables. Códigos de procedimiento inaplicables o débiles. Incentivos perversos. Malas iniciativas de ley que posponen	Articular esfuerzo de toda la sociedad y, también, a través de partidos. Capacitación Latam Digital para legisladores, asesores y otros interesados en buenas leyes. Instrumentos internacionales. Convención de Budapest.

para delitos cibernéticos que permita la aplicación de ley.	continuamente el proceso de contar con buenas leyes. Leyes en colisión con derechos humanos y civiles. Excesivo énfasis en delitos en materia de propiedad intelectual.	
Ausencia de política estatal de concientización y educación por separado, ciudadanía en general y desarrollo de talentos.	Carencia de talento formado a profundidad y actualizado disponible para el Estado, por bajos sueldos e incentivos negativos (*ergo* rotación a sector privado). Políticas de concientización a través de la SEP y SCT débiles, insuficientes y a destiempo (ejemplo, documento SCT ciberseguridad durante Covid-19) (CIAPEM, 2020). Ideologización, romantización y otras fallas en programas de concientización. Insuficiente o nula captación de	Crear organismo nacional o mecanismos funcionales de construcción de consensos y participación y, a la vez, ejercer política multicanal para los estados. Dotar recursos para iniciar en los estados un modelo de creación de políticas y capacidades, capacitación, y que los estados inviertan con aportaciones de recursos propios; algunos mecanismos basados en “par y paso”. Elevar el nivel de concientización mediante esfuerzo multistakeholder. Acompañar la concientización con formación de pensamiento crítico y computacional en general. Acudir al sector educativo con apoyos y no sólo demanda de servicio. Activar la colaboración con sociedades profesionales y académicas. Fomentar, mediante presupuesto y plazas, la creación de licenciaturas, posgrados y educación continua en ciencias de la computación, matemáticas, estadística, informática y seguridad.

CUADRO 01. CONTINÚA

	talento de manera programada. Insuficientes programas de formación de talento.	
Variables propias de este estudio (hallazgos)	**Variables propias de este estudio (observaciones)**	**Variables propias de este estudio (recomendaciones)**
Inestabilidad de estructuras.	Cambios sexenales o más frecuentes, rotación de personal a sector privado.	Programa nacional de economía digital a 25 años que incluya la creación de un órgano de ciberseguridad en el nivel nacional, y propiciar el apoyo, ayuda de los estados. Aumentar sueldos y estructuras en sector público. Incentivos virtuosos. Buscar rotación de personal, planeada, con resultados positivos para ambos sectores.
Insuficiente dominio del idioma inglés.	Dificulta educación, entrenamiento, capacitación, interacción y colaboración. Limita relaciones con organismos nacionales, extranjeros e internacionales. Impide la participación exitosa en ejercicios. Dificulta el establecer confianza.	Programa de educación en ciberseguridad desde niveles básicos, incluido inglés como idioma secundario. Formación en inglés en todo el sistema educativo y oferta especializada en el sector dedicado a la ciberseguridad y a TIC en general.

CUADRO 01. CONTINÚA

Insuficiente conexión con sectores técnico y académico.	Desaprovechamiento de esfuerzos anteriores (CERT, Plataforma México, disc y otros) La reinvención constante lleva a la improvisación.	Alianzas macro desde el gobierno, pensando en economía digital macro. Relaciones firmes y constantes, tanto formales, como informales entre los sectores. Construcción de confianza Evaluación seria, evolución gradual.
No hay prioridad adecuada de las TIC desde la cabeza del Poder Ejecutivo.	No puede haber prioridad en otros niveles ni en los otros Poderes de la Unión. No se atiende la ciberseguridad como parte de la seguridad pública ni nacional. No se incentiva al personal ni la construcción de políticas y normas. Se desprecia u hostiliza la colaboración con el sector privado. Se desprecia u hostiliza a la sociedad civil y a la prensa. Se combate a los órganos autónomos.	Crear política macro, con órganos que sirvan no para fines políticos, sino para la economía e igualdad entre ciudadanos. Una vez creada la política y los organismos mencionados, que estos celebren pactos de colaboración con los principales sectores. Construir confianza con base en relaciones, cuerpos multiactor y resultados. Otorgar prioridad en seguridad nacional y pública con todas las cabezas de sector (designar a un subsecretario como responsable, incluir en lista de verificación de todas las conferencias de seguridad, llevar a Conago, Poder Legislativo, Poder Judicial y el CIAPEM). Respetar la contribución de los órganos autónomos.
Se minimiza la importancia estratégica	EDN y programa de la sct se basan en hipótesis de	Invertir en creación de polos tecnológicos, incentivar a las empresas dedicadas a las TIC, cibereconomía

nacional de la infraestructura crítica que es operada por actores privados (finanzas, teletrabajo, nube, salud, logística, alimentos, etcétera).	control estatal no sustanciadas. No se integran inventarios de infraestructura crítica suficientemente amplios. Se deja fuera a actores críticos. Algunas insuficiencias son reflejo de otras en infraestructura material (distribución y almacenamiento de energía, agua, dinero, alimentos, medicamentos, insumos para la salud, etcétera.	digital. Propiciar apoyos a desarrollos e investigaciones del país, empresas, academia, etcétera. Invitar al sector privado a incorporarse a la actividad con incentivos adecuados y confianza. Separar claramente de situación fiscal. Realizar inventarios verificables de infraestructura crítica, incluyendo situación de seguridad (nivel de madurez, contabilizando también personal disponible). Concientizar a empresas de necesidad de robustez y resiliencia y otorgar incentivos para que crezcan.
Excesiva intervención de empresas en diseños institucionales, paradójicamente, simultáneo con exclusión de empresas.	Las empresas participan en los procesos de la OEA y algunos nacionales. Intervención a través de cámaras y asociaciones, así como de consultorías Intervención en la fijación de estándares y normas. Captura de procesos NOM y NMX (ejemplo elecciones, NIST, ISO 29500, etcétera.)	Diversificación de participantes en procesos conducentes a la ENCS. Declaraciones de interés de participantes, incluyendo los de organismos internacionales. Incorporación de actores sociales, académicos y técnicos con separación de intereses y principios, incluidas asociaciones profesionales y sociales. Roles bien definidos y controlados para las empresas.

Insuficiente transparencia e información para evaluar nivel de madurez.	No se publica ni hay seguimiento del modelo de madurez de Oxford/OEA, cuestionario UIT, ni ningún otro.	Fomentar competencia entre instituciones de órganos de gobierno, estados. Fomentar competencias como *catch the flag* entre países, pero a un nivel local, con el objetivo de elevar las capacidades técnicas y desempeño de las organizaciones; sería uno de los pasos, con el tiempo, para medir esa madurez en ciber; también es un mecanismo para la construcción de confianza. Publicar cada año una evaluación independiente, de acuerdo con el modelo de madurez elegido, generando series de tiempo estables de alta comparabilidad. Comparativos anuales con OEA, OCDE, T-MEC y otros organismos y referencias relevantes. Auditar con base en evaluaciones. Retroalimentación a través de la sociedad.
Insuficiente flujo y colaboración internacional.	Los incidentes transnacionales no son debidamente atendidos (todos lo son en algún nivel).	Entender que ciber es global, definir presupuestos y participar en concursos, actividades globales ciber, foros académicos y de seguridad nacional. Participación en grupos OEA, ejercicios regionales (Norteamérica, Centroamérica, los Andes, Latinoamérica, OCDE) con observadores externos.

CUADRO 01. CONTINUACIÓN

Estrategia Digital Nacional	No se ha formulado una Estrategia Digital Nacional integral, con autoridad única y relevante, que sirva de anclaje a la estrategia nacional de seguridad. Los elementos de la EDN existentes y fragmentados, de alcances limitados y no suficientemente públicos, generan nuevas vulnerabilidades y dificultan formular una ENCS.	Se necesita un organismo o mecanismo estable, sustentable y con autoridad suficiente, en el o los que descanse la EDN, se brinde seguimiento continuo, se mida el desempeño, mejoren procesos de manera continua, se notifique a los actores que lo componen y tenga autoridad para ejercer como catalizador de cambio. Formular una Estrategia Digital Nacional como estrategia del Estado y de la nación, mediante un amplio proceso consultivo. Analizar cada elemento de la EDN por sus impactos en derechos, vulnerabilidades y seguridad. Formular una ENCS del Estado y la nación, mediante el concurso de todos los sectores, compatible con la EDN, y sustentable en el largo plazo.

Con base en la tabulación original en la que Leiva presenta su comparación de las ENCS de Colombia, Brasil, Chile y Argentina, he añadido una columna para la situación detectada en México. Leiva presenta una calificación binaria (sí/no); he añadido, para el caso de México, una calificación semicuantitativa o cualitativa según corresponda, como se observa en el cuadro a continuación:

CUADRO 02.

		COL	BRA	CHI	ARG	MEX
Protege	Infraestructuras críticas	X	X	X	X	Deficiente
	Economía		X			Deficiente
	Seguridad nacional		X			Mínima, desconocido
	Bienestar social	X	X			No existe programa alguno, SSPC Federal manda información dispersa y a veces confusa
Enfoque	Concientización	X	X	X		Mínima y deficiente
	Conocimiento		X			Mínima y deficiente
	Educación	X	X	X		Mínima y deficiente
	Capacidades cibernéticas militares	X				Información insuficiente, desconocido
Sector público	Liderazgo/coordinación	X	X	X	X	Mínima y deficiente
	Marco jurídico	X			X	En evolución. Deficiente y en evolución poco productiva. Sin uso exitoso alguno desde su creación, en 1999
Sector privado	Participación en la estrategia	X	X	X		Marginal. Autodefensa. Reactiva
Cooperación intersectorial	Cooperación en su grupo	X	X	X	X	Marginal y no pública
	Cooperación con otros países	X	X	X	X	Mínima

A continuación, se explican brevemente las calificaciones asentadas en el cuadro:

1 **Infraestructuras críticas.** Se actúa por separado para la protección cibernética de infraestructuras de distribución de energía eléctrica y de oleo y gasoductos. Los ductos de transporte de combustibles están sometidos a ataques físicos constantes. Los incentivos políticos para reportar avances contra el delito en este ramo dificultan la evaluación de su éxito. El informe de Estrategia Nacional de Seguridad Pública de la SSyPC 2020 refiere estadísticas y acciones para el control de delitos contra los ductos de combustible separadas de las acciones de inteligencia y en materia cibernética. Este no informa de intervención alguna en delitos de tal naturaleza. En materia de controles cibernéticos, los expertos entrevistados consideran que se actúa de forma extremadamente limitada (*aristeguinoticias*, 2020). Constantemente conocemos de su vulneración por medios públicos, Pemex, SE, Pronósticos Deportivos (Banxico, 2019).

2 **Economía.** No está publicada una estrategia para proteger a la economía en su conjunto. Las empresas y la banca expanden actividades como el comercio electrónico, con consideraciones mínimas de seguridad (sobre la banca, véase más adelante). Secretará de Economía recientemente vulnerada, afectada en el *core* de los registros de empresas, etcétera.

3 **Seguridad Nacional.** Si bien se conocen algunos enunciados y se sabe públicamente de la existencia de acciones para la defensa de la seguridad nacional, esta no está comprendida de manera amplia en las estrategias del sector público. Las fuerzas de defensa (Ejército y Marina) cuentan con capacidades que comprensiblemente no son divulgadas, lo que hace imposible una evaluación basada en elementos más explícitos. El comparativo con otros países, obtenido mediante evidencia indirecta de su participación en ejercicios internacionales, indica capacidades individuales altas y un número de personas que cuenta con ellas sumamente escaso. Conocimiento de intercambio de experiencias con otros órganos militares por la prensa, mas no por los organismos.

4 **Bienestar social.** El bienestar social no está considerado en la ciberseguridad nacional. Entidades como el Banco del Bienestar y Servidores de la Nación, utilizados para detectar la necesidad de apoyos económicos del gobierno federal por parte de la población, y para dispersar esos recursos, están sujetos a captura política, penetración y captura de fuerzas delictivas, asaltos a sucursales bancarias e insuficiencias en la infraestructura informática que puede debilitarse aún más en caso de llevarse a cabo un proyecto en curso de cambio en el *core* bancario. En otros aspectos el bienestar social no es una consideración estratégica publicada.

5 **Concientización.** Existen esfuerzos débiles y poco coordinados de la Secretaría de Comunicaciones y Transportes y de la Secretaría de Educación Pública. Los organismos relacionados con la banca difunden información para impulsar un mínimo de capacidad entre los usuarios para evitar ataques a su patrimonio. Autodefensa.

6 **Conocimiento.** No hay un esfuerzo coordinado para difundir y profundizar el conocimiento técnico, el razonamiento crítico y la capacidad personal para actuar contra ataques cibernéticos entre la población en general. Hay evidencia mínima de acción entre el funcionariado público, limitada por reducciones de sueldos, rotación de personal y reducciones drásticas de presupuestos. Personal especializado ha migrado al sector financiero; se cuenta con personal con poca experiencia actualmente y se observa improvisación.

7 **Educación.** Existe un número sumamente limitado de programas educativos, en el nivel superior y de posgrado, orientados a la ciberseguridad y disciplinas auxiliares. La matrícula es insuficiente. No existe política educativa al respecto.

8 **Capacidades cibernéticas militares.** No hay información explícita disponible que permita cuantificarlas. Por conocimiento externo se sabe que están creando un centro de comando para las capacidades cibernéticas, pero carecen de estrategia, visión y alcance.

9 **Sector público liderazgo/coordinación.** Limitado a la UGECTI (posteriormente Unidad de Gobierno Digital, eliminada con base en la política de austeridad gubernamental) de la Secretaría

de la Función Pública (SFP) e instancias sucesoras (en oficina de Coordinación de Estrategia Digital, en presidencia de la República, aparentemente), de la que no se conocen documentos de valor sustancial para los fines de la ciberseguridad nacional y el papel normativo de las adquisiciones de la Secretaría de Hacienda y Crédito Público y su Coordinación de Tecnologías de Información y Seguridad Informática. La reducción de sueldos y la eliminación del nivel jerárquico de la Direccion General de Tecnologías de la Información de las secretarías de Estado reduce los incentivos y capacidades de estas entidades. En 2019 y 2020 han sufrido ataques varias de estas.

10 **Sector público-marco jurídico.** No hay un marco jurídico específico y activo para la ciberseguridad nacional. Se han presentado iniciativas de ley federal para la seguridad informática que, por sus imperfecciones, no han progresado. Han sido aprobadas iniciativas de ley con incidencia en seguridad informática, en materia de propiedad intelectual e industrial, que no conducen a la protección de los usuarios individuales (para quienes, al contrario, generan nuevos riesgos de persecución y censura) y sólo se orientan a la persecución de conductas lesivas a dichos derechos de naturaleza económica. La adopción de Normas Mexicanas (NMX) para la seguridad en sistemas de elecciones propuesta incidiría de manera negativa en las mismas, al crear una interferencia indebida con la autoridad, electoral dotada de autonomía en el nivel constitucional. El Código Penal Federal, artículo 211 bis, del 1-7, sanciona los delitos informáticos. A la fecha ni un solo detenido usando ese marco legal.

11 **Sector privado participación en la estrategia.** Hasta 2018 el sector privado fue un participante y también un promotor activo de la elaboración de la ENCS. Actualmente se le observa marginado, con participación limitada a un cabildeo reducido y frecuentemente defensivo.

12 **Cooperación internacional en su grupo.** Existen indicios de actividades operacionales conjuntas con otros países. No se ha dado continuidad al trabajo integrado con la OEA, iniciado en 2016-2017. En la región de Norteamérica el T-MEC puede inducir algunas actividades internacionales conjuntas, de las cuales las más evidentes estarán relacionadas con la propiedad intelectual e industrial. Existe evidencia indirecta de colaboración en materia de inteligencia financiera, principalmente orientada a la detección de actos de corrupción del pasado y los correspondientes a la agenda del plan del gobierno contra la evasión fiscal, iniciada en periodos anteriores de gobierno. La Unidad de Inteligencia financiera (UIF) ha anunciado también acciones preventivas del lavado de dinero y orientadas al debilitamiento de organizaciones criminales; por su naturaleza, procede presumir colaboración internacional principalmente con Estados Unidos. En capacidades ciber, son escasos los casos de participación. Conocimiento de medios de pocos esfuerzos conjuntos en operaciones con Interpol, etcétera.

13 **Cooperación con otros países.** A nivel operacional se dan a conocer con cierta frecuencia maniobras contra delitos cibernéticos, principalmente los relacionados con la trata de personas y el abuso sexual contra menores. En otros planos, la representación de México ante la ONU es un actor eficaz en la negociación de instrumentos internacionales en marcha a través del Group of Governmental Experts (GGE), Open-Ended Working Group (OEWG) y negociaciones asociadas; ha hecho anuncios de participación que se prevé sustantiva en los acuerdos del Plan de Ruta de Cooperación Digital del Secretario General, António Guterres.

CONCLUSIONES Y RECOMENDACIONES

Las estrategias de ciberseguridad nacional deben armonizar la Estrategia Digital Nacional y la Estrategia Nacional de Seguridad. Conviene alcanzar los máximos niveles de madurez posible, avanzando en todas las variables que los componen. Es indispensable para la seguridad de las naciones mantener vigentes los principios fundamentales de Internet.

En México se requiere un esfuerzo especial para formular una estrategia de ciberseguridad clara, participativa, integral, transparente, abierta al mundo sin perjuicio de la seguridad nacional y que pueda ser llevada a la acción, vigilada y renovada a través de ciclos sucesivos de evaluación y retroalimentación.

AGRADECIMIENTOS

El presente trabajo se llevó a cabo dentro del proyecto Latam Digital, apoyado por CIDR, con sede en el Centro de Investigación y Docencia Económicas (CIDE). A ambas instituciones corresponde un profundo agradecimiento por facilitar la realización del proyecto en todas sus etapas. Toca un agradecimiento muy especial a la doctora. Judith Mariscal por su liderazgo, visión, tolerancia e invariable apoyo. El apoyo de Alejandra Ruiz del Río ha sido sustancial, igualmente invariable, motivador e invaluable para la planeación y seguimiento de las acciones. A Gloria Mayne le agradezco su actividad y su actitud, y su participación para llevar a cabo contactos insustituibles. Juan Carlos Guel hizo una revisión crítica del texto y aportó conocimiento y puntos de vista expertos, sumados a lo largo de muchos años, por lo que le corresponde un especial agradecimiento. Carlos Estrada, Andrés Velázquez y Jeimy José Cano aportaron mucho más que sus conocimientos y experiencia; su visión y su perspectiva, complementarias entre sí, abren nuevos caminos. Agradezco también a Alejandro Villalobos su contribución sobre infraestructura crítica en energía (petróleo y combustibles).

APÉNDICE

Cuestionario utilizado en entrevista estructurada

1. ¿Cuáles son los factores críticos para producir una ENCS exitosa?
2. Entre los países de Latinoamérica y el Caribe, ¿cuáles son las ENCS más exitosas o prometedoras, por qué?
3. Me han comentado otros analistas que un factor de éxito de la ciberseguridad en Colombia, en tanto estrategia nacional o política pública, es la prolongada colaboración con Estados Unidos de en el combate al narcotráfico y otros males. ¿Qué tan cierto es esto?
4. ¿Qué impacto tiene la rotación de personal y los cambios de políticas resultantes de los respectivos cambios en gobiernos, por ejemplo, después de elecciones, *vis-á-vis* la continuidad de las políticas?
5. ¿Qué impacto tienen las competencias en software, ciencias de la computación y demás tecnológicas; *soft skills* de relaciones; y el manejo del idioma inglés?, ¿pueden influir en la construcción de confianza entre CERT y unidades similares?
6. ¿Hasta qué nivel es útil para una ENCS la aportación de la OEA y dónde debe volverse un esfuerzo propio o autónomo del país?
7. ¿Es importante (en todos los países/en algunos países) el tránsito de personal entre el gobierno y el sector privado? En los casos en que exista, ¿se debe a un diferencial de sueldos o hay otros factores en juego?
8. ¿Cuáles son tus recomendaciones generales a futuro para mejorar la ciberseguridad en la región?

BIBLIOGRAFÍA

Almanza J., A.R. (2020). XX Encuesta Nacional de Seguridad informática. Lecciones aprendidas y visión de futuro. *ACIS Sistemas,* (155), 24-60. doi: 10.29236/sistemas.n155a4

aristeguinoticias (2020). "Hackeo al sistema de la Secretaría de Economía provoca suspensión de trámites", 24 de febrero. Recuperado de https://bit.ly/35nKry3

Banxico (2019). *Principales incidentes cibernéticos ocurridos en 2019 en el sistema financiero nacional.* Recuperado de https://bit.ly/3IWPwvP

Becerril, A. (2019). La ciberseguridad en la Seguridad Nacional: amenazas y retos en el ciberespacio. A. Pisanty (ed.) *Revista de Administración Pública, LIV*(1), 113-148. Recuperado de https://bit.ly/35lTW0J

Camacho Hernández, S. (2019). DNSChain y Namecoin: una mirada a la revolucion del DNS. A. Pisanty (ed.) *Revista de Administración Pública, LIV*(1), 189-208. Recuperado de https://bit.ly/3vDhb0u

Cambronero, F. (2019). Ciberseguridad y la gobernanza multistakeholder. A. Pisanty (ed.) *Revista de Admnistración Pública, LIV*(1), 263-300. Recuperado de https://bit.ly/35lTW0J

Comité de Informática de la Administración Pública Estatal y Municipal (CIAPEM) (2020). *La SCT orienta sobre el mejor uso de las tecnologías de telecomunicaciones y radiodifusión durante la contingencia por el Covid-19.* Recuperado de https://bit.ly/3tlJ2zG

Centro de Ciberseguridad Industrial (CCI) (2021). *Comparativa de Estrategias de Ciberseguridad de Latam.* Madrid: CCI. Recuperado de https://bit.ly/3711CWy

Consejo Nacional de Política Económica y Social, Colombia (CONPES) (2020). *Política Nacional de Confianza y Seguridad Digital.* Bogotá, Colombia: CONPES. Recuperado de https://bit.ly/3pArUVM

DeNardis, Cogburn, Levinson y Musiani (2020). *Researching Internet Governance.* Cambridge, Massachussetts: Massachussetts Institute of Technology.

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security, 4*, 92-100. doi:http://dx.doi.org/10.4236/jis.2013.42011

Durazo Moreno, A. y Secretaría de Seguridad y Protección Ciudadana. (SSPC) (2020). *Informe Anual. Estrategia de Seguridad Pública.* Recuperado de https://bit.ly/34c4v5P

Espinosa García y Morales Luna (2019). Seguridad de la información en instituciones de educación superior de México. A. Pisanty (ed.) *Revista de Administración Pública, LIV*(1), 149-188. Recuperado de https://bit.ly/35lTW0J

Estrada Nava, C. (2021). Atlas de riesgos para la Seguridad Nacional Cibernética de México. A. Pisanty (ed.) *Revista de Administración Pública, LIV*(1), 231-262. Recuperado de https://bit.ly/35lTW0J

FIRST. Improving Security Together. Recuperado de https://bit.ly/35MYhJS

García, A.A. (2018). *Ciberseguridad nacional en México y sus desafíos.* Recuperado de https://bit.ly/3hzQhyC

Gleckman, H. (2018). *Multistakeholder Governance and Democracy. A Global Challenge.* London/New York: Routledge.

Global Cybersecurity Capacity Center (GCSCC). (2016). *Cybersecurity Capacity Maturity Model for Nations (CMM) Revised Edition.* Oxford, UK: Oxford University. Recuperado de https://bit.ly/3sG41ya

Global Cybersecurity Capacity Center (GCSCC) (2016). *Modelo de Madurez de Capacidad de Seguridad Cibernética de Oxford.* Recuperado de https://bit.ly/3MfFk3v

Guel, J.C. (2020-2021). Comunicación personal.

Hanna, N. (2016). *Mastering Digital Transformation: Towards a Smarter Society, Economy, City and Nation.* Bingley, UK: Emerald Publishing. doi:10.1108/S2059-28412016

Harcourt, A., Christou, G. y Simpson, S. (2020). *Global Standard Setting in Internet Governance.* Oxford: Oxford University Press.

International Telecommunications Union (ITU). (2018). *Global Cybersecurity Index 2018.* Geneva: ITU. Recuperado de https://bit.ly/35Pkqar

International Telecommunications Union (ITU). (2021). *Global Cybersecurity Index 2020.* Geneva: ITU. Recuperado de https://bit.ly/3sD1STZ

Kosévich, E. Y. (2019). Estrategias de seguridad cibernética en los países de América Latina. *Iberoamérica Journal, 4*(1), 137-159. doi:10.37656/s20768400-2020-1-07

Leiva, E.A.. (2015). Estrategias Nacionales de Ciberseguridad: Estudio comparativo basado en enfoque top-down desde una visión global a una visión local. *Revista Latinoamericana de Ingeniería de Software, 3*(4), 161-176. doi:https://doi.org/10.18294/relais.2015.161-176

Montes, R. (2020). , 09 11). "SFP elminará ocho áreas por el ajuste a recursos". *Milenio,* 9 de septiembre. Recuperado de https://bit.ly/3Mj2aqX

Moreno, J., Albornoz, M. y Maqueo, S. (2019). Ciberseguridad: estado de la cuestión en América Latina. A. Pisanty (ed.) *Revista de Administración Pública, LIV*(1), 23-46. Recuperado de https://bit.ly/35lTW0J

Organización de los Estados Americanos (OEA) y Banco Interamericano de Desarrollo (BID) (2016). *Ciberseguridad: ¿Estamos preparados en América Latina y el Caribe? Observatorio de la ciberseguridad en América Latina y el Caribe.* Washington, DC: Banco Interamericano de Desarrollo. Recuperado de https://bit.ly/3IH3dPj

Organización de los Estados Americanos (OEA) y Banco Interamericano de Desarrollo (BID) (2020). *Ciberseguridad: riesgos, avances y el camino a seguir en América Latina y el Caribe.* Washington, DC: Banco Interamericano de Desarrollo. Recuperado de https://bit.ly/3CeD7jX

Pisanty Baruch, A.. (2019). Regímenes para la ciberseguridad. A. Pisanty (ed.) *Revista de Administración Pública, LIV*(1), LIV. Recuperado de https://bit.ly/35lTW0J

Pisanty, Baruch, A.. (2020). "Open Internet Governance: The 6F Framework And Covid-19". L. B. al., (ed.) *Medianama*, 21 de mayo. Recuperado de https://bit.ly/3vyEJUF/

Rodríguez Rodríguez, M. (2019). Inteligencia y ciberseguridad nacional. A. Pisanty (ed.) *Revista de Administración Pública, LIV*(1), 79-112. Recuperado de https://bit.ly/35lTW0J

Venegas-Andraca, S. (2019). Tecnología cuántica y Ciberseguridad. A. Pisanty (ed.) *Revista de Administración Pública, LIV*(1), 209-230. Recuperado de https://bit.ly/35lTW0J

Vignettes, M. (2019). Esfera ética del ciberconflicto. A. Pisanty (ed.) *Revista de Administración Pública, LIV*(1), 47-78. Recuperado de https://bit.ly/35lTW0J

CAPÍTULO 07

ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD DESDE UN ENFOQUE DE ECONOMÍA POLÍTICA

CAROLINA AGUERRE*

* CETyS, Universidad de San Andrés y GCR21, Universität Duisburg Essen. Centro de Investigación y Docencia Económicas (CIDE). Centro Latam Digital

La ciberseguridad es un tema complejo en el cual recaen elementos de estabilidad y permanencia de las políticas públicas de los Estados, tanto en materia de provisión de servicios, cada vez más dependientes de las tecnologías digitales, como de garantías de provisión de bienes públicos, como la seguridad y la defensa. Pero la ciberseguridad es también un sector productivo pujante y en crecimiento, valuado en 173 mil millones de dólares, en 2020.[1]

La ciberseguridad es, además, un desafío complejo, que hasta podría entrar dentro de lo que la literatura se conoce como *wicked problems*. Para su abordaje es necesario combinar experiencia y conocimientos en materia de gobernanza, de políticas, aspectos operativos, técnicos y legales.

Si bien en el mundo hace al menos dos décadas que en el nivel global los Estados reconocen los aspectos críticos de seguridad vinculados con la infraestructura de redes y tecnologías digitales, los desafíos aumentan y se hace necesario considerar una respuesta planificada y organizada que permita fortalecer la infraestructura, dotar de capacidades a las organizaciones y entidades responsables, a los afectados por un problema de seguridad digital, y desarrollar habilidades y competencias para las personas responsables y la ciudadanía, entre otros elementos centrales. Estas motivaciones han estado en la base de los fundamentos para el desarrollo de las estrategias nacionales de ciberseguridad. En América Latina y el Caribe el trabajo en esta materia se ha dinamizado desde comienzos de la década de 2010, aunque aún hay mucho camino por recorrer en materia de desarrollo de políticas, pero sobre todo, en cuanto a su instrumentación.

Este documento tiene como objetivo analizar el papel de las estrategias nacionales de ciberseguridad desde una perspectiva de la economía política. Este abordaje permite identificar elementos críticos vinculados con la motivación para la formulación y puesta en práctica de las estrategias nacionales sobre el tema y las relaciones entre los actores. Específicamente se toma en cuenta el contexto de América Latina y el Caribe para situar la discusión del desarrollo de dichas estrategias en la región, pero en clave comparada con países más desarrollados, particularmente europeos, donde además existen más estudios sobre la temática, documentos con más años de existencia.

La primera parte del trabajo aborda los aspectos conceptuales de la ciberseguridad desde una perspectiva de la economía política. En segundo lugar se examinan las estrategias nacionales de ciberseguridad en la discusión internacional. La tercera parte se aboca a los elementos de política industrial en materia de ciberseguridad en tanto apunta al papel del Estado en la conformación de un entorno para las reglas de juego con los actores del sector privado. Luego se analizan algunas dimensiones de las estrategias nacionales en perspectiva comparada en la región, tomando en cuenta dimensiones de gobernanza y de su evaluación con indicadores externos desarrollados por el BID/OEA (2020) y el índice global de ciberseguridad (GCI en adelante) de la Unión Internacional de Telecomunicaciones (por sus siglas en inglés, ITU, 2018). Finalmente, se elaboran comentarios sobre los hallazgos y el papel que cumplen las estrategias nacionales para el desarrollo de la práctica de la ciberseguridad en la región.

ASPECTOS CONCEPTUALES DE LA ECONOMÍA POLÍTICA DE LA CIBERSEGURIDAD EN PERSPECTIVA DE GOBERNANZA

Existen pocos conceptos tan ambiguos en el campo de la política digital como el de ciberseguridad. En particular, porque el término también se elabora sobre ámbitos polisémicos como es el de las tecnologías digitales –de por sí variadas y de propósitos generales– y porque la noción de seguridad depende de su objeto y ámbito de aplicación. De hecho, existen diversas formas incluso de escribir este concepto (Cambronero, 2019), pero siguiendo a diversos autores (Creese *et al.*, 2020; Klimburg, 2017) y las referencias adoptadas por distintos organismos internacionales (BID/OEA, 2020),

1 Según reporte de Forbes (2020), en el cual, además, se prevé que el valor de la industria aumente a 270 mil millones de dólares para 2026.

se tomará la definición de ciberseguridad provista por el Sector de Normalización de las Telecomunicaciones de la Unión Internacional de las Telecomunicaciones (UIT), expresada en la recomendación UIT-TX.1205 y adoptada en la Resolución 181 en noviembre de 2010: "El conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciber entorno".

De acuerdo con esta conceptualización, la seguridad incluye una o más de las siguientes propiedades: disponibilidad, integridad y confidencialidad. Esta caracterización comienza a esbozar la multiplicidad de requisitos que subyacen al efectivo cumplimiento de la ciberseguridad.

A esta diversidad, se le suma el fenómeno del cibercrimen, que ha adquirido cierta predominancia en los discursos sobre ciberseguridad, generando una suerte de equivalencia entre ambos enfoques, aun cuando el cibercrimen es mucho más específico. Esta doble característica, la polisemia y la atribución de una parte (el cibercrimen) por el complejo de actividades en juego, plantean una dificultad específica en la elaboración de políticas integrales en la materia, pero sobre todo, en la producción de marcos analíticos adecuados para abordar el desarrollo de políticas públicas sobre la ciberseguridad (y sus conceptos afines) (Bustos y Aguerre, 2019).

La economía política es una perspectiva analítica sustentada en diversas teorías, liberales, marxistas, institucionales, entre otras, y es practicada en distintos ámbitos disciplinares. El abordaje que se le dará a la economía política en este trabajo parte de una perspectiva amplia, desde las ciencias sociales, enfocada en las relaciones entre actores para la producción de bienes y servicios, incluyendo bienes públicos, como es la seguridad y la defensa pública. Esta perspectiva también posibilita ahondar en las relaciones entre política (de Estados) y mercados (Strange, 2015), las dos fuerzas imperantes en materia de orden normativo que legitima prácticas y conocimiento sobre este tema.

La ciberseguridad es un problema que se encuentra atravesado (y que atraviesa) por intereses económicos y políticos, se encuentran imbricados, pues asuntos de índole geopolítica también interpelan

a los actores de la industria. Por ello la ciberseguridad es también un problema de gobernanza global, en tanto, aun si un Estado logra desarrollar capacidades defensivas y ofensivas, la seguridad no se encuentra garantizada cuando estas amenazas provienen del exterior de la jurisdicción sobre la cual se tiene competencia, como sucede en muchos casos. Ya desde el año 2004 desde la Asamblea General de la ONU se han desarrollado discusiones específicas en esta materia en el Governmental Experts Group y en el Open Ended Working Group (este último espacio fue promovido a fines de 2018). Si bien no se han registrado avances sustantivos en materia de generación de normas para el comportamiento responsable de los Estados en el ciberespacio, desde la adopción por unanimidad en la Asamblea General de la Organización de Naciones Unidas (ONU), en diciembre de 2015, se reconoce la necesidad de aplicar las normas del derecho internacional a este campo, aunque aún resta por avanzar en los aspectos más específicos y problemáticos de su aplicación. De esta manera, la cooperación internacional en materia de ciberseguridad es uno de los grandes retos contemporáneos, tanto para Estados, como para los actores del mercado.

La ciberseguridad es un problema de gobernanza que implica a distintos actores, también conocido como fenómeno *multistakeholder*. La aplicación de la ciberseguridad recae no sólo en los gobiernos, sino que también depende de la práctica de los actores corporativos, así como de los individuos. Antes de la expansión de Internet, el Estado era el que debía contrarrestar las amenazas a la seguridad en ese ámbito, sin embargo, la idea de un único responsable por la seguridad en el ciberespacio es obsoleta por las propias reglas de diseño y funcionamiento de las redes de comunicaciones digitales, como ya se mencionó en el apartado anterior. Se requiere la colaboración de la industria y la sociedad civil para que el Estado mejore y mantenga dicha seguridad. La Comisión Europea (2013: 4) afirmó en su estrategia de seguridad cibernética que "todos los agentes pertinentes, ya sean las autoridades públicas, el sector privado o los ciudadanos individuales, deben reconocer esta responsabilidad compartida [y] adoptar medidas para protegerse". Esta cualidad lleva a la discusión a sus múltiples partes interesadas y los vínculos y distancias entre distintos modelos de gobernanza y con participación de diferentes tipos de actores. La influencia de los debates sobre

los modelos de gobernanza *multistakeholder* de Internet sobre este ámbito se encuentran cada vez más presentes (Cambronero, 2019) y han formulado algunas recomendaciones esenciales para promover estrategias de colaboración entre los actores que fomenten la integridad de los protocolos y la infraestructura crítica de Internet,[2] como una forma de evitar los problemas asociados con la fragmentación de la red de redes.

El fenómeno del ciberespacio vinculado al rápido crecimiento de la conectividad a las redes de comunicaciones y el ascenso del modelo de gobernanza *multistakeholder* como opción cada vez más aceptable para los temas digitales han puesto en tela de juicio, intencionalmente, pero también involuntariamente, si las entidades organizadas, como el Estado, son capaces de hacer frente al ciberespacio dominado por el sector privado. Desde la perspectiva de la estructuración (Giddens, 1989), los Estados son estructuras institucionalizadas, formadas con dichos principios, y esto implica que están pensados como entidades estables a través del tiempo y el espacio. El fenómeno de la estructuración, aplicado por la sociología de la tecnología reconoce a esta última como producto y medio de la acción humana; pero también incorpora a las condiciones institucionales de la interacción con la tecnología y, las consecuencias institucionales de la interacción con la tecnología (Orlikowski en Bryant, 1999). De ahí que, el Estado debe adaptarse tanto a nuevos retos, pero también a nuevos modelos de gobierno en este ámbito (Hurel, 2016).

Si bien el sistema de ciberseguridad está atravesado por interdependencias entre factores de nivel personal y sistémico, al encontrarse en un sistema descentralizado y abierto como Internet, se vuelve un problema aún más complejo. Los mecanismos de coordinación entre actores no pueden ser garantizados, por lo que las estrategias nacionales de ciberseguridad cumplen un papel importante, en tanto brindan puntos de contacto y guían los procesos entre los actores y sus distintas agendas. También como factor de desarrollo de capacidades y de una agenda local. Desde una perspectiva del desarrollo, es necesario un involucramiento y participación activa de la ciudadanía en la evolución de las políticas públicas, y aún más en esferas intensivas de conocimiento (Stiglitz, 2002), como es el caso de la ciberseguridad.

Aunque la ciberseguridad es un problema que requiere de conocimiento, este se encuentra distribuido entre actores públicos y privados y no está sujeto a un único centro de control o autoridad. A su vez, sus aristas no se encuentran consensuadas ni articuladas. Por ello, múltiples abordajes de gobernanza de la ciberseguridad, en sus distintos niveles, apuntan a medidas que comprenden ámbitos de coordinación (como los centros de respuestas ante incidentes informáticos; de formación (escuelas, academias, organismos internacionales) y normativos en distintos niveles (nacionales, internacionales) y capacidades en materia de aplicación de normas y leyes, pero también de definición de lo que es aceptable o correcto en dichos ámbitos. Esto implica reconocer que hay una legitimidad basada en estas formas de ordenar el problema que se sustentan en un conocimiento que crecientemente se codifica en forma de regulaciones (Haggart, 2019).

TRAYECTORIAS DE LAS ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD

Las motivaciones para priorizar una agenda de ciberseguridad en el nivel nacional se sostienen en dos grandes pilares: *i)* el reconocimiento del papel central de las TIC para el tejido productivo y social contemporáneo; *ii)* el aumento de los ciberataques y el ciberdelito en un contexto de repliegue de actividades en el espacio público físico (ITU, 2018b; OCDE, 2012; BID/OEA, 2020). El espacio público virtual es el de la esfera pública contemporánea, lo cual quedó demostrado durante la pandemia de Covid-19. Sumado a esos dos objetivos, uno de los principales desafíos de las políticas de seguridad en el entorno digital es perseguir y preservar la apertura de la Internet como plataforma para la innovación y las nuevas fuentes de crecimiento (OCDE, 2012).

2 Este es el caso, por ejemplo, de la Global Commission for the Security and Stability of Cyberspace y su propuesta de normas para el comportamiento responsable de los Estados en el ciberespacio, y constituye una de las respuestas de un ámbito no gubernamental ante el asunto.

El índice global de cooperación para la ciberseguridad de la UIT hace referencia a aspectos centrales de la coordinación entre niveles de actores, tanto en los niveles nacional, como regional y global. Es relevante detenerse en los componentes de este indicador, no sólo por su relevancia normativa en materia de estándares de ciberseguridad, sino también porque el marco elabora medidas de cooperación entre actores contemplando cinco dimensiones: legal, técnica, organizacional, desarrollo de capacidades y cooperación.

Las estrategias nacionales de ciberseguridad se encuentran comprendidas dentro del pilar organizacional, el cual atiende la instrumentación de toda iniciativa nacional, lo que necesariamente incluye la presencia de agencias públicas. La evaluación del índice sobre este pilar ve que el desarrollo de la estrategia nacional, con un modelo de gobernanza para la ciberseguridad y un organismo supervisor, dan rumbo a los esfuerzos de los distintos sectores que deben estar alineados en el desarrollo de la ciberseguridad. Este índice evalúa la presencia de estrategias e instituciones en el nivel nacional, no ya su instauración, que constituye un ámbito crítico.

Asimismo, la estrategia nacional en la materia es incluida dentro de las dimensiones organizacionales en el GCI 2018 de la UIT. ¿Cuáles son las implicaciones de dicha conceptualización desde una perspectiva de economía política?

Para este índice, las medidas organizativas son indispensables para la correcta instrumentación de cualquier iniciativa. El Estado nacional debe establecer objetivos estratégicos amplios y metas, junto con un plan integral en la instauración, entrega y medición. Los organismos nacionales deben estar presentes para aplicar la estrategia y evaluar los resultados. Sin una estrategia nacional, un modelo de gobernanza y un organismo de supervisión, los esfuerzos de los diferentes sectores entran en conflicto, impidiendo que se obtenga una armonización en el desarrollo de la ciberseguridad. Las estructuras organizativas se evalúan en función de la presencia de instituciones y estrategias que implican el desarrollo de la ciberseguridad en el nivel nacional (UIT, 2018: 11).

Además, la UIT ha desarrollado un manual para el desarrollo de estrategias nacionales de ciberseguridad que es relevante en cuanto a la precisión del alcance de una estrategia, ya que esta puede adoptar variadas formas y adquirir diversos niveles de detalle, dependiendo de los objetivos y niveles del país en particular de la preparación cibernética. En tanto no exista un marco común para la definición de los parámetros de una estrategia nacional de ciberseguridad, este documento de la UIT toma en consideración que la misma se conforma por tres componentes: *i)* una expresión de la visión, los objetivos de alto nivel, los principios y las prioridades que guian a un país en el tratamiento de la ciberseguridad; *ii)* una visión general de las partes interesadas y encargados de mejorar dicha seguridad en la nación y sus respectivos papeles y responsabilidades; y *iii)* una descripción de las medidas, programas e iniciativas con que un país se compromete a proteger su ciberinfraestructura nacional y, en el proceso, aumentar su seguridad y resistencia.

Por otra parte la Agencia Europea de Seguridad de las Redes y de la Información (ENISA, por sus siglas en inglés) propone un marco para evaluar una estrategia de ciberseguridad, basado en los siguientes aspectos: 1) desarrollar políticas y capacidades de ciberdefensa; 2) lograr la ciberresiliencia; 3) reducir la ciberdelincuencia; 4) apoyar a la industria en materia de ciberseguridad; 5) asegurar las infraestructuras de información críticas (ENISA, 2012).

Evolución y características de la primera generación de estrategias

Desde una perspectiva cronológica, las primeras estrategias nacionales de ciberseguridad se desarrollaron principalmente en países de Europa, donde para comienzos de la década de 2010 la mayoría ya tenía algún plan, incluyendo naciones como India y Japón. Estados Unidos fue, sin embargo, el precursor con la publicación de su primera estrategia en 2003. A continuación, se extraen algunas dimensiones clave de estos documentos en términos de economía política, es decir, atendiendo fundamentalmente a las relaciones entre actores (internos y externos), como también los principios orientadores de las mismas.

A comienzos del nuevo milenio era prácticamente un puñado de países muy desarrollados los que comenzaban a desarrollar un trabajo articulado en torno a una estrategia de ciberseguridad, como Estados Unidos, Israel, Estonia. En 2012, treinta años más tarde de la primera publicación de las directrices de seguridad de la información de la OCDE de 1992, este organismo realizó un análisis comparativo

de una nueva generación de estrategias nacionales de seguridad cibernética en diez países de esa alianza. El trabajo de 2012 reveló que la formulación de políticas en la materia se encontraba en un punto de inflexión, en tanto se había jerarquizado políticamente el tema, y se apoyaba en un liderazgo más firme. Esas estrategias adoptaron en la última década un tono más "holístico", contemplando aspectos económicos, sociales, educativos, jurídicos, de aplicación de la ley, técnicos, diplomáticos, militares y relacionados con la inteligencia. Los planes de acción refuerzan la investigación y desarrollo (I+D) de la ciberseguridad y la supervisión en tiempo real de las infraestructuras gubernamentales. Tienen por objeto desarrollar un sector industrial en la materia más sólido y aprovechar los motores económicos y los incentivos; identifican los actores o sectores empresariales críticos para la economía; crean asociaciones con los proveedores de servicios de Internet y fomentan los ejercicios de ciberseguridad a la vez que la protección de personas vulnerables, en particular los menores. El informe además señala que las "consideraciones de soberanía" han adquirido cada vez más importancia. Este elemento es central para una discusión sobre los incentivos políticos que pueden estar subyacentes a una estrategia doméstica y la preocupación por proteger el espacio nacional.

Un factor que también señala el informe de la OCDE (2012) respecto de la primera generación de estrategias nacionales de ciberseguridad es el desafío de la preparación contra los ataques cibernéticos mediante estrategias, pero con posiciones que no sean contrarias al principio de apertura de Internet, un aspecto fundamental para la robustez de la economía digital. A la fecha, la mayoría de los países del mundo han desarrollado capacidades defensivas en la materia, más que ofensivas. Para este último aspecto es básico reconocer que aún hay poca información y los instrumentos de atribución de un ciberataque son aún fragmentados y poco transparentes.

Las estrategias de ciberseguridad tienen por objeto mejorar la coordinación gubernamental en los planos normativo y operacional, y aclarar las funciones y responsabilidades. Refuerzan la cooperación entre los sectores público y privado, incluso algunas de ellas creando las condiciones para un diálogo entre múltiples partes interesadas en el proceso de elaboración y aplicación de las políticas en

la materia. También hacen hincapié en la necesidad de respetar valores y derechos fundamentales, como la privacidad, la libertad de expresión y la libre circulación de la información. También instan a una mayor cooperación internacional. Algunas estrategias también apoyan enfoques políticos más flexibles y ágiles, y hacen hincapié en la dimensión económica de la política de ciberseguridad (OCDE, 2012).

El estudio de Luiijf *et al.* (2013), en su análisis de 19 estrategias nacionales, señala que los objetivos están orientados al cumplimiento de al menos alguno de los tres más grandes: *1)* promover un alineamiento dentro del gobierno; *2)* fomentar la coordinación y foco en la planificación público-privada y el desarrollo de papeles, responsabilidades y relaciones entre actores; *3)* transmitir la intención nacional a otros Estados y partes interesadas.

Algunos de los elementos comunes de las estrategias nacionales de ciberseguridad comparten las siguientes características (Luiijf *et al.* 2013; OCDE, 2012):

1. Una mayor coordinación gubernamental en los niveles político y operacional, el enfoque interinstitucional. A medida que la ciberseguridad se convierte en una cuestión de prioridad nacional, la responsabilidad de la elaboración y aplicación de la política de ciberseguridad se asigna claramente dentro del gobierno. Se destaca la necesidad fundamental de coordinación entre los organismos pertinentes –y esta se asigna generalmente a un organismo específico o nuevo–, y también la responsabilidad de los demás órganos gubernamentales implicados, para facilitar la cooperación, fomentar las sinergias, evitar la duplicación y poner en común las iniciativas. Se destaca que la evolución de un enfoque multiinstitucional a uno interinstitucional requiere un liderazgo sólido para permitir la coordinación y la cooperación entre los silos gubernamentales preexistentes. Existen variaciones entre los tipos de acuerdos específicos –que varían de un país a otro– y reflejan las culturas y estilos de gobierno.
2. Refuerzo de la cooperación entre los sectores público y privado. Las estrategias analizadas reconocen que el ciberespacio pertenece y es operado en gran medida por el sector privado y que los usuarios también desempeñan un papel clave. Reconocen que las políticas deben basarse en asociaciones público-privadas

inclusivas, que pueden incluir a las empresas, la sociedad civil, la comunidad técnica de Internet y el mundo académico. Sin embargo, las modalidades de esas consultas y el nivel de detalle de las estrategias varían.

3. Mejora de la cooperación internacional. La mayoría de las estrategias comparten como objetivos clave la cooperación internacional y la necesidad de mejorar las alianzas y asociaciones con países o aliados de ideas afines, incluida la facilitación de la creación de capacidad de los países menos adelantados. Sin embargo, muchos países proporcionan pocos detalles sobre la forma de lograr mayor cooperación internacional. Se señala la necesidad de un alto grado de armonización de la legislación contra el delito cibernético, generalmente en apoyo del Convenio de Budapest, de 2001, el cual ha sido ratificado por varios países de América Latina, incluyendo a México.
4. Respeto de los valores fundamentales: las estrategias hacen hincapié en la necesidad de que la política de seguridad cibernética respete los valores fundamentales, que generalmente incluyen la privacidad, la libertad de expresión y la libre circulación de la información. Varias estrategias mencionan explícitamente la necesidad de mantener la apertura de la Internet y ninguna estrategia sugiere modificarla en favor del fortalecimiento de la ciberseguridad. Por el contrario, la apertura de la red se describe en general como un requisito para su desarrollo ulterior económico.

POLÍTICA INDUSTRIAL DE LA CIBERSEGURIDAD

La política industrial es una perspectiva plausible para el análisis de las estrategias nacionales de ciberseguridad desde un enfoque de economía política. Aunque la práctica de las normas industriales en el mercado de la ciberseguridad sigue siendo incipiente, como se verá más adelante en el apartado de estrategias nacionales en América Latina y el Caribe, la literatura en esta materia ofrece diversas explicaciones de las fuerzas que impulsan la variación de las opciones entre los gobiernos (Aggarwal y Evenett, 2013). Por ejemplo, mientras que Beijing utiliza un modelo de capitalismo deliberado dirigido por el Estado, Japón promueve el desarrollo del mercado de la seguridad cibernética impulsado por el sector privado. Entre las democracias de occidente hay una variación considerable en cuanto a la forma en que los países aplican y ponen en práctica políticas que reflejan su tipo de régimen, política burocrática, geopolítica y ubicación en la escala de desarrollo (Aggarwal y Reddie, 2018).

Las políticas industriales en materia de ciberseguridad se han construido a la sombra de las relaciones entre el Estado y la sociedad, en las que diversos organismos gubernamentales elaboran y aplican normas en el marco de la política burocrática, con la aportación y los desafíos de los agentes sociales, incluidos los trabajadores, los consumidores, los grupos de interés y las empresas de tecnología de la información. La variación de los tipos de política industrial empleados por los distintos gobiernos refleja, en cierta medida, las relaciones distintivas entre el Estado y la sociedad en cada país (Aggarwal y Reddie, 2018).

El trabajo de estos autores destaca que existe una variación considerable en la forma en que los gobiernos han tratado de fomentar la inversión en el sector privado de la ciberseguridad en lo que se refiere al capital humano, la reglamentación y la respuesta al cabildeo de las empresas. Parte de una categorización de estas comprende: *1)* las de seguridad cibernética; *2)* las de tecnología de Internet y *3)* las adyacentes a Internet.

La primera categoría incluye las compañías que trabajan directamente en los desafíos relacionados con la seguridad cibernética para clientes comerciales y/o gubernamentales. Su función abarca desde la creación de productos relacionados con dicha seguridad hasta la protección de las redes, pasando por la consultoría sobre conocimientos básicos de seguridad en la materia para los empleados, la realización de evaluaciones de las amenazas y el seguimiento de los ciberataques y los piratas informáticos. Ejemplos de este tipo de empresas son Darktrace, FireEye, Palantir, Qadium y Kaspersky Lab.

En segundo lugar, el estudio identifica a las compañías de tecnología de Internet que dependen de la ciberseguridad (proporcionada por empresas externas y por equipos internos) para proteger sus operaciones y productos, pero que no participan en el mercado en sí. Entre los ejemplos de este tipo de empresas se

incluyen las que trabajan en lo que a menudo se denomina el "gran espacio de datos", como Alphabet, Facebook y Yahoo, para vender productos, así como los fabricantes de hardware, como intel, Qualcomm, Microsoft, Apple e IBM, que requieren protección contra las infracciones relacionadas con sus proyectos de investigación y desarrollo más recientes y para mantener sus productos a salvo de los ataques cibernéticos.

Por último, hay empresas adyacentes a la red, cuyos productos tienen componentes basados en Internet pero que tienen intereses comerciales fundamentales fuera del sector tecnológico. Los autores señalan aquí a las compañías que trabajan en la Internet de las cosas (IoT), como General Electric, Kenmore y PG&E, así como espacios comerciales que usan la red para vender bienes del "mundo real", como los grandes supermercados, son ejemplos de este tipo de firmas. Todas las empresas dependen cada vez más de la Internet como un mercado para conocer a los clientes, llevar a cabo la logística y hacer un seguimiento de los datos de los consumidores. Todas estas compañías de diferentes industrias y países se enfrentan a los retos que plantea la inseguridad cibernética y la aparente falta de seguridad. Cada tipo de empresa también desarrolla distintos vínculos y formas de interacción con un gobierno, que van desde peticiones de protección, hasta el cabildeo.

Comprender los tipos de firmas de cada nivel es un ejercicio útil para conceptualizar los intereses que aportan al espacio temático, así como para estudiar cómo pueden considerarlos los agentes gubernamentales en cada contexto nacional. También es relevante para examinar qué tipos de agentes podrían aprovechar el poder de los grupos de presión en relación con las demandas de intervención estatal. Si bien los países de América Latina no han desarrollado grandes compañías internacionales en esta materia, la cadena de valor de la seguridad digital permite identificar, o no, actores locales en cada uno de los tres niveles ubicados, proporcionando servicios al Estado, empresas y ciudadanos de los países y muchas veces fuera de ellos. La presencia, ausencia y diversidad de estos actores locales en cada contexto nacional de la región de América Latina y el Caribe agrega un componente más por tener en cuenta en materia de las consideraciones y alcances de las estrategias nacionales de ciberseguridad.

CARACTERÍSTICAS REGIONALES EN MATERIA DE ESTRATEGIAS NACIONALES DE CIBERSEGURIDAD

A partir de las consideraciones realizadas por los diversos aportes de la literatura que han relevado prácticas, desarrollado horizontes normativos y descrito el entorno económico del sector y sus relaciones con los actores públicos en distintos contextos, a continuación se desarrollará un análisis de las estrategias de ciberseguridad regionales con base en estas categorías.

Para el caso de la región de América Latina y el Caribe (ALC), el informe del Banco Intermaricano de Desarrollo y la Organización de Estados Americanos (BID/OEA, 2020) Riesgos y Avances y el Camino a seguir en América Latina y el Caribe", destaca que hay 12 países que ya aprobaron estrategias nacionales de ciberseguridad: Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, Jamaica, México, Panamá, Paraguay, República Dominicana, y Trinidad y Tobago, y varios otros en progreso.[3] Es relevante destacar que se toma en cuenta este informe por el papel preponderante que ha desarrollado la OEA en la región durante la última década en la promoción de capacidades en la materia, incluyendo el respaldo para el desarrollo de los documentos de dichas estrategias nacionales, fundamentalmente con actores públicos. Este estudio además analiza los niveles de madurez de capacidad en ciberseguridad siguiendo el Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM por sus siglas en inglés), una metodología desarrollada por el Centro Global de Capacidad en Seguridad Cibernética (GCSCC, por sus siglas en inglés) de la Universidad de Oxford.

3 En septiembre de 2020 Nicaragua publicó su primera estrategia nacional de ciberseguridad mediante decreto presidencial para el periodo 2020-2025. El estudio BID/OEA (2020) señala al momento de la publicación de su reporte que los otros países de la región que se encuentran en proceso de desarrollo de dicha estrategia son: Perú, Ecuador, Suriname, Guyana, Barbados y Belice.

PAÍSES DE LA REGIÓN CON ESTRATEGIAS Y RANKING EN EL ÍNDICE DE PREPARACIÓN EN CIBERSEGURIDAD

CUADRO 01.

* Para la calificación en alguna de las cinco etapas de madurez elaboradas por este índice, la autora tomó las calificaciones de los tres subindicadores correspondientes a la Estrategia Nacional de Seguridad Cibernética elaboradas por este estudio (desarrollo de la estrategia, organización y contenido) para promediar la inclusión en una de las etapas ya que dicho estudio no promedia por indicador.

Países con documento de estrategia nacional de ciberseguridad BID/OEA (2020)	Autoridad(es)	Creación de Agencia Especializada para seguimiento	Intencionalidad de una política industrial nacional	Intencionalidad de una política industrial nacional	Nivel de desarrollo de la estrategia nacional de seguridad cibernética BID/OEA (2020)*	Posición en el índice de ciberseguridad de la UIT (2018)
Argentina	Secretaría de Modernización	Dirección Nacional de Ciberseguridad	Sí	Sí	Formativa	94
Brasil	Presidencia	Comitê Gestor da Segurança da Informação	No	Sí	Formativa	70
Chile	Presidencia-SENATIC	Comité Interministerial para la ciberseguridad	No	Sí	Consolidada	83
Colombia	CONPES	Comisión Intersectorial	No	Sí	Estratégica	73
Costa Rica	MICITT	Comité Consultivo para la Ciberseguridad	Sí	No	Consolidada	115
Guatemala	Ministerio de la Gobernación	Comité Nacional de Seguridad Cibernética	SD	No	Consolidada	112
Jamaica	Gobierno nacional	No	No	No	Consolidada	94
México	Comisión Intersecretarial para el Desarrollo del Gobierno Electrónico	Subcomisión de Seguridad del CIDGE	Sí	Sí	Consolidada	63
Panamá	Autoridad Nacional para la Innovación Gubernamental	CSIRT	Sí	No	Consolidada	97
Paraguay	Presidencia-SENATIC	Comisión Nacional de Ciberseguridad	SD	No	Consolidada	66
República Dominicana	Presidencia INDOTEL	Centro Nacional de Ciberseguridad	SD	No	Consolidada	92
Trinidad y Tobago	Gobierno nacional	TTCSA	Sí	No	Consolidada	123

El estudio concibe cinco etapas de madurez: la inicial, cuando recién son incipientes las discusiones en esta materia en el ámbito nacional; formativa, cuando hay algunos aspectos que han comenzado a definirse; consolidada, cuando hay indicadores instalados y funcionando, aunque no se le ha dado consideración especial a los recursos por asignar; estratégica cuando ya hay una elaboración específica del Estado y las organizaciones sobre las elecciones más relevantes para ese contexto, y por último, la etapa dinámica, en la cual existen mecanismos para adaptar las estrategias considerando el entorno y las tecnologías cambiantes. El índice, a su vez contiene cinco dimensiones: *i)* política y estrategia de seguridad cibernética; *ii)* cultura cibernética y sociedad; *iii)* formación, capacitación y habilidades de seguridad cibernética; *iv)* marcos legales y regulatorios; *v)* estándares, organizaciones y tecnologías. Las estrategias (denominadas en este estudio Estrategia Nacional de Seguridad Cibernética) se encuentran ubicadas como el primer indicador dentro de la primera dimensión. Como se analizará a continuación, la existencia de una estrategia nacional no necesariamente implica haber alcanzado una madurez y capacidad máxima, es solamente uno más de los múltiples niveles y aspectos que conlleva la gobernanza de la ciberseguridad.

El cuadro 01 sistematiza las estrategias nacionales de ciberseguridad en la región tomando en cuenta diversas dimensiones de la literatura analizada en una síntesis propia que permite capturar algunos de los elementos salientes en clave de economía política comparada.

En primer lugar, es importante señalar que las estrategias aquí consignadas se basan en el estudio de BID/OEA (2020) para la región de ALC y no se han tomado en cuenta avances recientes, como el decretado en septiembre de 2020 por la presidencia de Nicaragua. El informe BID/OEA (2020) consideró a Nicaragua con el nivel más bajo (inicial) en materia de desarrollo de la estrategia nacional de seguridad cibernética, pero a seis meses de esa edición, el gobierno de Daniel Ortega publicó su estrategia mediante decreto presidencial. Las condiciones para dar curso a dicha estrategia en su país cambiaron abruptamente y esto es en parte posible por las características autoritarias del actual régimen político de esa nación. Este ejemplo da cuenta de que la formulación objetiva de una estrategia nacional de ciberseguridad puede darse sin las connotaciones de gobernanza desarrolladas anteriormente en otras secciones de este capítulo. Sin embargo, desde una perspectiva de economía política, subraya las relaciones existentes entre la estrategia misma y sus características *top down*, con ausencia de diálogo y participación de otros sectores.

FUENTE:

(en pág. anterior) elaboración propia con base en BID/OEA (2020) Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y el Caribe, y en el análisis documental de las estrategias nacionales y documentos de soporte oficiales.

Con base en el estudio BID/OEA (2020), es importante destacar que no existe una metodología uniforme para la consideración de lo que constituye un comportamiento "estratégico" en la materia. Se puede observar una variación en los criterios establecidos por el BID/OEA, basados en la metodología CMM, y los criterios de la UIT, que son más amplios, y a partir de los cuales una estrategia de ciberseguridad para la administración pública nacional (como es el caso de Uruguay), es considerado un "enfoque nacional".

En segundo lugar, se puede observar que el modo, en tanto año de prevalencia de promulgación de las estrategias es 2018, siendo Colombia el primer país en la región en desarrollar un documento con tales características en 2011. Esto supone un rezago (de unos cuatro en promedio) con respecto a la mayoría de las estrategias nacionales de ciberseguridad publicadas en países europeos. Si bien los gobiernos de la región de América Latina y el Caribe son conscientes de la necesidad de proteger el espacio digital para el funcionamiento de la sociedad, la ciberseguridad no ha ganado presencia en la agenda política de la región con la urgencia que se esperaría. Como señalan BID/OEA (2020), solamente 12 países habían aprobado una estrategia nacional en la materia (un aumento considerable con respecto a los cinco que sí las tenían en 2016), y únicamente diez naciones han establecido un organismo gubernamental central responsable de la gestión de la ciberseguridad (BID, 2020). Este avance tan tímido se debe primordialmente a la ausencia de talento humano calificado, en el que la brecha de profesionales en ciberseguridad se estima en 600 000 personas en la región. Y aun frente a esta escasez, únicamente 20 de los países estudiados cuentan con alguna oferta académica en ciberseguridad (BID/OEA (2020).

En tercer lugar, se destaca el papel preponderante de la presidencia y oficinas/secretarias aledañas de los poderes ejecutivos

de los gobiernos nacionales en esta materia, seguidas de secretarías vinculadas a la gestión pública y la modernización del Estado, y finalmente la inclusión de los ministerios y secretarías vinculadas con las tecnologías de la información y la comunicación (TIC). En relación con la autoridad que lo impulsa y promueve, en prácticamente todos los casos donde las estrategias nacionales se han comenzado a instaurar (la excepción es Jamaica, donde el documento no ha sido acompañado por acciones concretas), se han creado agencias, centros o comisiones especializadas que promueven la coordinación e impulsan la transversalidad del asunto en los distintos niveles y actores de gobierno involucrados, en línea con las dimensiones destacadas anteriormente (OCDE, 2012). En este aspecto también emergen algunos rasgos distintivos de cada contexto nacional vinculados con la capacidad de articulación con el sector privado. En particular, la existencia en algunos países de diversos equipos de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) controlados por el sector privado, además del CSIRT o equipo de respuesta (o preparación) para emergencias informáticas (CERT, por sus siglas en inglés) nacional que poseen todos los países de esta lista, constituye un espacio concreto de trabajo en materia de coordinación y de mitigación ante incidentes en las redes.

Otro aspecto relevante desde la perspectiva de los distintos vínculos entre los actores, es que la mayoría de las estrategias nacionales de ciberseguridad en la región y sus mecanismos de gobernanza no contaron con un mecanismo formal de participación de actores no gubernamentales en la elaboración de la estrategia, ni en la consulta previa ni en una fase posterior de validación. Si bien queda fuera del alcance de este trabajo realizar un análisis y descripción pormenorizado de cada contexto donde se desplegó la estrategia, es relevante aclarar que en trabajos previos (Bustos y Aguerre, 2020; Hurel, 2020) se consignan estos vínculos informales existentes entre los actores nacionales, tanto públicos, como privados, en lo que respecta a los aspectos de instrumentación y coordinación para la mitigación y fortalecimiento. Otros trabajos señalan estos elementos de cooperación formal-informal entre los sectores ante los incidentes informáticos (Bradshaw, 2015).

Uno de los casos excepcionales en la región en materia de participación *multistakeholder* en la elaboración de la estrategia es México:

> En México, el Gobierno de la República, en su rol de facilitador, promovió espacios de diálogo, discusión y aprendizaje mediante foros y talleres en un proceso de colaboración denominado "Hacia una Estrategia Nacional de Ciberseguridad" de marzo a octubre de 2017. En estos espacios, los distintos actores de la sociedad compartieron ideas, inquietudes y propuestas en materia de ciberseguridad que arrojaron grandes coincidencias sobre las necesidades que debía atender la Estrategia (Gobierno de México, 2017: 3).

Otros casos como Panamá y Trinidad Tobago contaron con la participación formal de actores no gubernamentales en la etapa de consulta. El de Costa Rica es relevante en tanto el seguimiento e instauración se realiza con el mecanismo del Comité Consultivo para la Ciberseguridad, convocado por el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT), en el que además de distintos organismos de gobierno se invitó al sector privado, la academia y la sociedad civil.

En cuanto a la consideración de la aplicación de alguna forma de política industrial en materia de ciberseguridad, de las estrategias nacionales no se desprenden políticas integrales de las mismas, como las consignadas al comienzo del capítulo, aunque sí se presentan intenciones de promoción del sector nacional en la provisión de servicios, por ejemplo, como es el caso de Colombia, en la adecuación de su plan estratégico en 2020, o Argentina, que promueve "Impulsar el desarrollo de la industria de ciberseguridad nacional" (PEN, 2019: 7). Asimismo, otros planes contienen un lenguaje más específico, como el de Chile: "Realizar estudios tanto de caracterización de la industria de ciberseguridad (oferta), como de acceso y uso de ciberseguridad en el país (demanda), con el objeto de orientar programas especiales para impulsar la industria de ciberseguridad nacional, en sectores definidos" (Gobierno de Chile, (2017: 21). Estos términos sugieren, por un lado, la caracterización incipiente del sector y los estadios preliminares en la definición de una política

específica de promoción sectorial –más allá que existen empresas nacionales que proveen servicios en esta materia hace años–. Las estrategias tampoco llegan a brindar especificaciones de los distintos niveles de empresas vinculadas al sector en cada país.

La mayoría de los casos de la región que poseen una estrategia tienen un grado de desarrollo del segundo nivel inferior catalogado como "consolidado" por la metodología de CMM BID/OEA (2020), lo que implica que, aun contando con el instrumento, falta un abordaje profundo en materia de desarrollo, organización y contenidos de la misma. Un caso excepcional es el de Colombia, que ya tiene una década de oficialización de su primera estrategia y ha logrado el nivel más alto en la región en este indicador.

Finalmente, desde el punto de vista del índice de ciberseguridad de la UIT (2018), los países de todas las Américas, con excepción de Estados Unidos (posición 2 y Canadá 9), se encuentran ubicados justamente detrás de los primeros 50 puestos. Uruguay ocupa el lugar 51, seguido de México (63), Paraguay (66), Brasil (70) y Colombia (73). Varios países de Centroamérica y el Caribe están en las últimas posiciones. Es pertinente preguntarse por esas ubicaciones. Si bien no se han encontrado relaciones tan claras entre, por ejemplo, el índice de desarrollo humano o el producto interno bruto (PIB) per cápita y las capacidades en materia de ciberseguridad, desde una interpretación más crítica en la relación entre tecnología y contexto institucional en el que se desenvuelve, los países con mayor desarrollo social, económico y científico tienen mejor desempeño en esta materia. Como señala Orlikowski (2000), el estudio de las tecnologías siempre se encuentra situado en una temporalidad y contexto; y en este caso resulta evidente que la ciberseguridad se encuentra inserta en un contexto humano e institucional del que no es tan fácil sustraerse.

Sin embargo, tanto el informe de BID/OEA (2020) como el índice de ciberseguridad global (UIT, 2018) ubican a Uruguay liderando en estos indicadores, a pesar de no contar propiamente con un documento nacional que se constituya como plan o estrategia. Asimismo, este país alcanza la máxima puntuación en temas referidos a la organización y coordinación de respuesta a incidentes; el desarrollo de la temática en el gobierno y la confianza de las personas en el uso de servicios de gobierno. El reporte BID/OEA (2020) también destaca que Uruguay cuenta con un CSIRT nacional, el CERT bajo la órbita de la Agencia de Gobierno electrónico y Sociedad de la Información y del Conocimiento (AGESIC), y un Centro de Operaciones de Seguridad (SOC) que funciona ininterrumpidamente desde 2016. También indica que, si bien no cuenta con una estrategia nacional, ha desarrollado un marco de ciberseguridad organizado con referencia a estándares internacionales. Este aspecto pone de manifiesto un tema relevante en la materia y es acerca de la pertinencia y necesidad de estas estrategias cuando existen planes específicos para atender distintos problemas relativos al ámbito. En esta línea argumental, Brasil recién publicó su estrategia a comienzos de 2020, luego de más de quince años de trabajo al respecto (Hurel, 2020) y consolidándose como el tercer país en la región en el índice global de ciberseguridad de la UIT, después de Uruguay y México.

COMENTARIOS FINALES

Los Estados se enfrentan crecientemente a presiones sistémicas para el desarrollo de una política nacional de ciberseguridad. La evidencia de los estudios de las estrategias nacionales de primera generación en el mundo con respecto a los casos de América Latina y el Caribe muestra una consolidación de una tendencia en materia de homogeneización de respuestas en forma de estas estrategias. Las mismas asumen un horizonte similar de expectativas, tanto en la definición, como en las soluciones de los problemas. Al mismo tiempo, se encuentran algunas condiciones de partida de cada contexto nacional desde una perspectiva de economía política, que se diferencian en su abordaje en tanto parten de distintos niveles de generalización del problema; brindan distintos grados de detalle de su instrumentación y de conceptualización de una propuesta de política industrial, todavía un elemento mayormente ausente.

Si bien todas las estrategias tienen por objeto abordar la seguridad en el ciberespacio a fin de mantener y desarrollar la prosperidad económica y social mediante el desarrollo continuo de una economía, atravesada por las reglas de lo digital, los aspectos económicos de la seguridad cibernética están adquiriendo

una mayor visibilidad en la región, siguiendo el devenir de otros contextos, como el europeo, que ya posee más años en su formulación. Aun cuando estas consideraciones son más escasas en el contexto de América Latina, ya que mayormente se vislumbran en los países más grandes de la región. La relación entre regímenes políticos y mercados en materia de provisión de servicios e infraestructura en la zona es aún incipiente en lo que respecta a la formulación estratégica de su desarrollo.

Las estrategias nacionales de ciberseguridad constituyen un punto de partida más que de llegada, en materia de desarrollo de capacidades efectivas en la gobernanza de la ciberseguridad. El propio problema es un asunto complejo, que requiere de instancias de coordinación y desarrollo de políticas multinivel tanto al interior de un Estado, como con el entorno internacional. El establecimiento de puntos de coordinación dentro de los gobiernos para las estrategias nacionales crea una oportunidad para mejorar la coordinación intergubernamental y con los distintos sectores nacionales, así como también para fomentar la cooperación internacional en los niveles político y operativo. Este elemento de mayor coordinación también aumenta el efecto estabilizador que se está buscando instaurar con mucho ímpetu desde hace más de una década por parte de agencias internacionales como el Consejo de Seguridad de la ONU, la UIT, la OEA, y la Organización para la Cooperación y el Desarrollo Económicos (OCDE) y espacios *multistakeholder*, como pueden ser el Global Forum on Cyber Expertise (GFCE), o el Global Commission on the Stability of Cyberspace (GCSC).

Como fue analizado, en relación tanto con los países que poseen un documento de estrategia, como aquellos que no, esta última emerge como una condición relevante, pero no suficiente en lo que respecta el desarrollo de capacidades en esta materia. El no contar con una estrategia nacional explícita no implica que no se aborde en forma planificada y coordinada desde el Estado nacional con acciones tendientes a dar respuesta a los principales problemas vinculados con la seguridad en la infraestructura digital de actores organizados y de la ciudadanía. Esto es, si bien la gobernanza de la ciberseguridad legitima cada vez más la práctica del desarrollo de una estrategia o plan nacional, aún no es una condicionante de su grado de avance en la materia. Sin embargo,

en el contexto actual, cuya presión internacional sistémica busca alinear los incentivos, compromisos y acciones de los Estados, la estrategia –dinámica y actualizada– será un instrumento que, como se señaló anteriormente, tenderá a proliferar.

En comparación con otras, las estrategias de ciberseguridad en la región requieren de una mejor comprensión de la estructura de incentivos de los actores del mercado en relación con la ciberseguridad y la promoción de medidas informativas. Tanto en las estrategias locales como en las de otros países, emerge como la necesidad de desarrollo de una mayor fuerza de trabajo en materia de ciberseguridad ante la falta de talento humano y las necesidades insatisfechas en los mercados.

A diferencia de lo observado en los estudios de las estrategias europeas, en las cuales se identifica un mayor grado de independencia tecnológica en relación con la seguridad de la tecnología de la información como un importante objetivo de política –con algunas excepciones como Chile y Brasil–, las estrategias en la región no tienen aún este énfasis en el aspecto de "soberanía tecnológica". De todas formas, el nivel de abstracción de muchas de ellas puede llevar a una aplicación en ese sentido, dependiendo de los cambios de los signos políticos de los gobiernos de turno.

Futuros abordajes podrían identificar más claramente las fuentes que legitiman las acciones de los actores públicos y privados en la región en materia de organización de los ecosistemas nacionales mediante las estrategias y sus aproximaciones para la instrumentación. Los estudios crecientemente normativos y prescriptivos que se están desarrollando, tanto por parte de organismos internacionales de carácter multilateral, como por parte de las asociaciones vinculadas a la industria tecnológica y de estandarización, tenderá a construir puentes más firmes para el desarrollo de estos instrumentos y habrá que estar preparados.

REFERENCIAS BIBLIOGRÁFICAS A DOCUMENTALES

Aggarwal, V.K. y Evenett, S.J. (2013). A Fragmenting Global Economy: A Weakened WTO, Mega FTAs, and Murky Protectionism. *Swiss Political Science Review*, *19*(4), 550-557. Recuperado de https://bit.ly/3KfYMLx

Aggarwal, V. y Reddie, A. (2018). Comparative industrial policy and cybersecurity: The US case. *Journal of Cyber Policy*, *3*(3). Recuperado de https://bit.ly/3MjCZEN

Barrios Achavar, V. (2018). Política Nacional de Ciberseguridad, 2017-2022. Biblioteca del Congreso Nacional de Chile. Recuperado de https://bit.ly/3MjCZEN

BID/OEA (2020). Reporte Ciberseguridad 2020: Riesgos, avances y el camino a seguir en América Latina y el Caribe. Recuperado de https://bit.ly/3sHdSnj

Bradshaw, S. (2015). Combating Cyber Threats: CSIRTs and Fostering International Cooperation on Cybersecurity. Global Commission on Internet Governance Paper Series, Paper no. 23

Bryant, C.G. (1999). The uses of Giddens' structuration theory. (Reihe Soziologie/Institut für Höhere Studien, Abt. Soziologie, 37). Wien: Institut für Höhere Studien (IHS), Wien. Recuperado de https://bit.ly/3sJqCdo

Bustos, G. y Aguerre, C. (2019). Marco analítico para un estudio comparado sobre gobernanza de la ciberseguridad en el Sur Global: los casos de Argentina y Brasil. Documento de investigación Centro Latam Digital. México.

Bustos, G. y Aguerre, C. (2020). Políticas sobre ciberseguridad en América Latina y el Sur Global: Argentina, un caso pionero signado por la discontinuidad. Documento de investigación Centro Latam Digital. México.

Cambronero, F. (2019). Ciberseguridad y la gobernanza multistakeholder. *Revista de Administración Pública 148, LIV*(1). Recuperado de https://bit.ly/34er9KT

Comisión Europea (2013). Estrategia de ciberseguridad de la Unión Europea: Un ciberespacio abierto, protegido y seguro. Recuperado de https://bit.ly/35wmu7t

CONPES (2011). Lineamientos de política para la ciberseguridad y la ciberdefensa. Documento CONPES 3701. Recuperado de https://bit.ly/3IKWYd4

Creese, S., Dutton, W.H., Esteve, P. y Shillair, R. (2020). Cybersecurity Capacity Building: Cross-National Benefits and International Divides en GIGANET Annual Symposium 2020. Recuperado de https://bit.ly/3IKWYd4

ENISA (2012). National Cyber Security Strategies. Recuperado de https://bit.ly/3sH2N5O

Forbes (2020). 2020 Roundup Of Cybersecurity Forecasts And Market Estimates. Recuperado de https://bit.ly/3CbxzXG

GFCE (2018). National Strategies. Interviews behind the cover. Recuperado de https://bit.ly/3tOfUld

Giddens, A. (1989). *Sociology*. Londres: Polity Press.

Gobierno de Chile (2017). Estrategia Nacional de Ciberseguridad. Recuperado de https://bit.ly/377K0bH

Gobierno de la República de Trinidad y Tobago (2012). Estrategia Nacional de Seguridad Cibernética. Recuperado de https://bit.ly/3pBp3Mk

Gobierno de México (2017). Estrategia Nacional de Ciberseguridad. Recuperado de https://bit.ly/3sJfzRu

Gobierno Nacional de Panamá (2013). Estrategia nacional de seguridad cibernética. Recuperado de https://bit.ly/35MdLxR

Government of Jamaica (2015). National Cybersecurity Strategy. Recuperado de https://bit.ly/3txqSLs

Haggart, B. (2019). Taking Knowledge Seriously: Towards an International Political Economy Theory of Knowledge Governance. En Haggart, B., Henne, C., Tusikov, N. (eds.) *Information, Technology and Control in a Changing World*. Suiza: Palgrave Macmillan.

Hurel, L.M. (5 de abril de 2020). Brazil's First National Cybersecurity Strategy: An Analysis of its Past, Present and Future. *Internet Governance Project*. Recuperado de https://bit.ly/3txQqrU

Hurel, Louise M. (2016). Cybersecurity and Internet Governance: Two Competing Fields? Tesis de licenciatura. Pontificia Universidad Católica de Río de Janeiro.

ITU (2018a). Global Cybersecurity Index. GCI. Recuperado de https://bit.ly/34h2DJ2

ITU (2018b). A Guide to Developing a National Cybersecurity Strategy. Recuperado de https://bit.ly/3IIFzIf

Klimburg, A. (2017). The darkening web, New York, Penguin Press.

Luiijf, E., Besseling, K. y Graaf, P. (2013). Nineteen National Cyber Security Strategies. *International Journal of Critical Infrastructure Protection, 9*(3). Recuperado de https://doi.org/10.1504/IJCIS.2013.051608

MICITT (2017). Estrategia Nacional de Ciberseguridad de Costa Rica. Recuperado de https://bit.ly/3vEePyB

Ministerio de la Gobernación (Mingob) (2018). Estrategia Nacional de Seguridad Cibernética. Documento Técnico núm. 1 (1-2018). Recuperado de https://bit.ly/3vBaKez

OCDE (1992). Guidelines for the Security of Information Systems. Recuperado de https://bit.ly/3trOv8s

OCDE (2012). Comparative analysis of national cybersecurity strategies. Recuperado de https://bit.ly/3sGdGVq

Orlikowski, W.J. (2000). Using Technology and constituting structures: a practice lens for technologies in organizations. Organization Science 11(4).

PEN (2019). Estrategia Nacional de Ciberseguridad de la República Argentina. Recuperado de https://bit.ly/3MnCXvt

Presidencia de la República de Brasil (2020). Estratégia Nacional de Segurança Cibernética. Recuperado de https://bit.ly/3tnV4sk

Presidencia de la República Dominicana (2017). Estrategia Nacional de Ciberseguridad 2018-2021. Recuperado de https://bit.ly/3sIbaxY

Presidencia de Nicaragua (2020). Estrategia nacional de ciberseguridad 2020-2025. Recuperado de https://bit.ly/35qIJfk

Senatic (2018). Plan Nacional de Ciberseguridad, Paraguay. Recuperado de https://bit.ly/3pFo0LD

Strange, S. (2015). States and Markets. Bloomsbury Revelations, Londres (1a ed. 1998).

CAPÍTULO 08

LA TRANSICIÓN HACIA LA E-DEMOCRACIA: LECCIONES PARA MÉXICO

PERLA CAROLINA GRIS LEGORRETA*
FERNANDO ROCHA ROSARIO**

* Instituto Belisario Domínguez.

** Facultad de Ciencias Políticas y Sociales de la Universidad Nacional Autónoma de México.

La utilización de las tecnologías de la información y la comunicación (TIC) en el ámbito gubernamental ha recibido importante atención en términos de su función como un mecanismo para hacer más eficiente la provisión de bienes y servicios públicos; sin embargo, esta no es la única contribución de las TIC, pues han sido objeto también de un uso más sofisticado para ampliar y mejorar la interacción entre autoridades y ciudadanos. Este capítulo presenta una discusión sobre las condiciones que se requieren para transitar de la mera utilización de las TIC en la provisión de bienes y servicios públicos hacia su uso efectivo para establecer relaciones de intercambio entre los distintos actores que participan en el espacio público.

El texto se estructura en tres secciones. La primera presenta un análisis conceptual de la democracia electrónica (e-democracia), así como de conceptos asociados como son el gobierno electrónico, la participación y la gobernanza electrónicas. El propósito de esta revisión teórica es identificar el estado del debate sobre dichos temas. La segunda sección se centra en discutir tres casos en los cuales se han utilizado las TIC para mejorar la interacción con la ciudadanía, lo cual permite distinguir los desafíos que han tenido estos países en la implementación de esos modelos. Finalmente, la última sección presenta algunas reflexiones derivadas del análisis teórico y empírico.

LA E-DEMOCRACIA: BASES CONCEPTUALES

La incorporación de la tecnología en la política ha motivado, al menos desde la segunda mitad del siglo XX, la creación de conceptos con los cuales pueda reconocerse la innovación técnica en la actividad gubernamental y ciudadana. Desde los años setenta esta conceptualización se ha concentrado en los procesos democráticos, lo cual conduce a reflexionar sobre la diferencia entre la democracia y la e-democracia. A este término se han asociado otros como gobierno electrónico, participación electrónica y gobernanza electrónica; también se han desarrollado indicadores para medir su presencia en el mundo, tales como la E-Government Survey de la Organización de las Naciones Unidas (ONU) y Freedom On the Net de Freedom House; se han establecido instituciones para dicho propósito, por ejemplo, en 1999 fue fundado en Escocia el International Teledemocracy Centre (ITC); en 2009, el Consejo Europeo hizo recomendaciones a sus Estados miembros para "la instauración, puesta en obra y evaluación de la democracia electrónica" (2009: 3); asimismo, el Parlamento Europeo ha investigado qué políticas públicas pueden mejorar la participación electrónica en la Unión Europea (Korthagen *et al.*, 2018). Así, la pregunta clave que aborda este capítulo es, ¿en qué consiste la democracia electrónica? Es menester reanalizar la intensión[1] de estos nuevos conceptos para disponer de mayor certeza en la categorización de su extensión empírica, su operacionalización y, finalmente, su instrumentación mediante políticas públicas.

Como una primera aproximación al tema, se hace una breve exposición sobre la historia de la conceptualización de la relación entre tecnología y política, con el fin de diseñar un concepto consistente, preciso y exacto de democracia electrónica, con el examen de la relación entre democracia y su profundización en democracia electrónica, lo cual conlleva exámenes conceptuales de gobierno electrónico, participación electrónica y gobernanza electrónica; y, por último, se discuten algunos de los potenciales beneficios y riesgos que se derivan lógicamente del término.

La tecnología en la política

Tanto Platón (*Político*, 293a-294b), como Aristóteles (*Política*, 1286a) se preguntaron cómo se distingue un gobierno ejercido por el humano de uno ejercido únicamente por leyes y cuál podía considerarse mejor. Después de la Segunda Guerra Mundial, la reflexión versó sobre cómo sería un gobierno ejercido por una máquina (Wiener, 1948; 1952),[2] esto es, un sistema centralizado que procesara grandes

1 Siguiendo a Sartori (1970) con su énfasis en una construcción lógica de conceptos, recordamos al lector la distinción entre *intensión* y *extensión*. La intensión de un concepto es su conjunto de propiedades mientras que la extensión es el conjunto de entidades empíricas en las que puede ser aplicado (Copi y Cohen, 1954).

2 Esta concepción técnica asumía algunas premisas sobre la política, por ejemplo, que se trata de un conjunto organizado de relaciones entre entidades internas y ambientales, como lo esbozó Easton (1953), lo cual podría funcionar sólo como primera abstracción dado que empíricamente resultaría inconsistente pues estas interacciones son mayormente conflictos institucionalizados.

cantidades de datos y eligiera la decisión más plausible con un cálculo lógico (Neveu, 1977), evitando con ello el sesgo de las pasiones y las falacias o trivialidades en los debates. La pretensión de evitar ambigüedades en facultades humanas, tal como el lenguaje, a través de la lógica, data desde Leibniz (1646-1716) con su *Calculus ratiocinator* y desde Boole (1815-1864) con sus *Leyes del pensamiento*, empero, probablemente Auschwitz alentó la intervención tecnológica en la política dado que la democracia occidental mostró que podía desembocar en su contrario totalitario (Vedel, 2003).

Según Vedel (2003), esta primera aspiración puede fecharse hasta los setenta, cuando gradualmente se transitó a la fase de la "teledemocracia", en la cual, dado el desarrollo de los medios masivos con las redes televisivas en los ochenta, la distribución de información a una mayor cantidad de ciudadanos y la superación de límites espaciales posibilitó la idea de reestablecer la democracia directa ateniense, principalmente en comunidades locales o, al menos, recrear la relación entre los ciudadanos y sus representantes mediante la transmisión de sus sesiones laborales (Vedel, 2003; Van Dijk, 2013; Korthagen *et al.*, 2018). La cuestión, en aquella época, ya no era cómo diseñar una máquina para gobernar sino cómo los distintos grupos sociales adquirirían una cultura técnica para utilizar eficazmente los dispositivos (Vedel, 2003), un aspecto que, como se discute más adelante, continúa siendo examinado.

A partir de los años noventa surgió la idea de comunidad virtual (Van Dijk, 2013), impulsada por el desarrollo de Internet que, aunque primitivamente comenzó a existir en los sesenta como ARPANet (Advanced Research Projects Agency Network), el cual se volvió público en 1993 y posibilitó la percepción de un ciberespacio descentralizado y sin jerarquía donde los ciudadanos podrían autoorganizarse en comunidades de interés y participar en los procesos políticos. Esta concepción culminó con el surgimiento de la Web 2.0 (Van Dijk, 2013) en la cual la ciudadanía tiene el potencial de participar en la toma de decisiones en formas homólogas a las físicas, esto incluyó, por ejemplo, transitar de la petición rubricada a la petición electrónica (*e-petition*) firmada desde múltiples cuentas de usuario, de los foros consultivos o reuniones locales a los foros y sesiones virtuales o grupos de interés en redes sociales, de las pancartas a los *hashtags*, entre otras manifestaciones.

La democracia electrónica/democracia digital, *e-democracy/digital democracy*, *cyberdémocratie/démocratie numérique*, *e-demokrati* es un fenómeno empírico que ha sido abordado por distintas disciplinas, como matemáticas, ingeniería, ciencias sociales y la administración (Houston, 2016; Sundberg, 2019), por lo que existen múltiples aproximaciones, tanto en las causas como en los efectos de su existencia (Mossberger, 2008; Lee, Chang y Berry, 2011; Sundberg, 2019) o en las relaciones entre los actores y las funciones y capacidades de estos, como mecanismos de operación (Kneuer, 2016). Es necesario hacer explícitas ahora las implicaciones lógicas de sus diferentes conceptualizaciones, dado que no existe un firme consenso en su definición, para obtener un concepto consistente con *democracia* y el potencial de la tecnología en información y comunicación (TIC).

La e-democracia frecuentemente es una definición estipulativa o normativa, la cual, conforme a Copi y Cohen (1954), es aquella que no es ni falsa/verdadera ni válida/inválida, pues es directiva, es decir, manifiesta únicamente sus valores. Un ejemplo es la proporcionada por el Consejo Europeo (2009): "un medio de defender y reforzar la democracia, las instituciones y los procesos democráticos con la ayuda de las TIC y de la inversión y reinversión de los ciudadanos en la vida democrática (8)".

Esta primera definición muestra una noción inmediata de lo que es la e-democracia: el mejoramiento de los procesos democráticos con el uso de las TIC, es decir, la intersección entre actividades democráticas y TIC (diagrama 1).[3]

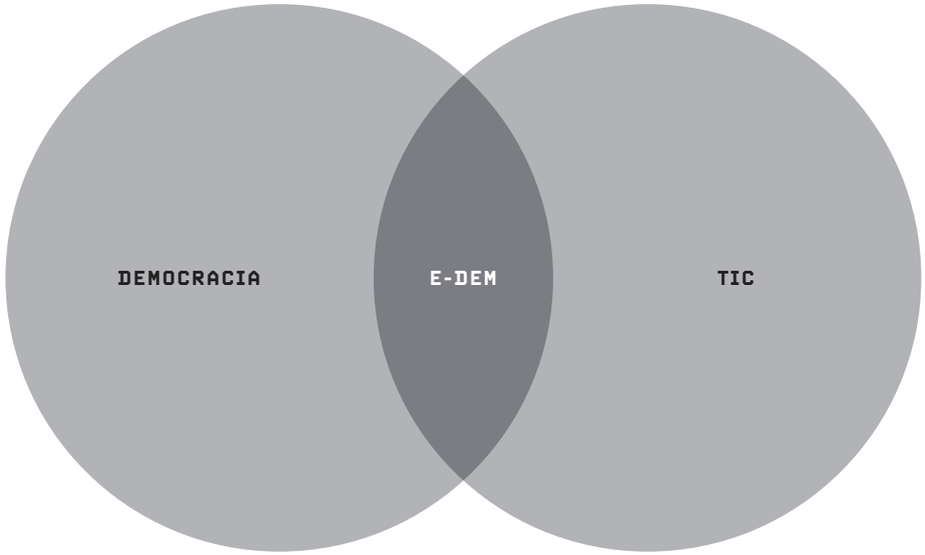
Ello supone que la presencia de infraestructura tecnológica es una condición necesaria[4] para la e-democracia, la cual, no obstante, es garantía de su existencia, como indicó Dahl (1989)

3 Dado que se alude a relaciones de conjuntos y condiciones necesarias/suficientes, se utilizan, considerando a Mahoney y Vanderpoel (2015), diagramas de Venn-Euler como un apoyo visual para la comprensión del análisis conceptual.

4 Al respecto es relevante recordar en qué consisten las condiciones necesarias/suficientes. Una condición es necesaria para algo si esto no puede existir sin aquella, pero la presencia de dicha condición no garantiza su existencia. Una condición es suficiente para algo si su existencia garantiza la presencia de este, pero su inexistencia no asegura la ausencia de aquel (Copi y Cohen, 1957; Mahoney, Kimball y Koivu, 2015).

CONCEPTO BÁSICO DE DEMOCRACIA ELECTRÓNICA

DIAG. 01.



FUENTE: elaboración propia.

y como lo ejemplifica el *Kwangmyong*, el intranet nacional de Corea del Norte controlado por el gobierno, así como el caso de la censura de Internet en China mediante su conjunto de normas Computer Information Network and Internet Security, Protection and Management Regulations establecido en 1997 y su Gran Cortafuegos (Freedom House, 2019).

A partir del planteamiento, podría surgir la siguiente pregunta, ¿la infraestructura tecnológica debe residir en las autoridades (gobierno electrónico) o en la ciudadanía (participación electrónica)? Dado que la e-democracia usualmente se extrae de los modelos de democracia liberal, democracia deliberativa y democracia directa (Päivärinta y Sæbø, 2006; Van Dijk, 2013; Hennen, 2020), la respuesta a esta pregunta puede variar. Para esclarecerlo, es importante definir los elementos principalmente involucrados, con un examen, si no profundo, sí consistente y preciso.

Gobierno electrónico

La definición de gobierno electrónico (e-Gov), para los propósitos de este texto, se basa principalmente en Grönlund (2002) y Welp (2011) y se define como un gobierno que digitaliza estratégicamente su administración interna y los servicios públicos con el fin de simplificar y aumentar la eficiencia de sus procesos de producción y provisión a los ciudadanos. Dicha definición contiene dos aspectos de los tres que, según Grönlund (2002), son comunes en la multiplicidad de conceptualizaciones del gobierno electrónico: mejoramiento de servicios, eficiencia operacional e incentivación de la democracia. Se omite esta última propiedad, concibiendo sólo una relación *top-down* entre autoridades y ciudadanos, dado que la intención es definir gobierno electrónico en, por decirlo de alguna manera, su estado puro, puesto que son posibles los gobiernos no democráticos. No obstante, como se explicará más adelante, un gobierno electrónico lógicamente es condición necesaria para la democracia electrónica.

La definición refiere también a la parte interna y externa del gobierno (Grönlund, 2002): internamente dichas agencias son integradas y automatizan algunas de sus actividades, mientras que externamente los ciudadanos puedan ser provistos de servicios sin tener interacción física con la agencia gubernamental (Sundberg, 2019).

Asimismo la definición propuesta considera la "digitalización estratégica", para lo cual se argumenta la razón por la que se conserva este valor hacia la estrategia, pero no hacia la democracia. La digitalización estratégica es necesaria para que un gobierno sea electrónico, dado que, así como como política pública no es una intervención fortuita de las autoridades, el empleo casual de las TIC tampoco vuelve electrónico a un gobierno.

No obstante, la digitalización de los servicios, la automatización de procesos e integración de las agencias conlleva los siguientes riesgos: la concentración de poder en alguna autoridad; la tecnificación y disminución de control de autoridades (Welp, 2011) y, en general dentro del ciberespacio, la dependencia de la seguridad de las TIC: confidencialidad, integridad, autenticidad y disponibilidad de la información personal o pública, y desempeño, rendición de cuentas, mantenibilidad y regulación de los mecanismos electrónicos (Grönlund, 2002; Vedel, 2003; Ackerman, 2011).

Participación electrónica

Mientras el gobierno electrónico puede considerarse una relación *top-down* con el ciudadano, la participación electrónica (e-participation), siguiendo a Kneuer (2016), puede concebirse como relaciones *top-down* y *bottom-up* entre el gobierno y el ciudadano en actividades que pueden categorizarse, conforme a la Organización para la Cooperación y el Desarrollo Económicos (OCDE) (2003), en obtención de información, diálogo, monitoreo y toma de decisiones, las cuales tratan respectivamente, el problema de poca transparencia, cerradura del espacio público y arbitrariedad decisional (Vedel, 2003; Chatelanant, 2011). Esto se considera dado que, como la misma palabra indica, la participación consiste en ser parte y, en este caso, lo es involucrándose en los procesos externos de las autoridades a través de las TIC. Por ejemplo, Macintosh (2004) y Van Dijk (2013) muestran cómo la participación electrónica se asocia con las fases del proceso de políticas públicas, principalmente con la conformación de la agenda, la planeación y la evaluación.

Se asume la relación *bottom-up* por la posibilidad que tienen los ciudadanos de, por iniciativa propia, comunicarse con las autoridades para informarse sobre sus actividades, supervisarlas o incidir en sus procesos decisionales, es decir, el potencial de crear voluntariamente estos canales, sea de manera institucional o extra institucionalmente, tal como las peticiones y consultas electrónicas o las campañas digitales. Por otro lado, también se considera la relación *top-down*, pues dichos canales pueden ser promovidos desde las autoridades, los cuales suelen estar estructurados para un único fin, por ejemplo: el voto electrónico y los foros virtuales.

Por lo tanto, la participación electrónica, con base en las ideas de Macintosh (2004) y Van Dijk (2010, 2013), se define como la utilización de las TIC para involucrar a los ciudadanos en las actividades de las autoridades, obteniendo información sobre ellas, supervisándolas o influyendo en sus procesos decisionales.

Se reconoce también que el compromiso cívico puede variar conforme al empleo de los medios digitales. Macintosh (2004) propone tres grados sobre esto: capacidad electrónica (*e-enabling*), compromiso electrónico (*e-engaging*) y empoderamiento electrónico (*e-empowering*), los cuales van desde tener acceso a información sobre las autoridades, deliberar sobre cuestiones de política pública hasta incidir en ellas. La definición presentada aquí no enfatiza en el último nivel dado que sería una concepción fragmentada por la valoración de una democracia participativa, pero sí considera la posibilidad de cada uno de los niveles, es decir, que existan las condiciones materiales y reglamentarias para que un ciudadano transite de la mera capacidad electrónica al empoderamiento electrónico.

Gobernanza electrónica

La definición de gobernanza es menos clara que las anteriores, dado que es susceptible de ser confundida con gobernabilidad (Banco Mundial, 1997, 2007), gobierno o incluso aludir a la calidad del ejercicio de gobierno, como la han concebido implícitamente Gerring y Thacker (2008) y Grindle (2010). Otros académicos la han definido como la coordinación entre el gobierno, los ciudadanos y el sector privado para resolver un problema público (Aguilar, 2016), que es la concepción asumida en este texto, esto debido a su mayor utilidad y precisión conceptual. Si se concibe gobernanza como calidad del ejercicio gubernamental, es posible, como expone Grindle (2010), concentrarse en una "buena gobernanza" y volverla una definición estipulativa, como anteriormente fue descrita para el caso de democracia electrónica. De igual forma, si se considera gobernanza como la capacidad de las autoridades de gobernar o la susceptibilidad de la sociedad de ser gobernada, propiedades atribuidas a gobernabilidad, siguiendo a Aguilar (2016), entonces sólo será posible enfatizar la eficiencia del gobierno, pero no su suficiencia, cuestión que trata la gobernanza como coordinación entre actores gubernamentales, sociales y privados, con la premisa de que los problemas contemporáneos rebasan, por sí mismos, la gobernabilidad de las autoridades o aumentan la ingobernabilidad de la sociedad (Aguilar, 2016). Por otra parte, si se concibe gobernanza con los atributos de gobierno, se estará confundiendo cualidad con sujeto, acción con actor.

Por lo tanto, la gobernanza electrónica se entiende aquí como la coordinación, mediante las TIC, intencional y planificada entre el gobierno, los ciudadanos y el sector privado para resolver un problema público.

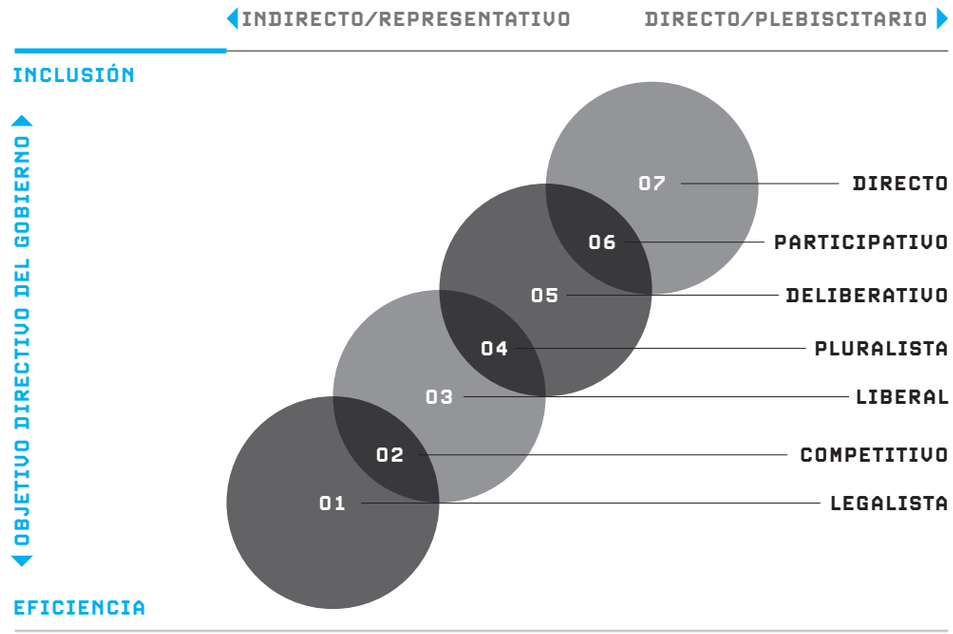
Retornando a la e-democracia

La pregunta planteada párrafos antes fue: ¿infraestructura tecnológica en las autoridades o en la ciudadanía para la presencia de la democracia electrónica? Otra cuestión que fue asumida, pero que puede ser una interrogante es si la participación electrónica considera también los canales extra institucionales y si sólo son consideradas como participación electrónica las incidencias efectivas de los ciudadanos en los procesos decisionales de las autoridades. Como se mencionó, las respuestas a estas preguntas pueden variar conforme al modelo de democracia empleado. Las diversas tipologías que se han realizado han sido a partir de la graduación de dos ejes: Van Dijk (2000) elabora seis modelos graduando el principal objetivo del gobierno (formación de la opinión ciudadana o proceso decisional) y el medio primario para ese fin (democracia representativa o democracia directa); Päivärinta y Sæbø (2006), en cambio, constituyen cuatro modelos con la graduación de la intervención ciudadana en el proceso decisional (inclusión implícita o explícita) y en la configuración de la agenda (gobierno o ciudadanos); Lindner (2007), por su parte, obtiene ocho modelos graduando la incidencia ciudadana en el proceso decisional (representación o intervención directa) y la relación comunicacional (vertical u horizontal); y Hennen (2020) presenta tres modelos y seis submodelos graduando el modo del proceso decisional (indirecto o directo) y el objetivo rector del gobierno (inclusión o eficiencia). Con base en estos trabajos, se consideran tres submodelos de las intersecciones entre cuatro modelos (diagrama 2), graduando, como Hennen (2020), la incidencia ciudadana en los procesos decisionales de las autoridades (indirecta o directa) y el principal objetivo de estas (inclusión o eficiencia).

Asimismo se retoman –aunque de manera amplificada– las tres dimensiones de Kneuer (2011; 2016) de la democracia:[5] constitucional o de control, consistente en el conjunto de reglas (que permiten, obligan y prohíben) sobre los derechos humanos y políticos; procedimental, la cual versa sobre la capacidad de *inputs* en

5 Tales dimensiones fueron realizadas identificando condiciones semejantes entre los conceptos de democracia dados por Pérez-Liñán (2001), Beetham (2002) y Diamond y Morlino (2005).

DIAG. 02. MODO DE PROCESO DE TOMA DE DECISIONES



FUENTE:
basado en Van Dijk (2000, 2013), Lindner (2006) y Hennen (2020).

los procesos decisionales, tales como la participación, competición y rendición de cuentas; y de efectividad, consistente en la eficacia gubernamental. Por último, es importante mencionar las implicaciones del empleo de las TIC (Hacker y Van Dijk, 2000):

- creación de canales de comunicación
- libertad de la estructuración gubernamental
- reducción de costos del proceso *online* en comparación con la alternativa *offline*
- superación de límites espaciales y temporales
- supresión de mediadores en los procesos comunicacionales
- mayor posibilidad de interacciones horizontales e incremento de eficiencia de las actividades

Contrastando la tipología y las dimensiones anteriores con base en las implicaciones de las TIC, serán descritas, conforme a los conceptos dados de gobierno electrónico, participación electrónica y gobernanza electrónica, otras dos posibles conceptualizaciones de la e-democracia.

En el modelo legalista, caracterizado por la suficiencia –dada por ser la eficiencia el objetivo principal y la representación la forma de incidir en el proceso decisional– de la existencia de reglas y procedimientos determinantes de la separación de poderes públicos, sistema de pesos y contrapesos y representación de los ciudadanos (Van Dijk, 2013), la e-democracia consistiría meramente en la presencia de un gobierno que ha digitalizado sus procesos externos de manera que el equilibrio entre autoridades se preserve, lo que sería parcialmente la dimensión constitucional de Kneuer (2011). Por lo tanto, en este arquetipo no es necesario que la sociedad disponga de infraestructura tecnológica.

El submodelo competitivo es descrito por Van Dijk (2013) como un contexto en el que los líderes compiten por el apoyo de una comunidad, por lo que la representación y eficiencia de esta no sólo es sobre las autoridades, sino sobre cualquier líder social con pretensiones políticas. La democracia, por lo tanto, en este modelo consistiría en, además de las condiciones anteriores del modelo legalista –dado que las condiciones de un arquetipo pueden considerarse necesarias para los modelos subsecuentes–, la plenitud de la dimensión constitucional y parcialmente la dimensión procedimental de Kneuer (2011), integrando los derechos humanos y políticos, los cuales son necesarios para que haya una libre competencia por el liderazgo y el apoyo de una comunidad; asimismo, la incorporación de las TIC, según Hennen (2020), sería para mejorar la comunicación entre candidatos y comunidades durante campañas electorales, la cual es permitida por la reglamentación anterior y capacidad electrónica de los ciudadanos, conforme a la escala de Macintosh (2004) antes mencionada. La participación electrónica aparece, pero sólo como relación *top-down* y en su nivel mínimo.

El modelo liberal es descrito como un contexto en el que la privacidad del ciudadano es protegida reglamentariamente de la intervención gubernamental, además de garantizar una toma de decisiones vinculante, aunque los procesos democráticos aún son concebidos como análogos al mercado económico donde actores compiten por satisfacer al ciudadano, quien se comporta como un consumidor (Päivärinta y Sæbø, 2006; Hennen, 2020). Para procurar la privacidad individual y mantener la posibilidad de que los actores contiendan por el elector, la libertad de Internet es una condición necesaria.

El submodelo pluralista sobresale por la presencia de minorías en coaliciones en vez de una mayoría preponderante, donde aquellas son representadas ya no sólo por los políticos, sino también por organizaciones sociales, asimismo aquí las TIC posibilitan debates *online* y una mejor formación de la opinión ciudadana (Van Dijk, 2013; Hennen, 2020), por lo que se puede concluir que, en este caso, comienza a presentarse difusamente el compromiso electrónico en los ciudadanos de Macintosh (2004) y que la dimensión procedimental de Kneuer (2011, 2016) existe con más nitidez.

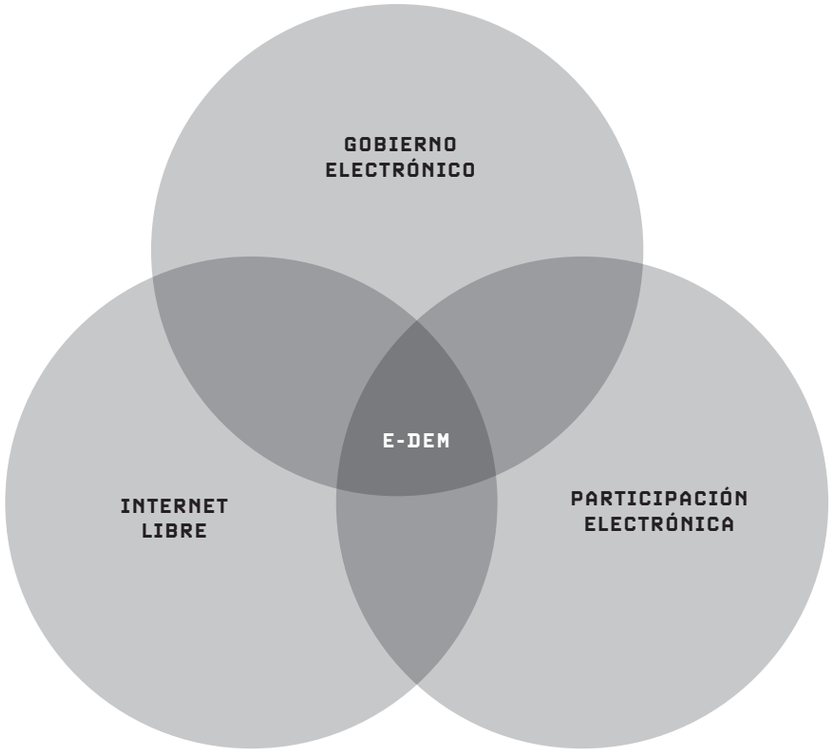
Con respecto al modelo deliberativo, es concebido como un contexto donde los ciudadanos disponen de mismas condiciones para deliberar libremente en el espacio público, actividad que no es espontánea, ya que pretende incidir en los procesos decisionales, aunque la determinación de estos permanece plenamente en las instituciones (Van Dijk, 2013; Hennen, 2020). La incorporación de las TIC facilita una comunicación horizontal entre ciudadanos y constituye nuevos canales para con las autoridades, por lo que aquí la participación electrónica se muestra también como una relación *bottom-up*.

En el arquetipo participativo el involucramiento ciudadano en la toma de decisiones de las autoridades es fundamental, por lo que es una actividad inherente a la vida cotidiana y existen condiciones para una incidencia institucional o extrainstitucional; no obstante, existen aún decisiones que atañen meramente a las autoridades. (Van Dijk, 2013; Hennen, 2020). Las TIC posibilitan el empoderamiento electrónico de Macintosh (2004) y completan la dimensión procedimental de Kneuer (2011), por lo que en este contexto la gobernanza electrónica es funcional.

Por último, en el modelo plebiscitario, las deliberaciones ciudadanas tienen un efecto directo sobre los procesos decisionales de las autoridades o estas constantemente crean canales para no sólo consultar al ciudadano, sino para que su decisión se manifieste en la decisión final de la autoridad (Päivärinta y Sæbø, 2006; Van Dijk, 2013; Hennen, 2020). El empleo de las TIC posibilita que los efectos de la deliberación o expresión ciudadana sean directos e inmediatos. La distinción entre este modelo y el anterior es el incremento de la certeza de que la participación electrónica incidirá en los procesos decisionales.

CONCEPTO CONJUNTIVO DE DEMOCRACIA ELECTRÓNICA DE KNEUER (2016)

DIAG. 03.



FUENTE: elaboración propia.

Los modelos anteriores se distinguen por la suficiencia de sus condiciones posibles para considerar la presencia de la democracia y, por lo tanto, de la e-democracia, por ejemplo, las del modelo directo en el arquetipo legalista pueden ser posibles, mas no necesarias, para aseverar que el contexto legalista es democrático, mientras que en el arquetipo directo dichas condiciones sí son necesarias para afirmar que es democrático. Conforme se transita de modelo en modelo, las restricciones pueden ser mayores o menores para considerarlo democrático.

En los arquetipos participativo y directo es posible reconocer la conceptualización de Kneuer (2016), quien considera como dimensiones de la e-democracia las siguientes condiciones: infraestructura tecnológica e Internet libre, participación electrónica *top-down* y *bottom-up* y gobierno electrónico. Estas tres dimensiones, aunque Kneuer (2016) no lo menciona, son una conjunción productora de la democracia electrónica, por lo que cada una es una condición INUS[6] para ella (diagrama 3).

Aparentemente esta conceptualización es plausible dado que incorpora equilibradamente elementos estructurales (infraestructura tecnológica, gobierno electrónico, participación electrónica *top-down*) y normativos (Internet libre y participación electrónica *bottom-up*) de la e-democracia. No obstante, si estas condiciones son INUS, entonces cada una existe por sí misma, lo cual ya no es consistente, ¿es posible entonces la existencia de un Internet libre sin un gobierno electrónico o participación electrónica y viceversa?

Kneuer (2016) presenta a la e-democracia como efecto de la conjunción de tres condiciones INUS, entre las cuales una ya es, por sí misma, una conjunción: la infraestructura tecnológica, que es el aspecto técnico, y un Internet libre, que es el reglamentario. La autora parece considerar que existe infraestructura tecnológica si y sólo si existe una igualdad de acceso a ella, empero, estas no son circunstancias bicondicionales y la primera ni siquiera es equiparable a la capacidad electrónica de Macintosh (2004), pues una autora sólo estima la posibilidad de acceder mientras que la otra retoma, además, la inteligibilidad del contenido al que se accede. Esto es, Kneuer (2016) sólo se basa en una disponibilidad igual de los medios digitales ante los ciudadanos, "una red de banda ancha con igual distribución" (673). No obstante, no basta la presencia de estas herramientas para afirmar que se accede a ellas, el conocimiento técnico de utilización es una cuestión también relevante, como lo discuten DiMaggio y sus colegas (citado en Mosserberger, 2008): el efectivo empleo de las TIC puede variar conforme al "acceso a Internet, extensión de uso, conocimiento de estrategias de

6 *Insufficient but Necessary for a condition Unnecessary but Sufficient* (Mackie, 1980), es decir, es una condición insuficiente, pero necesaria para un conjunto de condiciones innecesarias, pero suficientes.

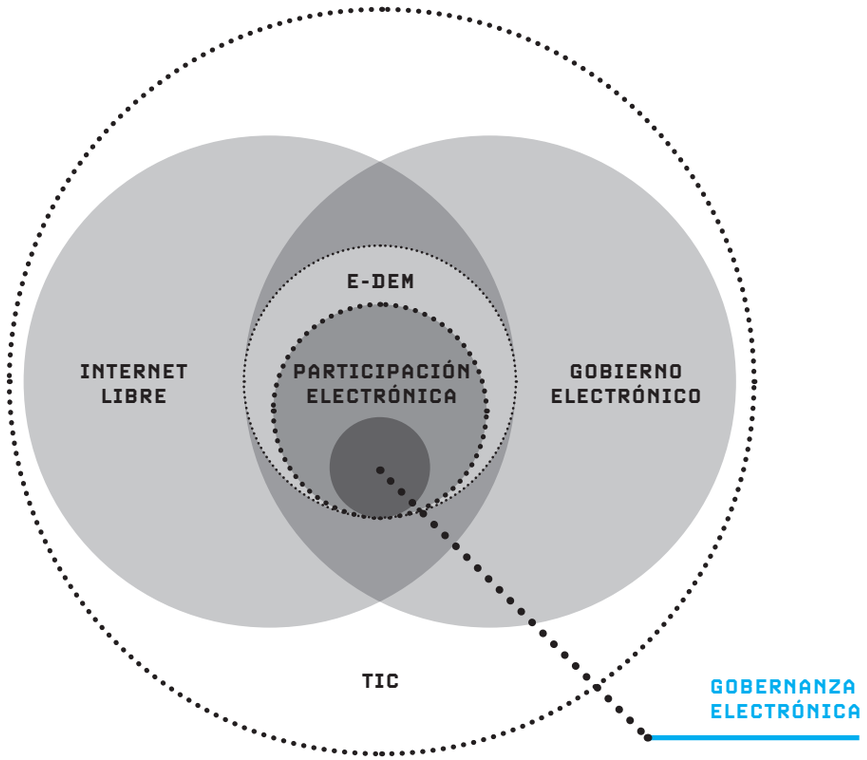
búsqueda, calidad de conexiones [...] y capacidad de evaluar la calidad de información" (13), que es lo que para ellos posibilitaría una ciudadanía digital. Y con respecto de la igualdad, esta sólo sería consistente donde toda o una gran mayoría de la población tuviera las capacidades anteriores, es decir, que no existiera la "fractura tecnológica" explicada por Ziegler (2016) o que marginara a una porción sumamente pequeña de la ciudadanía, pues en un contexto donde la democracia electrónica prepondera, quienes no sepan utilizar las herramientas para ejercerla serán análogamente analfabetos. Esto es consistente con los modelos presentados, en el arquetipo legalista no es necesaria la infraestructura tecnológica en la sociedad para que exista e-democracia, pero desde el modelo competitivo comienza a existir la participación electrónica, la cual, aunque sólo consista en su modo *top-down* y nivel de capacidad electrónica, generaría una fractura tecnológica entre quienes saben usar los medios digitales y quienes ignoran su uso. Por lo tanto, la infraestructura tecnológica no es lógicamente bicondicional con el acceso a ella y menos con igualdad de acceso, así que se conciben distintas la presencia de las TIC, el libre acceso a ellas y la capacidad de utilizarlas eficazmente.

Ahora, ¿cada condición, manifestadas como INUS, existen por sí mismas, es decir, ninguna es necesaria para otra? La infraestructura tecnológica puede existir sin Internet libre, como se ejemplificó con los casos de Corea del Norte y China, pero es imposible que el Internet libre exista sin infraestructura tecnológica, pues esta es su fuente material, su condición necesaria. El gobierno electrónico no existe sin TIC, dado que posibilita la digitalización de sus procesos internos o externos, por lo que la infraestructura tecnológica también es condición necesaria para él, no obstante, no ocurre lo mismo con el Internet libre: si este es libre se debe a que el gobierno lo regula mínimamente o no interviene en él porque no es capaz o no es su intención; si no es capaz, entonces definitivamente el gobierno no es electrónico –aunque su sociedad sí disponga de medios digitales–; si lo regula, entonces evidentemente las autoridades disponen de medios digitales con los cuales identificar contenido, usuarios y demás, por lo que el gobierno es electrónico, pero también puede suceder que el Internet sea libre porque el gobierno, aunque haya digitalizado diversos procesos suyos, no considere que es públicamente relevante regularlo, aunque sea mínimamente. Por lo tanto, el Internet libre y el gobierno electrónico no son mutuamente condiciones necesarias, con lo cual se confirma que dos condiciones de la conceptualización de Kneuer (2016) sí pueden existir por sí mismas. Con respecto de la participación electrónica, no existe por sí misma dado que para una relación *top-down* las autoridades requieren medios para crear y mantener los canales digitales con los ciudadanos y, según sea el caso, almacenar y procesar la información que les proporcionen, lo cual también ocurre en un *bottom-up*, especialmente en los canales institucionales, por ejemplo, el voto electrónico, el cual requiere una digitalización de procesos internos y externos del gobierno. En consecuencia, el gobierno electrónico es condición necesaria de la participación electrónica, pero tampoco existe sin un Internet libre, especialmente cuando la participación es *bottom-up* y extrainstitucional: es decir, si un conjunto de ciudadanos delibera en el ciberespacio asuntos inapropiados para el gobierno y este obstruye su asociación al bloquear sus cuentas o el sitio web donde interactuaban, entonces no existió participación electrónica, lo mismo ocurre cuando se difunde información o un ciudadano hace una petición electrónica. Entonces un Internet libre y un gobierno electrónico son conjuntamente necesarios para la participación electrónica. Con este breve examen lógico, se concluye que la conceptualización de Kneuer (2016) no es plenamente correcta, pues la participación electrónica no puede existir por sí misma.

Por lo tanto, con base en lo anterior, se afirma lo siguiente: es condición lógicamente necesaria de la democracia electrónica la infraestructura tecnológica, condiciones conjuntamente necesarias un Internet libre y un gobierno electrónico y son condiciones lógicamente suficientes la participación electrónica y la gobernanza electrónica (diagrama 4).

CONCEPTO DE CONDICIONES NECESARIAS/SUFICIENTES DE LA DEMOCRACIA ELECTRÓNICA

DIAG. 04.



FUENTE: elaboración propia.

Con respecto de la participación y gobernanza electrónicas, ambas son lógicamente condiciones suficientes de la e-democracia, pero la primera es condición necesaria de la segunda. La coordinación entre el gobierno, la sociedad y el sector privado mediante las TIC sólo es posible en un contexto donde los tres actores disponen de estas herramientas digitales y son capaces de usarlas, por lo que resulta necesaria la digitalización estratégica interna y externa del gobierno para ser emisor y receptor y la posibilidad de influir en sus procesos decisionales a través de la tecnología para que los ciudadanos puedan organizarse con las autoridades.

De consiguiente, la participación electrónica es condición necesaria de la gobernanza electrónica. Asimismo, cuando está presente la participación electrónica, por todo el examen anterior, indica que la infraestructura tecnológica, el gobierno electrónico y el Internet libre, están presentes. Así, también lo está la democracia electrónica. Vale la pena reflexionar y exponer esto.

Las condiciones necesarias/suficientes son útiles para saber cuándo está ausente o presente cierta entidad. Si durante este análisis lógico sólo hubiesen sido identificadas las condiciones suficientes, únicamente se obtendrían hipótesis para reconocer la existencia de la e-democracia en algún Estado, mas no para reconocer su ausencia. Ambas condiciones se complementan.

Como se mencionó durante la exposición de los modelos de democracia, la consideración de la existencia de esta varía conforme a la suficiencia de ciertas condiciones, por lo que, para ser consistentes con esto, pero también precisos, este examen lógico proporciona una conceptualización equilibrada entre aspectos estructurales y normativos, como el concepto de Kneuer (2016). La infraestructura tecnológica y el gobierno electrónico pueden considerarse como elementos estructurales, mientras que el Internet libre, la participación y gobernanza electrónicas como los elementos normativos.

Por último, es posible hacer otra inferencia a partir de la conceptualización lógica propuesta: sobre la importancia de las condiciones necesarias/suficientes para la democracia electrónica. Una condición necesaria, conforme a Mahoney y Vanderpoel (2015), es más relevante que otra cuanto menos típica es, mientras que una condición suficiente es más relevante que otra cuanto más típica es. Con base en lo planteado y en lo representado en el diagrama 4, es posible concluir que la conjunción de un Internet libre y un gobierno electrónico es una condición necesaria para la e-democracia más importante que la infraestructura tecnológica, mientras que la participación electrónica es una condición suficiente más relevante que la gobernanza electrónica.

Este conjunto de conceptos da cuenta de las distintas condiciones que afectan la implementación de modelos como la e-democracia, resulta entonces relevante profundizar en estas a partir de experiencias prácticas, como se desarrolla en la siguiente sección.

EXPERIENCIAS INTERNACIONALES: LA E-DEMOCRACIA EN LA PRÁCTICA

La revisión teórica presentada anteriormente permite discutir la dimensión empírica del concepto de e-democracia pues, al descomponerlo en condiciones necesarias/suficientes y estas en distintas categorías, es posible estructurar el análisis de los siguientes tres casos que sobresalen por la implementación del gobierno electrónico, la participación y la democracia electrónicas.

Esta sección persigue dos objetivos principales. El primero es hacer una descripción de los tres casos, considerando las características del diseño y de la implementación de los modelos. El segundo es identificar aquellos elementos de aprendizaje que sean de utilidad para su implementación en el contexto mexicano.

Malta: El caso de referencia en gobierno electrónico

De acuerdo con el e-Government Benchmark 2019, la República de Malta es el país con mejor desempeño en términos de gobierno electrónico en el continente europeo. El ejercicio de comparación mide el desempeño con base en cuatro dimensiones: *1)* énfasis en el usuario, es decir, la facilidad de acceso y uso de los servicios electrónicos; *2)* transparencia de los procedimientos gubernamentales, así como del control que tienen los usuarios sobre sus datos personales; *3)* movilidad transfronteriza, entendida como la accesibilidad que hay a los servicios para ciudadanos europeos y *4)* habilitadores clave, referentes a la disponibilidad de identificaciones y documentos electrónicos (Comisión Europea, 2019).

Lo anterior es resultado de la modernización gubernamental desde hace, al menos, dos décadas. En específico, el desarrollo de la política de gobierno electrónico se centró en asumir la necesidad de ser implementada con la colaboración del sector privado y generando condiciones para que estas acciones influyeran en la sociedad. La Organización de las Naciones Unidas para la Educación la Ciencia y la Cultura (UNESCO, por sus siglas en inglés) ha identificado en el caso de Malta lecciones interesantes respecto de tres temas fundamentales que facilitaron la adopción de esta herramienta: *1)* marco jurídico para regular el comercio electrónico, la protección de datos y el uso indebido de la informática; *2)* la promoción del uso del Internet, tanto en el ámbito ciudadano como empresarial y *3)* creación de organizaciones específicas para la implementación de esta política, por ejemplo, la Comisión de la Sociedad y la Economía de la Información (UNESCO, 2002).

En línea con lo discutido en el apartado teórico de este texto, el caso de Malta, siguiendo las ideas de Macintosh (2014), se centra en políticas dirigidas a generar capacidad electrónica (*e-enabling)*, es decir, en establecer las condiciones necesarias para potenciar el uso de las TIC.

CUADRO 01. COMPONENTES PRINCIPALES DE LA ESTRATEGIA DIGITAL NACIONAL DE MALTA

Ciudadanía digital	Empresa digital	Gobierno digital
• Dirigido a mejorar el bienestar de los ciudadanos (énfasis en grupos vulnerables, por ejemplo, a partir de garantizar el acceso a Internet y potenciar el uso de las TIC para mejorar la calidad de vida).	• Promoción de competitividad empresarial y del mercado local, por ejemplo, a partir de dotarles de más herramientas para la exportación.	• Reducción de burocracia e incremento de eficiencia y transparencia.
• Habilidades digitales básicas como herramientas de empoderamiento ciudadano a partir de programas educativos sobre el uso seguro y crítico del Internet.	• Atracción de inversión extranjera, promoción de empresas emergentes y de alianzas estratégicas.	• Mayor cercanía entre los servicios públicos y la sociedad civil y empresas.
• Servicios digitales accesibles, asequibles y seguros, por ejemplo, la provisión de Internet gratuito en edificios públicos y plazas.	• Promoción de condiciones para que las empresas puedan aprovechar las ventajas del mercado europeo y del norte de África.	• Mejora del proceso de toma de decisiones gubernamentales.
		• Promoción de mayor intercambio de información entre dependencias gubernamentales.

FUENTE: elaboración propia con base en MCA (2014).

CUADRO 02.

Acción	Descripción
1. Transacciones con el gobierno	Favorecen el establecimiento de transacciones seguras del gobierno con la ciudadanía y el sector privado mediante distintos canales, incluye, por ejemplo, el uso de facturas y recibos electrónicos, formatos electrónicos, etcétera.
2. Ventanilla única	La ciudadanía se beneficia del concepto de ventanilla única, a partir de esquemas como el portal único y la personalización de los servicios.
3. Ambiente digital colaborativo	Esfuerzos gubernamentales con actores clave para apoyarv la adopción de tecnología que integre servicios interdepartamentales; para facilitar el uso, la gestión, la retención, la preservación y el archivo de los registros digitales para que estos permanezcan accesibles y utilizables; proteger el conocimiento corporativo y mejorar la seguridad, integridad, accesibilidad, trazabilidad y archivo de los datos; fortalecer el intercambio de conocimientos; habilitar flujos de trabajo; promover entornos colaborativos para el trabajo unificado en múltiples dispositivos y medios.
4. Herramientas de análisis	Promover la adopción de herramientas para el análisis de datos gubernamentales que robustezca la toma de decisiones.
5. Innovación en TIC	El gobierno aprovecha su posición como un importante proveedor para estimular la demanda de TIC innovadoras; las políticas innovadoras mejoran los ciclos de adquisición y ofrecerán un mejor valor, de esta forma, como usuario de esta tecnología (i.e. recibos electrónicos) busca incentivar su adopción en otras arenas.
6. Alianzas estratégicas	Se exploran oportunidades de cooperación, alianzas y asociaciones con multinacionales acreditadas para maximizar el retorno de las inversiones y adoptar las mejores prácticas internacionales.
7. Datos de gobierno abierto	Facilitan el intercambio de información al interior del gobierno, así como al exterior con base en lo dispuesto por la ley. Los datos estructurados se publican de forma tal que se puedan interconectar (datos vinculados del gobierno abierto) y sean más útiles para las entidades gubernamentales, terceros y sistemas respectivos. La adopción de tecnologías de *Big Data* permite procesar datos complejos, mejorando la toma de decisiones en áreas críticas como finanzas, atención médica, transporte, servicios públicos y el medio ambiente.
8. e-democracia	Hay un compromiso gubernamental para utilizar las TIC y alentar a los ciudadanos a participar en la toma de decisiones de las autoridades e implementan iniciativas para mejorar la visibilidad, transparencia y rendición de cuentas del gobierno. Esto es posible observarlo en los esfuerzos para que los gobiernos locales y las organizaciones de la sociedad civil funjan como intermediarios con la ciudadanía y promuevan su involucramiento.
9. e-aprendizaje	Es establecida una infraestructura completa de TIC para educadores, estudiantes y padres, fomentando una mentalidad digital y ampliando las oportunidades de aprendizaje. Los educadores reciben apoyo para hacer un uso completo de las plataformas de aprendizaje electrónico y otras tecnologías de aprendizaje digital.
10. e-salud	Los ciudadanos son empoderados al proporcionarles un acceso seguro y fácil a sus registros de salud y los proveedores de atención médica obtienen acceso seguro a los registros de los pacientes. Esto se materializó a través del sistema myHealth en el que tanto médicos como pacientes pueden ver sus registros y acceder a diversos servicios.
11. Transporte	Se utiliza la tecnología digital en el transporte terrestre, marítimo y aéreo, con énfasis en el despliegue de sistemas inteligentes de transporte para mejorar la seguridad vial, el flujo de tráfico y los viajes dentro del país. La automatización de este servicio, por ejemplo, permite a los ciudadanos solicitar permisos relacionados con el transporte a través de formularios electrónicos.

FUENTE: elaboración propia con base en información del Gobierno de Malta (2019).

Este conjunto de condiciones ha derivado en el diseño de un robusto entramado institucional dirigido a facilitar la adopción de las TIC en distintos ámbitos del quehacer gubernamental. Un elemento central de este caso de estudio es el desarrollo de la estrategia digital nacional (Digital Malta) establecida en 2014 y diseñada bajo un horizonte temporal sexenal. Dicha estrategia está basada en tres componentes principales (véase cuadro 01).

Dado el alcance de este capítulo, nos centraremos en profundizar en el componente de gobierno digital con el propósito de conocer a detalle el conjunto de acciones que se han implementado en Malta para potenciar el uso de las TIC en la provisión de bienes y servicios públicos (véase cuadro 02).

Al observar este conjunto de acciones se descubre que la estrategia digital trasciende la adopción de TIC para la provisión de bienes y servicios, pues existen distintas acciones dirigidas al fortalecimiento de las capacidades gubernamentales, así como a mejorar los canales de interacción con la ciudadanía y el sector empresarial. Estas implican no sólo el establecimiento de infraestructura, sino la promoción de su adopción, así como las condiciones para garantizar su uso efectivo.

Así, para llevar a cabo las acciones de cada uno de estos tres componentes, Digital Malta recae, a su vez, en tres estrategias transversales dirigidas a acompañar estos esfuerzos, en concreto, la regulación y legislación, a la infraestructura y al capital humano (MCA, 2014).

Al respecto, la regulación en torno al gobierno electrónico se ha diseñado desde la perspectiva de establecer condiciones reglamentarias que favorezcan la implementación de las acciones de la estrategia digital nacional. En este tenor, la regulación diseñada en el caso de Malta está orientada por dos principios fundamentales:

a La legislación y la política en materia de TIC será no discriminatoria y tecnológicamente neutral. Promoverá la creación de valor, innovación y crecimiento en todas las industrias y la sociedad en general.

b Las medidas legislativas y las estrategias regulatorias promovidas en otras jurisdicciones serán monitoreadas y evaluadas para ver si se requieren mejoras en el nivel local (Gobierno de Malta, 2009).

En este sentido, un aspecto que vale la pena señalar es la importancia de que la legislación facilite las interacciones entre los distintos actores, es decir, que genere condiciones para que las acciones que se promuevan se den en un espacio de certidumbre. Es relevante aludir a lo discutido en el apartado teórico sobre el tema de la infraestructura, como una condición necesaria para la adopción del gobierno electrónico. La experiencia de Malta en este aspecto enfatiza la importancia de que dicha infraestructura, por una parte, atienda las necesidades técnicas del gobierno; mientras, por otra, tenga la flexibilidad suficiente para adaptarse a los cambios tecnológicos (Ramnarine y Endeley, 2008).

El tema del capital humano también es relevante en términos de que hay una necesidad de fortalecer las capacidades existentes para potenciar la utilidad de las TIC (UNESCO, 2002). Esto es observable en el caso de la adopción de tecnologías en el sector educativo en donde, además de la incorporación de TIC se contempló la capacitación de los profesores para su uso.

Por lo tanto, es posible concluir que, el gobierno electrónico de Malta sobresale por llevar un proceso dinámico: *1)* La digitalización de sus procesos externos es realizada por una organización gubernamental específica, lo cual concentra y especializa la fuerza de las autoridades para lograr que tal digitalización sea estratégicamente operativa, propiedad importante de gobierno electrónico como se mencionó previamente; *2)* Se establece un marco jurídico para facilitar la interacción digital mediante la regulación, con lo cual se protegen los derechos humanos y políticos, aspecto que también contribuye a disponer de un Internet libre; *3)* La promoción de la digitalización en actividades de la sociedad y del sector privado, dado que, aunque el gobierno electrónico sea una relación *top-down*, es menester que el receptor disponga de los medios para integrarse a dicha relación digital; esto procura el nivel mínimo de participación electrónica en la población, la capacidad electrónica en su aspecto material; *4)* La capacitación para utilizar eficazmente las TIC, con lo cual se cubre el aspecto cognitivo de la capacidad electrónica; y, *5)* Incentivar la innovación de las TIC, con lo cual se procura una constante modernización.

Así, cuando es digitalizado el gobierno de Malta, las autoridades simultáneamente procuran condiciones necesarias y

suficientes de la democracia electrónica: mientras los procesos son digitalizados, se crean igualitariamente condiciones reglamentarias y cognitivas para la libre, igual y eficaz utilización de las TIC en los asuntos públicos.

Islandia: La adopción de la e-democracia

El caso islandés provee información relevante sobre la implementación de un modelo de e-democracia con el que se han mejorado los mecanismos de inclusión ciudadana en la toma de decisiones al respecto de asuntos públicos, a partir de dos proyectos principales que se han documentado. El primero es la experiencia de la utilización del *crowdsourcing*[7] para la elaboración de una nueva constitución, descrito y discutido por Korthagen *et al.* (2019). De acuerdo con los autores, esta práctica fue resultado de las demandas ciudadanas, posteriores a la crisis financiera de 2008, por reformas estructurales en el país. La experiencia de Islandia preveía, en distintas fases del proceso de reforma constitucional, la participación de la ciudadanía utilizando las plataformas tecnológicas para la interacción. En primer lugar, logró insertarse el tema sobre la necesidad de una nueva constitución en la agenda parlamentaria, señalando la importancia de incorporar la participación ciudadana en este proceso. Posteriormente, se determinaron los criterios para dicha participación, los cuales incluyeron el establecimiento de una Asamblea Constituyente conformada por 25 ciudadanos electos por voto popular, así como la organización de un foro nacional donde 950 ciudadanos seleccionados aleatoriamente dieron su opinión acerca de aspectos clave del proyecto de reforma. El proceso continuó con la redacción del documento en el cual los ciudadanos podían hacer sugerencias para que este fuera aprobado por la asamblea (Korthagen *et al.,* 2017).

No obstante, a pesar de este proceso de carácter participativo, el resultado no fue el esperado:

7 De acuerdo con Brabham (2017), el *crowdsourcing* puede definirse como "un modelo de producción y resolución de problemas [...] en el cual las organizaciones aprovechan la inteligencia colectiva de las comunidades en línea" (1). En la línea de lo anterior, Ghezzi *et al.* (2017) abonan a la definición del *crowdsourcing* como un modelo que favorevce la co-creación y el involucramiento de las personas en los procesos de innovación de una organización.

> Durante las primeras tres fases, el pueblo de Islandia ha tenido bastante influencia en el proceso, pero en la última fase de toma de decisiones, la participación ciudadana se redujo considerablemente. La estrategia de redactar un borrador de constitución a través del *crowdsourcing* podría clamar legitimidad. Aun así, no es posible rastrear el aporte de los participantes al borrador final (Korthagen *et al.*, 2017: 182).

El borrador de la constitución derivado del experimento no fue aprobado por el parlamento islandés; así, la experiencia provee conocimiento interesante acerca de la factibilidad de replicar el modelo. Al respecto, Landemore (2014) plantea preguntas relevantes acerca de este ejercicio, por ejemplo, si en contextos con población menos homogénea podrían obtenerse resultados similares. Asimismo, dentro de los aprendizajes obtenidos por la autora destacan temas relacionados con los mecanismos para la participación de la ciudadanía, el nivel de involucramiento en las distintas etapas, así como la representatividad de las opiniones de los participantes. A pesar de que, como se señaló, este modelo de constitución no llegó a concretarse, sí representa un punto de partida importante sobre la forma en la que la e-democracia puede llevarse a la práctica.

El segundo proyecto del caso islandés es Your priorities, una plataforma informática impulsada desde la sociedad civil como una respuesta a la crisis democrática que vivió el país tras la financiera de 2008 (Jacobs, 2017).

La idea central de esta plataforma consiste en proveer un espacio

> De deliberación y generación de ideas en línea que conecta gobiernos y organizaciones [*sic*] sin fines de lucro con ciudadanos [los] usuarios agregan ideas, ven las ideas de otras personas y participan en una deliberación civil sobre cada idea. Sus prioridades se pueden usar en proyectos públicos en el contexto de incluir un gran número de ciudadanos en la toma de decisiones, y también en proyectos privados donde grupos más pequeños de personas pueden trabajar juntas de forma remota en ideas, deliberaciones y decisiones (Citizens, 2020).

Esta iniciativa, como explican sus promotores, busca "dar igualdad de oportunidades a las personas para que lo conozcan [...] al final, si las personas lo usan de manera efectiva, pueden hacer que las cosas sucedan, esta es una función democrática normal" (England, 2015). Dentro de los proyectos que promueve Your priorities, es posible identificar tres categorías principales: debate sobre políticas (*policy crowdsourcing*), presupuesto participativo, empoderamiento ciudadano a través de inteligencia artificial (Citizens Foundation, 2020).

Vale el esfuerzo profundizar en el funcionamiento de cada uno de esos tipos de proyectos con el fin de tener un mayor entendimiento de los procesos de deliberación que incorpora un modelo como el mencionado. El primero, el debate sobre las políticas se lleva a cabo a través de un mecanismo mediante el cual todos los participantes exponen argumentos a favor o en contra sobre un tema de política, incentivando la discusión; posteriormente, estos argumentos se votan y es posible, para los usuarios, identificar fácilmente el conjunto de argumentos presentados. Esta herramienta ha sido utilizada en, además de Islandia, países como Estonia, Noruega, Hungría, Croacia, entre otros.

El segundo, relativo al presupuesto participativo, tiene un carácter educativo que es importante destacar. Esta herramienta, por una parte, pretende generar mayor conciencia ciudadana sobre cómo se construye el presupuesto y sobre cómo se gasta. Por otra parte, busca facilitar el análisis de cuánto cuesta implementar las ideas propuestas por la ciudadanía. Un ejemplo de la instrumentación de esta herramienta se documentó en la ciudad de Reikiavik, a partir del proyecto My Neighbourhood, en el cual los habitantes de la ciudad pueden proveer ideas para mejorar sus vecindarios. Posteriormente, el gobierno local hace un análisis de los costos y la viabilidad de estas ideas, y las cuales son puestas a votación ciudadana a través de un mecanismo de voto electrónico. Un aspecto interesante es que pueden votar por medio de este los mayores de 16 años, mientras que otras elecciones la edad mínima son 18 años. Los ciudadanos pueden ver cómo se utiliza el presupuesto en los proyectos seleccionados (Citizens Foundation, 2020). La implementación de My Neighbourhood, desde su inicio en 2011, representa alrededor de 3 millones de euros al año destinados a proyectos de mejora comunitaria propuestos por los ciudadanos (Consejo de Europa, 2018).

La tercera categoría se refiere al uso de la inteligencia artificial en la generación de mejores condiciones para la participación ciudadana. De forma específica esta tecnología se utiliza para ayudar a los ciudadanos a eliminar prejuicios en las discusiones que tienen lugar en la plataforma informática y, de esta manera, apoyar la toma de decisiones a partir de acercarles la información que es considerada más relevante. Adicionalmente, el uso de esta tecnología favorece la disminución de los costos de la participación y la mejora de las condiciones para el involucramiento ciudadano (Bjarnason, 2017).

Del caso islandés se aprende, por lo tanto, sobre participación electrónica *top-down*, mostrando cómo pueden ser tratados los tres componentes del proceso: la provisión de información, organización de la deliberación y análisis gubernamental de las alternativas propuestas para someterlas a votación electrónica, posibilitando así una incidencia en los procesos decisionales.

Brasil: Los desafíos del voto electrónico

Las TIC en los procesos electorales han tenido distintos usos dirigidos a facilitar las distintas actividades que tienen lugar en esta materia. El caso del voto electrónico, por sí mismo, ha sido un elemento que se ha analizado principalmente a partir de las ventajas que se han identificado en términos de la reducción de costos, del manejo de información y de la obtención expedita de resultados. En este sentido, Tuesta (2007) identifica que este instrumento:

> Produce un impacto significativo en los materiales, actividades y procedimientos electorales: elimina las boletas de votación, el padrón de electores impreso, el acta electoral (y las copias), la urna o ánfora electoral, reduce las mesas de votación, los locales de votación, los miembros de la mesa, elimina los votos por error, el llamado "error material", disminuye el tiempo de entrega de los resultados, elimina el resultado provisional, reduce el personal eventual contratado para un proceso electoral y ahorra en el presupuesto público en el mediano plazo (954).

La adopción de un modelo de voto electrónico, además, ha generado discusiones relevantes acerca del nivel de seguridad que provee y de la confianza que genera en los votantes (Alvarez *et al.,* 2018; Wang *et al.*, 2017). El tema de seguridad ha sido un aspecto central en el análisis de los sistemas de votación electrónicos. En Noruega, por ejemplo, recientemente un grupo de investigadores puso a prueba la seguridad informática de su sistema de voto electrónico, señalando distintos escenarios desde los cuales este puede vulnerarse a partir de que alguno de los elementos esté corrompido (Cortier y Wiedling, 2017). La seguridad informática de los sistemas ha sido objeto de estudio en los últimos años, enfatizando la importancia de desarrollar protocolos que garanticen la secrecía del voto (véase, por ejemplo, Yavuz *et al.,* 2018; Hjálmarsson *et al.,* 2018). El debate sobre el uso del voto electrónico presenta distintos argumentos acerca de las ventajas de su utilización, así como al respecto de las consideraciones que deben tomarse en cuenta para su instrumentación (Adeshina y Ojo, 2017; Gibson *et al.,* 2016).

Así, la revisión de la experiencia brasileña resulta pertinente en virtud de dos razones principales. La primera es que existe un importante cuerpo de evidencia sobre la utilización del voto electrónico que provee un entendimiento más preciso de cuáles han sido los alcances y limitaciones del uso de este instrumento. La segunda es que representa un caso con mayores similitudes al mexicano, por lo que las lecciones que se deriven de su estudio pueden estar más vinculadas con la realidad del país.

La adopción del voto electrónico en Brasil estuvo motivada, fundamentalmente, por la crisis de desconfianza y legitimidad en el sistema electoral. Este proceso lo describen detalladamente Lheureux de Freitas y Macadar:

> A principios de 1995, el Tribunal Superior Electoral (TSE) nombró una comisión de expertos electorales (jueces, técnicos de TI, administradores) cuya tarea era establecer la votación eléctrica. Cuatro meses después, la comisión proporcionó las pautas para el voto electrónico brasileño, tales como: máquinas independientes que funcionan con electricidad y batería (partes de su territorio comprendidas por bosques donde las personas necesitan votar), interfaz numérica, hardware personalizado, impresión de votos, fusión de las estaciones de votación para disminuir la cantidad total, votación electrónica a 30 millones de votantes en 1996, etc. Además, la comisión redactó un proyecto de ley que habilita y dictamina la votación electrónica [futura ley 9.100, 29 de septiembre de 1995] (2017: 62).

La transición hacia esta modalidad de votación se completó en el nivel nacional en el año 2000, después de un proceso de aproximadamente cuatro años con el fin de establecer las condiciones para su utilización (Arahna y van de Graaf, 2018), en donde el desarrollo de infraestructura y capacidades favorecieron la institucionalización de estas prácticas. Desde entonces, se ha gestado un debate sobre su efectividad basado predominantemente en el cuestionamiento de la seguridad que ofrece. En este sentido, Filho apunta que el caso brasileño "muestra que el voto electrónico puede proporcionar una gran rapidez en la presentación de resultados pero que tal velocidad muy difícilmente está acompañada por la fiscalización, comprometiendo la transparencia del proceso electoral" (2005: 4).

Es, por tanto, relevante señalar que la discusión sobre la efectividad de este modelo en el caso brasileño se centra en ponderar el incremento de la eficiencia del sistema, por ejemplo, en lo relativo al conteo de los votos, con la posible vulnerabilidad que presenta en términos de seguridad, lo cual se traduce en cuestionamientos sobre su legitimidad.

En lo relativo a las ventajas de la adopción del voto electrónico, Bhering (2013) alude a aspectos como la mejora en los procesos de registro de votantes y conteo de votos, en consecuencia, mejoras también en los tiempos de difusión de los resultados, así como mayor transparencia. Las ganancias en eficiencia no son un elemento menor en el contexto brasileño dada la magnitud de su padrón electoral, el cual, en 2018, estaba compuesto por poco más de 147 millones de personas (TSE, 2018). Otro aspecto importante es que la utilización del voto electrónico ha facilitado este proceso para el electorado, simplificándolo a partir de presentarle en la pantalla el nombre y fotografía de los candidatos, en contraste con el sistema

anterior en donde el votante debía escribir en la boleta el nombre del candidato de su preferencia (Dias y Teles, 2018).

A pesar lo de anterior, los cuestionamientos, centrados en la vulnerabilidad de la seguridad, al sistema de voto electrónico en Brasil no han estado ausentes del debate. Aranha *et al.* (2014), por ejemplo, identificaron distintas áreas de vulnerabilidad en los sistemas de voto electrónico que demandaban, desde sus perspectivas, ajustes informáticos. En la misma línea, Aranha y Pilla (2018) enfatizan que estos temas siguen estando presentes en la discusión y que, incluso, ha suscitado la reconsideración sobre la pertinencia de volver al modelo de boletas electorales impresas. Asimismo, también se han documentado críticas a la implementación del sistema de voto electrónico en Brasil, derivadas de las condiciones del país en términos de desigualdad, analfabetismo, entre otras (Hapsara *et al.,* 2016).

En términos generales, esta experiencia destaca la necesidad de analizar, de acuerdo con el contexto, las condiciones que existen para migrar a un sistema de votación electrónica. Por una parte, la automatización de los procesos inherentes a la función electoral pueden contribuir al incremento de la eficiencia; por otra, los cuestionamientos relativos a la seguridad pueden mermar la confianza en este modelo, es aquí precisamente donde, aludiendo a lo discutido en el apartado teórico, el tema de la infraestructura tecnológica no garantiza la implementación eficaz de un modelo de esta naturaleza. El caso brasileño muestra la implementación de las condiciones necesarias para la democracia electrónica, pero no una garantía de sus condiciones suficientes.

REFLEXIONES FINALES

El propósito central de este capítulo ha sido discutir algunos de los elementos más relevantes para el establecimiento de la e-democracia. La primera parte, centrada en el ámbito teórico provee lecciones interesantes que vale la pena recapitular, en especial, porque aluden a las condiciones, tanto necesarias, como suficientes, para examinar la relación entre la infraestructura tecnológica, el gobierno electrónico, la e-democracia, participación electrónica y gobernanza electrónica, haciéndose

más complejas sus propiedades durante la transición. Así, de estas discusiones destacan los siguientes puntos:

- Como una condición necesaria, la existencia de infraestructura tecnológica posibilita, por una parte, la automatización de procesos y servicios; mientras, por otra, el establecimiento de canales de interacción entre distintos actores, por ejemplo, autoridades y ciudadanos. No obstante, la existencia de infraestructura tecnológica *per se* no garantiza la adopción efectiva del gobierno electrónico ni de la e-democracia.
- Sobre esto, es relevante aludir al gobierno electrónico como una herramienta que, precisamente a partir del uso estratégico de la tecnología, busca simplificar y aumentar la eficiencia de sus tareas y, con base en esto, se establece una relación *top-down* entre gobierno y ciudadanía.
- El caso de la participación electrónica, por su parte, representa una interacción más compleja dado que involucra relaciones tanto *top-down* como *bottom-up* entre el gobierno y la ciudadanía. Esto amplía la capacidad de injerencia de los ciudadanos al trascender del ámbito de los servicios públicos a la capacidad de involucrarse en distintas etapas del proceso de políticas públicas.
- Más allá del uso de las TIC en distintos procesos gubernamentales, la e-democracia implica múltiples niveles de utilización que pueden derivar en un mayor nivel de interacción entre sector público, privado y social.
- Dentro de estas discusiones sobre las condiciones necesarias y suficientes, la literatura también hace referencia a la libertad del Internet, siendo una condición necesaria de la e-democracia para garantizar la libre interacción entre ciudadanos y gobierno.

De igual forma, este capítulo también ha permitido la discusión de aspectos empíricos de los modelos a partir de tres casos de estudio de los cuales se desprenden las siguientes lecciones:

- En el caso de Malta, en donde se han promovido importantes esfuerzos en materia de gobierno electrónico, se identifica que una política de este tipo requiere una serie de acciones para

establecer las condiciones necesarias para su funcionamiento, esto incluye, por ejemplo, creación de organizaciones específicas para la implementación de esta política, adaptación del marco jurídico y promoción de uso de las tecnologías de la información y la comunicación.

- Asimismo, este ejemplo también provee una lección interesante en relación con la importancia de que el marco jurídico facilite las interacciones entre los distintos actores, generando un ambiente de certidumbre.
- La capacitación del capital humano también es importante, dado que así se potencia la utilización eficaz de las tecnologías de la información y la comunicación.
- El caso de Islandia, con la promoción de plataformas como Your priorities, permite identificar los distintos canales de interacción que pueden establecerse entre gobierno y ciudadanía.
- En específico, la experiencia de Your priorities muestra las condiciones que favorecen el debate público y la participación activa de la ciudadanía en la toma de decisiones sobre asuntos que le afectan, al destacar la importancia de transmitir conocimientos a la ciudadanía acerca del funcionamiento del proceso de políticas públicas.
- El tipo de participación que documenta el caso islandés enfatiza la forma en la que pueden implementarse mecanismos de interacción digital que permitan la provisión de información, organización de la deliberación y análisis gubernamental de las alternativas propuestas ciudadanas para someterlas a votación electrónica, posibilitando así una incidencia en los procesos decisionales.
- La experiencia brasileña, con la implementación del voto electrónico, favorece también la identificación de dos aspectos importantes: el primero es la importancia de garantizar la certidumbre en el proceso, en este caso, la secrecía del voto; el segundo es la importancia de ponderar las potenciales ganancias en eficiencia con la vulnerabilidad del sistema que puede traducirse en cuestionamientos a la legitimidad.

Así, tanto las discusiones teóricas como la experiencia empírica presentadas en este texto dan cuenta de que el gobierno electrónico, la participación electrónica y, en un nivel de mayor desarrollo, la e-democracia, funcionan con condiciones específicas, las cuales trascienden la mera disponibilidad de infraestructura tecnológica pues requieren, según sea el modelo, la digitalización estratégica, la reglamentación que otorgue certidumbre a los actores en sus interacciones digitales, un Internet libre, la promoción de la utilización de las TIC y la posibilidad de canales electrónicos para que los ciudadanos, con un menor costo de participación y mayor eficiencia, incidan en los procesos decisionales de las autoridades.

BIBLIOGRAFÍA

Ackermann, T., Miede, A. Buxmann, P. y Steinmetz, R. (2011)). "Taxonomy of Technological IT Outsourcing Risks: Support for Risk Identification and Quantification". 19° European Conference on Information Systems, Finlandia.

Adeshina, S.A. y Ojo, A. (2017). Factors for e-voting adoption -analysis of general elections in Nigeria. *Government Information Quarterly* (en prensa).

Aguilar, L. F. (2016). *Democracia, gobernabilidad y gobernanza*. México: Instituto Nacional Electoral.

Alvarez, R.M., Levin, I. y Li, Y. (2018). Fraud, convenience, and e-voting: how voting experience shapes opinions about voting technology. *Journal of Information Technology & Politics, 15*(2), 94-105.

Aranha D.F., Karam, M.M., Miranda, A. y Scarel, F. (2014). Software vulnerabilities in the Brazilian voting machine. En En D. Zissis y D. lekkas. *Design, Development, and Use of Secure Electronic Voting Systems* (149-175). Estados Unidos: IGI Global.

Aranha, D.F. y van de Graaf, J. (2018). The Good, the Bad, and the Ugly: Two Decades of E-Voting in Brazil. *IEEE Security & Privacy, 16*(6), 22-30.

Aristóteles (2011). *Ética nicomáquea*. Madrid: Gredos.

Bannister, F. y Connolly, R. (2012). Defining e-Governance. *e-Service Journal 8*(2), 3-25.

Beetham, D. (2004). Towards a Universal Framework for Democracy Assessment. *Democratization, 11*(2), 1-17.

Bhering, P. C. (2013). "El voto electrónico en Brasil". Seminario Internacional: Experiencias comparadas en la implementación del voto electrónico, celebrado en Lima, Perú del 22 al 23 de octubre.

Bryson, J.M., Crosby, B.C. y Bloomberg, L. (2014). Public value governance: moving beyond traditional public administration and the new public management. *Public Administration Review, 74*(4), 445-456.

Chatelanat, C. (2011). *La démocratie électronique: un catalyseur de participation et de légitimité pour l'Union européenne? Collection Euryopa,* 72. Genève: Institut Européen de l'Université de Genève.

Citizens Foundation (2020). *Citizens Foundation. Connecting Governments & Citizens. Islandia*. Recuperado de https://bit.ly/3pOBIM7

Consejo Europeo (2009). *La démocratie électronique. Recommandation CM/Rec(2009)1 et exposé des motifs*. EU: Publishing Editions Conceil of Europe.

Copi, I. M. y Cohen, C. [1953] (2016). *Introduction to Logic*. USA: Routdlege.

Cortier, V. y Wiedling, C. (2017). A formal analysis of the Norwegian E-voting protocol. *Journal of Computer Security,* (25), 21–57.

Dahl, R. [1989] (1992). *La democracia y sus críticos*. España: Paidós.

Diamond, L. y Morlino, L. (Eds.). (2005). *Assessing the Quality of Democracy*. Baltimore: Johns Hopkins.

Dias, M. y A. Teles (2018). Vote in Brazil and general elections 2018: are the pillars of democracy in danger? *Global Journal of Politics and Law Research, 6*(6), 1-15.

Dunleavy, P. (2006). New public management is dead-long live digital-era governance. *Public Administration. Res. Theory, 16*(3), 467-494.

England, P. (2015). Priorities of the people: an interview with Iceland's Citizens Foundation. Recuperado de de https://bit.ly/3HNjVep

Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M. y Hjálmtýsson, G. (2018) "Blockchain-Based E-Voting System". 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, 983-986.

Filho, A.B. (2005). El Voto Electrónico en Brasil. En *Voto Electrónico - Las nuevas tecnologías en los procesos electorales*. Buenos Aires: Grupo Editorial Planeta.

Freedom House. (2019). *Freedom on the Net 2019: The Crisis of Social Media*. Washintong DC: Freedom House.

Gerring, J. y Thacker, S.C. (2008). *A Centripetal Theory of Democratic Governance*. NY: Cambridge University Press.

Gibson, J. P., Krimmer, R., Teague, V. y Pomares, J. (2016). A review of E-voting: the past, present and future. *Annals of Telecommunications,* (71), 279-286.

Grindle, M. (2010). "Good Governance: The Inflation of an Idea". HKS Faculty Research Working Paper Series, RWP10-023, John F. Kennedy School of Government, Harvard University.

Grönlund, A. (2002). *Electronic Government: Design, Applications and Management*. USA: Idea Group Publishing.

Grönlund, A. y Horan, T. A. (2004). Introducing e-Gov: History, Definitions and Issues. *Communications of the Association for Information Systems, 15*(39), 713-729.

Hacker, K. L. y Van Dijk, J. (2000). What is the Digital Demoracy? En Hacker y Van Dijk (eds.). *Digital Democracy. Issues of Theory and Practice*. New Delhi: Sage.

Hapsara, M. Imran, A. y Turner, T. (2016). "E-Voting in Developing Countries. Current Landscape and Future Research Agenda". International Joint Conference on Electronic Voting, 36-55.

Hennen, L., Van Keulen, I., Korthagen I., Aichholzer, G., Linder, R. y Nielsen, R.Ø. (eds.) (2020). *European E-Democracy in Practice*. Suecia: Springer.

Houston, M. (2016). "Inside government: the role of policy actors in shaping e-democracy in the UK". Tesis doctoral. University of Southampton.

Janssen, M., Scholl, H.J., Wimmer, M.A. y Yao-hua, T. (eds.). Electronic Government: Proceedings of the 10th IFIP WG 8.5 International Conference, EGOV 2011 (Lecture Notes in Computer Science), Vol. 6846. Delft, The Netherlands, 345–354.

Kneuer, M. (2011). Deficits in Democratic Quality? The Effects of Party-System Institutionalisation on the Quality of Democracy in Central Eastern Europe. En G. Erdman, y M. Kneuer (eds.). *Regression of Democracy?* Países Bajos: VS Verlag.

Kneuer, M. (2016). E-democracy: A new challenge for measuring democracy. *International Political Science,* (37), 666-678.

Korthagen, I., Van Keulen, I., Hennen, L., Aichholzer, G., Rose, G., Linder, R., Goos, K. y Nielsen, R.O. (2018). *Prospects for e-democracy in Europe: Part II: case studies*. Brussels: EPRS/STOA.

Lee, C., Chang, K. y Berry, F.S. (2011). Testing the Development and Diffusion of E-Government and E-Democracy: A Global Perspective. *Public Administration Review, 71*(3), 444-454.

Limongi, F. (2016). *Access to electoral rights Brazil*. Italy: EUDO Citizenship Observatory.

Macintosh, A. (2004). "Characterizing E-Participation in Policy-Making". Proceedings of the Thirty-Seventh Annual Hawaii International Conference on System Sciences (HICSS-37), January 5-8, Big Island, Hawaii.

Mackie, J. L. (1980). *Cement of the universe: A study of causation*. Oxford, UK: Clarendon Press.

Mahoney, J. y Vanderpoel, R.S. (2015). Set Diagrams and Qualitative Research. *Comparative Political Studies, 48*(1), 65-100.

Mahoney, J., Kimball, E. y Koivu, K.L. (2009). The Logic of Historical Explanation in the Social Sciences. *Comparative Political Studies, 42*(1), 114-146.

Mossberger, K., Tolbert, C.J. y McNeal, R.S. (2008). *Digital Citizenship: The Internet, Society and Participation*. Cambridge, MA: MIT Press.

O'Donnell, G. (2004). Human Development, Human Rights, and Democracy. En O'Donnell, J. Cullel y O. Iazetta (eds.). *The Quality of Democracy: Theory and Application* (9-92). Notre Dame, IN: University of Notre Dame Press.

OECD (2003). *Promise and Problems of e-Democracy. Challenges of Citizen Engagement*. Paris: OECD.

Päivärinta, T. y Sæbø, Ø. (2006). Models of E-Democracy. *Communications of the Association for Information Systems, 17*(1), 6-27.

Platón (2011). *Político*. Madrid: Gredos.

Prins, C., Cuijpers, C., Lindseth, P.L. y Rosina, M. (2017). *Digital Democracy in a Globalized World*. USA: Edward Elgar Publishing, Inc.

Ruzaini S. A., Azlinah, M., Arshad, N.H. (2007). "Preliminary Study on Risk Management in E-Government Outsourcing Projects". 6th WSEAS International Conference on E-ACTIVITIES, 361–366.

Sartori, G. (1970). Concept Misformation in Comparative Politics. *The American Political Science Review, 64*(4), 1033-1053.

Sundberg, L. (2019). Electronic government: Towards e-democracy or democracy at risk? *Safety Science,* (118), 22-32.

Tribunal Superior Eleitoral (tse) (2020). *Estadísticas eleitorais. Brasil*. Recuperado de https://bit.ly/2yg2NQO

Tuesta, F. (2007). El Voto Electrónico. En *Treatise on Compared Electoral Law of Latin America* (952-974). Estocolmo, Suecia: International Institute for Democracy Electoral Assistance (IDEA).

Van der Meer, T. G. L. A. Gelders, D. y Rotthier, S. (2014). e-Democracy: Exploring the Current Stage of e-Government. *Journal of Information Policy,* (4), 489-506.

Van Dijk, J. (2013). Digital Democracy: Vision and Reality. En I. Th. M. Snellen, W. B. H. J. van de Donk y M. Thaens (Eds.). *Public Administration in the Information Age: Revisited* (221-234). Amsterdam: IOS Press.

Vedel, T. (2003). L'idée de démocratie électronique: origines, visions, questions. En P. Perrineau, (ed.). *Le désenchantement démocratique* (243-266) La Tour d'Aigues: L'Aube.

Wang, K., Mondal, S.K., Chan, K. y, Xie, X. (2017). A Review of Contemporary E-voting: Requirements, Technology, Systems and Usability. *Data Science and Pattern Recognition, 1*(1), 31-47.

Welp, Y. (2011). Latinoamérica conectada. Apuntes sobre el desarrollo de la democracia electrónica. En Welp *et al.* (2011). *Voto electrónico y democracia directa*. México: Flacso.

Wiener, N. [1948] (1984). *Cybernetics or control and communication in the animal and the machine*. Masss MIT Press.

Wiener, N. (1952). *Cybernetique et société*. París: Deux Rives.

Yavuz, E., A. K. Koç, U. C. Çabuk y Dalkılıç, G. (2018). "Towards secure e-voting using ethereum blockchain," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), Antalya, 1-7.

Ziegler, J. (2016). Cyberdémocratie et démocratie participative. *L'Internet et la démocratie numérique* (155-171). Perpignan: Presses Universitaires de Perpignan.

CAPÍTULO 09

PARTICIPACIÓN CIUDADANA EN MÉXICO Y REFLEXIONES PARA SU INNOVACIÓN

ARAM BARRA RAMÍREZ*
PABLO COLLADA CHÁVEZ**

* Internacionalista por la Universidad de las Amércias (UDLA), Ciudad de México y maestro en políticas públicas y en administración pública por la New York University (NYU) y el University College London (UCL). Actualmente se desempeña como oficial de programa en Open Society Foundations.

** Sociólogo por la Universidad Nacional Autónoma de México (UNAM). Actualmente es consultor en materia de comunicación, impacto y filantropía en América Latina y miembro de diversos consejos directivos de organizaciones de la sociedad civil en México, Colombia y Chile.

El concepto *participación ciudadana* está en constante movimiento, y el último par de décadas ha significado una evolución importante en nuestro entender tanto de la ciudadanía, como de la participación. En ese sentido, los últimos años han significado un camino sinuoso, pero interesante para los mecanismos y la tecnología a nuestra disposición para incentivar, evaluar y fomentar dicha participación. Con este texto buscamos resumir el desarrollo de la participación ciudadana en México. Para ello, hemos dividido el análisis en tres secciones principales.

La primera se enfoca en el estado y el andamiaje legal e institucional para la participación en México, así como los mecanismos de participación directa y las nuevas plataformas digitales y de infoactivismo. A través de esta revisión, pretendemos plantear una mirada crítica de los avances, así como de los vacíos que aún observamos en este campo y posibles áreas de mejora e innovación.

Para ello, hacemos uso de ejemplos recientes, como el terremoto de 2017 en la zona centro de México, así como los incipientes resultados de la respuesta a la pandemia de Covid-19 en el mismo país. En ambos casos se hacen evidentes nuevas metodologías de participación.

La segunda sección de este texto plantea la necesidad de ampliar las definiciones de participación ciudadana para entender la constante retroalimentación que dan las acciones de calle con las realizadas en línea. La rápida evolución de herramientas digitales ha cimbrado cómo los mexicanos participan, planteando la necesidad de evaluar constantemente el tipo de estrategia al respecto.

A partir del análisis hasta aquí proyectado, la tercera sección del texto busca identificar los principales retos para la participación ciudadana en México, así como las oportunidades más evidentes, incluyendo los nuevos medios masivos de comunicación, el flujo de información y las nuevas guerras de des/información. Estos nuevos espacios plantean desafíos para participar, así como para acceder a esos espacios.

La ya no tan reciente aparición de *big data*, la agregación de grandes cantidades de pequeños datos, y su valor agregado para entender tendencias, también esbozan nuevos retos para la participación. Por ello, el texto concluye con una aproximación a las posibilidades que plantea la inteligencia artificial (IA) para generar posibilidades de participación y retroalimentación de manera masiva e inmediata.

SECCIÓN 1: LA PARTICIPACIÓN CIUDADANA EN MÉXICO

Hubo un tiempo cuando la ciencia política comparada sostenía que el único camino hacia la democracia era el de un sistema electoral mayoritario y una cultura política altamente homogénea. Sin embargo, el día de hoy, como ironiza el politólogo Gerhard Lehmbruch, parece que todos los caminos llevan a "la Roma de la democracia" (Schneider y Eberlein, 2015).

Distintas democracias contemporáneas están compuestas por representación proporcional y una sociedad profundamente dividida y, sin embargo, son estables y capaces de ser receptivas a cambios de gobierno e innovación política tanto como las democracias mayoritarias. De hecho, esto explica la reciente aparición en la literatura de términos como *democracia proporcional*, *democracia de negociación*, *democracia de consenso* y *democracia de poder compartido* –como demuestran Arend Lijphart y Lehmbruch (Lijphart, 1977, 1984, 1999, 2008 y 2013; Lehmbruch, 1967, 1992, 1996, 2003 y 2012).

En ese sentido, la democracia actual se compone por una sucesión de momentos que comienzan con un acto constituyente y suceden con el Estado de derecho, la participación, la responsabilidad, la deliberación, la transparencia, entre otros, sin que por ello se sustituya la legitimación democrática (Innerarity, 2020). Para esto último, Innerarity propone privilegiar un acto de constante equilibrio de los momentos, orquestando un conjunto de valores y procedimientos entre los que se encuentra la participación ciudadana.

Esto es, a la par de elecciones libres, juicio de los expertos, soberanía nacional, protección de las minorías, primacía del derecho, autoridades independientes, rendición de cuentas, deliberación, representación (por citar algunos), la democracia se degrada cuando la participación ciudadana se obstaculiza o se excluye. Como menciona Innenarity: "No hay democracia sin popularidad, efectividad y legalidad, pero tampoco donde una de esas dimensiones se impone o excluye a las otras. Se degrada la democracia cuando se absolutiza el momento plebiscitario

o la lógica del clic, pero también cuando entregamos el poder a los expertos e impedimos la circulación de las élites" (Innerarity, 2020).

Es en este marco que nos interesa observar la participación ciudadana, un concepto tan dinámico como su ubicación en el ejercicio del poder. Esto es, lo que en un momento dado de la historia se aceptó como una relación saludable entre los diferentes grupos de la sociedad, en otro resulta obsoleto. En ese mismo sentido, los mecanismos con los que un gobierno legitimaba antes sus decisiones, puede parecer autoritario después.

Esto es de particular relevancia ante el creciente desprestigio de gobiernos, instituciones públicas, partidos, así como amplios sectores políticos alrededor del planeta. Frente a ello, la participación ciudadana y la figura misma de la ciudadanía se vuelven clave para la legitimidad de la democracia y el pacto social del que depende el Estado. Sin participación ciudadana no hay democracia.

Cómo se implica a las sociedades en el gobierno debe ser entendido, por lo tanto, como:

> Una intervención continua en su propio autogobierno a través de una pluralidad de procedimientos, unos más directos y otros más representativos, mediante lógicas mayoritarias y otras que no lo son, donde sea posible rechazar pero también proponer, con espacios para el antagonismo pero también para el acuerdo, que politicen y despoliticen los asuntos según lo que convenga en cada caso, que permitan la expresión de las emociones tanto como el ejercicio de la racionalidad (Innerarity, 2020).

Este marco es importante para reflexionar sobre el ejercicio de la ciudadanía hoy día, así como sobre los elementos que la componen. Sin embargo, la pregunta sigue en la mesa: ¿qué es la participación ciudadana?

LA PARTICIPACIÓN CIUDADANA

En una diversidad de acuerdos y convenios se ha establecido que *la participación* es un derecho básico en la construcción de las

democracias. El precepto clave de ello es que la delegación del ejercicio del poder no es un acto incondicional irrevocable, y que es a través de la participación ciudadana como se generan balances en la administración del Estado.

Desde esa perspectiva, podemos decir que una sociedad democrática es aquella en la que sus individuos gozan de un pleno ejercicio de la ciudadanía entendida como:

> El derecho y la disposición de participar en una comunidad política, a través de la acción autorregulada, inclusiva, pacífica y responsable, con el objetivo de optimizar el bienestar público y garantizar la vigencia de los derechos civiles, políticos, sociales, económicos y culturales. Los elementos de la ciudadanía involucran la participación, la acción, la comunidad, el bienestar social y el reconocimiento del ciudadano a tener derechos y garantizar su defensa y apropiación (Martínez Colín, *et al.*, 2012)

Si bien la ciudadanía es un derecho, también es un ejercicio que se consolida por medio de la participación. Evidentemente, la primera no se condiciona a la segunda, pero es a través de ella, en sus diferentes formas, que se adquiere el sentido de colectividad; se dinamizan las interacciones sociales; se impulsa el diálogo, y se habilitan los contrapesos en un régimen democrático.

De la misma manera, si bien la acción de elegir autoridades por la vía libre es uno de los componentes más básicos y esenciales de la participación, es apenas el inicio de una relación amplia que incluye la evaluación del ejercicio gubernamental, la coparticipación en acciones y decisiones de interés público, y el balance constante la ejecución de recursos y el bienestar de las sociedades. En ese sentido, es importante reconocer la diversidad de enfoques y funciones de la participación y los mecanismos que debe adoptar en un afán de recoger diferentes posturas.

En 2016, el gobierno de Chile convocó al Consejo Nacional de Participación Ciudadana y Fortalecimiento de la Sociedad Civil con el objetivo de brindar recomendaciones sobre su ley en la materia (Congreso de la Ciudad de México, 2019). En su documentación, el consejo detalló los siguientes tipos de participación:

1 ***Participación institucionalizada:*** es toda aquella que la iniciativa gubernamental tiene regulada en una figura específica, abierta a la acción ciudadana, a la construcción de espacios y mecanismos de articulación entre las instituciones gubernamentales y los diversos actores sociales;

2 ***Participación no institucionalizada:*** es la acción colectiva que interviene y se organiza al margen de las instancias gubernamentales; su regulación, estrategias, estructura y movilización emana desde la organización de la sociedad;

3 ***Participación sectorial:*** es la protagonizada por grupos o sectores diversos organizados a partir de su condición etaria, sexual, de clase, de género, étnica o cualquier otra referida a necesidades y causas de grupo. Atiende a su campo de incidencia, no se remite necesariamente al ámbito territorial, sino que tiene un impacto general;

4 ***Participación temática:*** es aquella protagonizada por colectivos o grupos diversos organizados a partir de un campo de interés y de incidencia específico relacionado con su actividad y prácticas cotidianas, con la defensa de valores socialmente relevantes o con temáticas y problemáticas de interés público que no se remite necesariamente al ámbito territorial, sino que tiene un impacto general, y

5 ***Participación comunitaria:*** es el conjunto de acciones desarrolladas por diversos sectores comunitarios en la búsqueda de soluciones a sus necesidades específicas. Se encuentra unida al desarrollo territorial de un sector o una comunidad y tiene como eje el mejoramiento de las condiciones de vida en la misma. Los problemas de la comunidad pueden ser resueltos de manera endógena, sin requerir la iniciativa de entes externos. Las soluciones se ajustan a su entorno, porque surgen del consenso de sus integrantes.

Recuperamos esta clasificación, pues queremos resaltar la idea neurálgica de que el valor de la participación ciudadana es definido en función del peso que genera en una gobernanza democrática. En ese sentido, los mecanismos que facilitan dicha participación pueden ser, como vemos en el caso de Chile, variados. Sin embargo, en su esencia, significan la demostración práctica de un ejercicio pleno de derechos en una sociedad dada.

NIVELES DE PARTICIPACIÓN

La calidad democrática también está vinculada a los niveles y calidad de la participación ciudadana, a la incorporación de la población en los procesos de toma de decisiones y a la legitimidad del gobierno.
Luis F. Fernández, Nosotrxs

Es importante establecer que los mecanismos de participación tienen varias formas de interacción y que, a su vez, responden a diferentes objetivos. Los primeros esfuerzos de categorización fueron realizados a finales de los años sesenta por Arnestein en su escalera de participación y han sido sofisticados y ajustados en diversas ocasiones por personajes como Hambleton y Hoggett (1994) o Brager y Specht (1973) y su adaptación por Shandy Arnberg (1996), entre otros (Guillen *et al.*, 2009).

Esencialmente, esta nivelación sirve para identificar las diferencias entre grados de poder e influencia en los distintos tipos de participación. Así se definen desde los ejercicios más inocuos y de nula influencia, como informar pobremente o levantar encuestas a placer con grupos de ciudadanos, a otros niveles donde la interacción va adquiriendo mayor influencia con esquemas como las consultas más amplias y transparentes, la creación de consejos y los modelos de cocreación.

En la cima de esta escalera de participación se ubican los niveles de mayor influencia. En estos mecanismos, el poder ciudadano se vuelve constante y vinculante, que es el estado más alto posible. Su instrumentación se puede ver en parlamentos comunitarios o los presupuestos participativos en los que se desarrolla la propuesta, se elige, se opera y se evalúa, o en espacios de toma de decisión, como son los referendos y/o los plebiscitos.

TECNOLOGÍA CÍVICA

A medida que la tecnología ha sido integrada en más espacios de interacción humana, han ido surgiendo categorías que buscan nombrarla y definirla. Tal es el caso de las relaciones alrededor del espacio cívico que han utilizado tecnología para su facilitación o ampliación. Así, el concepto *tecnología cívica* es utilizado cada vez más comúnmente e incluso han surgido diversas definiciones.

USOS COMUNES DE TECNOLOGÍA CÍVICA

CUADRO 01.

Acción comunitaria	**Gobierno abierto**
Foros vecinales	Uso de datos
Financiamiento colectivo	Visualización y mapeo
Información colectiva y memoria	Transparencia y acceso a la información
Organización comunitaria	Votación
Intercambio entre pares	Retroalimentación
	Debate

FUENTE: Fundación Knight.

Derek Poppert (2018) se refiere a ella como la "tecnología usada para mejorar o influir de manera directa en temas de gobernanza, política o asuntos socio-políticos". Por otra parte, Jason Rowley (2016) habla del conjunto de "productos, plataformas y servicios diseñados específicamente para reducir la fricción entre ciudadanos y gobiernos, atender problemas sociales y motivar a las personas a estar más involucradas en sus comunidades".

Según la Fundación Knight –que durante años ha realizado investigaciones para entender las funciones, impacto y tipos de tecnología cívica– existen dos grandes "familias". La tecnología orientada a la acción comunitaria, y aquella asociada a las herramientas de gobierno abierto, y sus aplicaciones se pueden resumir en el siguiente cuadro.

Por otro lado, Poppert divide en tres los usos de la tecnología cívica:

1 ***GovTech:*** utilizada por gobiernos para mejorar la eficiencia interna y la entrega de servicios, así como para interactuar hacia afuera con ciudadanos.
2 ***Incidencia:*** usada por organizaciones de la sociedad civil, campañas políticas o ciudadanos comunes con fines sociales y políticos de incidencia.
3 ***Votación:*** empleada para mejorar los procesos de votación, ya sea guías de votación digital o herramientas para simplificar los registros.

Para propósitos de este texto, recuperamos el concepto de *tecnología cívica* como una clave que permite entender la retroalimentación entre los mecanismos de participación ciudadana y su nivel. Esto, a su vez, permite evaluar la calidad misma de la participación en función del papel que juega para legitimar la toma de decisión colectiva en un sistema de participación democrática. Dicho sea de paso, es en este marco conceptual como aquí evaluamos la innovación en la participación ciudadana.

Evolución de los mecanismos de participación en México

Tras una ola de gobiernos autoritarios en América Latina, los procesos de transición generaron la creación de fuerzas políticas diversas y confrontadas. Con esos equilibrios de contrapeso, la sociedad civil ha seguido siendo relevante para promover la articulación y el diálogo. En ese contexto, la transición democrática de México abarcó peculiaridades que derivaron en el ecosistema de participación que conocemos hoy en día.

Históricamente, la sociedad civil en México fue profundamente asistencial o funcional a las estructuras políticas y electorales para ganar el poder. Con la llegada del Partido Acción Nacional a la presidencia de la República en 2000 –tras 70 años de régimen político priísta– se creó una serie de instituciones y entidades autónomas. Estas desempeñaron un papel crucial para aclarar la importancia de una sociedad civil independiente, con fuertes capacidades de incidencia.

Veinte años después, surgen nuevos desafíos, a medida que un nuevo proyecto político autodenominado de izquierda es liderado por Andrés Manuel López Obrador (AMLO) al frente del poder Ejecutivo nacional. Si bien este nuevo momento se ha visto caracterizado por una confrontación directa entre el presidente y algunos miembros de la sociedad civil, los grupos empresariales o los medios de comunicación, es importante resaltar los avances relevantes que nos trajeron a la coyuntura actual.

En ese contexto, y como planteó Barczak (2001), las herramientas de democracia directa como el referéndum, la iniciativa popular o el plebiscito, garantizan a los ciudadanos una participación directa en los procesos de toma de decisión. En el caso del país, usando a la Ciudad de México como ejemplo, hay que recordar que el Estatuto de Gobierno del Distrito Federal, aprobado por el Congreso de la Unión en 1994, reconoció en el nivel local tanto mecanismos de iniciativa popular, como de plebiscito.

Este avance fue paradigmático en el país y únicamente hasta la reforma al artículo 71 de la *Constitución Política de los Estados Unidos Mexicanos*, publicada el 9 de agosto de 2012, es que se reconoció el derecho de los ciudadanos a impulsar iniciativas ciudadanas en el ámbito nacional. Desde entonces, el mecanismo ha sido utilizado poco –hubo 11 iniciativas entre 2012 y 2018–, de las cuales únicamente la llamada Ley 3 de 3 o la Ley General de Responsabilidades Administrativas fue publicada en el *Diario Oficial de la Federación* en 2016. Pero el ejercicio sirve para reflexionar sobre la importancia de construir canales de participación ciudadana accesibles, efectivos y baratos para la población.

SECCIÓN 2: AMPLIAR LA MIRADA DE LA PARTICIPACIÓN CIUDADANA

Relación entre mecanismos de participación y la crisis de representatividad

Como apunta Robert Dahl, "[a] medida que la cantidad de ciudadanos aumenta más allá de cierto límite –impreciso–, la proporción de ellos que puede congregarse para participar es forzosamente cada vez menor" (Dahl, 2000). Lo que es más, si a esto sumamos la actual degradación de la confianza en los partidos políticos y otros órganos de representación, es poco probable que los ciudadanos mantengan compromiso con su participación activa. O incluso, como plantea Pogrebinschi (2013), los ciudadanos buscarán participar principalmente en decisiones que consideran de gran relevancia, pero se desentienden del ejercicio participativo regular.

Si bien en las últimas dos décadas se estableció una diversidad de mecanismos de participación ciudadana como los antes mencionados y también la revocación del mandato, el cabildo abierto, los concejos vecinales, el presupuesto participativo y la consulta popular, los instrumentos no necesariamente han mejorado la confianza en partidos políticos y órganos de representación, incluso si abrieron la oportunidad para la participación ciudadana a través del voto directo y universal más allá de la elección de representantes.

De hecho, según la Encuesta Nacional de Cultura Política y Prácticas Ciudadanas de 2012, en México ocho de cada diez ciudadanos perciben la política como un tema muy complicado o algo complicado y 65% declaran tener poco interés en ella.[1] Sobre la necesidad que tiene nuestro sistema de contar con partidos políticos, un tercio de los encuestados los percibe como poco o nada necesarios. Del total de la población, 44% encuentra que para trabajar en una causa común resulta difícil o muy difícil organizarse con otros ciudadanos. Para ocho de cada diez, el voto es el único mecanismo disponible para decidir si el gobierno hace bien o mal las cosas.

Esta pobre percepción sobre los mecanismos de participación ciudadana se entiende, en parte, dados los pocos resultados que han generado hasta ahora. En el caso de la iniciativa ciudadana, nuevamente como ejemplo, parece que la herramienta sirve más para provocar una discusión legislativa que para modificar en sí el marco legal.

En ese sentido, la percepción de legitimidad e impacto se reducen, y los mecanismos pierden su valor, toda vez que en su práctica se diluye el espíritu de la participación ciudadana, ya sea por mala voluntad, desinformación o encubrimiento de la información, o por simulación política. Esto último ha sido una particularidad característica de la cultura política mexicana y se puede apreciar en los ejercicios antes referidos.

Otro ejemplo relevante es el del mecanismo de parlamento abierto que en muchos de los casos parece más una simulación de escucha o una herramienta para comprar tiempo en el proceso legislativo. Si bien la figura, novedosa e ideal, promueve un congreso democrático moderno donde la pluralidad, la diversidad, el

1 Quinta Encuesta Nacional de Cultura Política y Prácticas Ciudadanas, Segob, 2012.

escrutinio y la participación son el valor central, en la práctica han venido a sustituir los antiguos "foros", en los cuales los programas eran definidos por los congresistas mismos. Esto es, el parlamento abierto tiene poco de abierto en la práctica.[2]

La experiencia de los cabildos autoconvocados en Chile

A forma de experiencia comparada, vale el esfuerzo mirar los cabildos autoconvocados que emergieron en Chile, fruto de las masivas movilizaciones sociales de finales de 2019 y comienzos de 2020, y producto de los cuales el país avanza rumbo a un referéndum para iniciar la redacción de un nuevo texto constitucional. Estos cabildos, como su nombre lo indica, fueron autoconvocados por la ciudadanía misma para encontrarse en consultorios, recintos educacionales, juntas de vecinos, lugares de trabajo, centros culturales, o sitios que permitan la reflexión colectiva.

Hubo cabildos convocados por comunidades específicas, como la cultural y que se establecieron como ejercicios de diagnóstico, priorización de desafíos e ideas para el futuro. Ocurrió lo mismo en temas ambientales o de salud. Hubo jornadas dedicadas a la atención de temas barriales e incluso empresas que organizaron sus propios cabildos para tratar temas internos de funcionamiento y toma de decisiones, y de cómo imaginar el futuro.

A partir del estallido social de octubre de 2019, se realizaron centenares de ejercicios de deliberación colectiva. Muchos de ellos ni siquiera fueron sistematizados ni recogidos, pero detonaron un proceso de repolitización y promoción del tejido social que seguramente seguirá teniendo eco en la cultura de la participación autoconvocada en los años por venir.

Como vemos en el ejercicio del parlamento abierto *vs* los cabildos autoconvocados en Chile, la participación ciudadana encontrará la utilidad de los mecanismos según su eficiencia y transparencia, con el objetivo de gozar de legitimidad y, por lo tanto, de ser útiles en sí mismos. Para promover y robustecer la participación ciudadana, dichos mecanismos deben enaltecer la pluralidad y la diversidad, y reflejar la complejidad en las formas de organización e interacción social.

En la medida en la que estos mecanismos no respondan a las necesidades de representatividad de una sociedad dada, estructuras de la sociedad civil organizada con seguridad buscará mecanismos alternos de participación con el ánimo de incidir en el proceso de toma de decisiones públicas, ya sea en los poderes Legislativo, en el Ejecutivo o en el Judicial, dependiendo de su objetivo. Por ello, vale el esfuerzo reparar en el andamiaje para promover el asociativismo.

DERECHO Y PROMOCIÓN DEL ASOCIATIVISMO

El asociativismo en México es normado por la llamada Ley de fomento a las actividades realizadas por las organizaciones de la sociedad civil, donde se estipula un registro federal (a través de una clave referida como clave única de inscripción, Cluni) para acceder a apoyos y estímulos que otorguen las dependencias y entidades federativas. Más allá del conocido y criticado recorte presupuestal en años recientes para este tipo de actividad, es importante resaltar el burocrático y complejo proceso para establecer personería legal que permita la participación ciudadana.

En ese sentido, y al igual que con otros mecanismos de participación antes referidos, parece que el marco legal para las organizaciones civiles está pensado para desincentivar su existencia o continuidad. De hecho, esto se puede observar en el número de organizaciones que tiene México frente a otros países de similar tamaño: el registro oficial plantea la existencia de poco más 32 mil organizaciones, ubicando la media nacional en apenas 27 organizaciones por cada 100 mil habitantes, en tanto que en Estados Unidos la relación es de 670; en Chile 650; en Argentina 270 y en Brasil 170 (García, 2019).

Una de las razones detrás de esta disparidad sin duda tiene que ver con el número de pasos burocráticos y los costos asociados que representa registrar una organización civil en México, a diferencia de otros países, cuyo proceso se simplifica. Es normal escuchar en

[2] EPara leer más sobre el mecanismo de parlamento abierto, véase: "¿Para qué un Parlamento Abierto?", en Animal Político, refiriendo al caso de Fundar, Centro de Análisis e Investigación. Disponible en https://bit.ly/3HCoxUN

México de organizaciones que tardan hasta 10 meses en lograr abrir una cuenta de banco organizacional.

Si bien México avanzó de forma importante en la aprobación de nuevos mecanismos que permitieran la participación ciudadana de manera general, el uso de estos ha sido pobre y en parte se debe al poco esfuerzo invertido en permitir y promover el asociativismo en México, una tarea pendiente para los grupos que históricamente han fomentado la participación ciudadana.

LA PARTICIPACIÓN EN MÉXICO: DEL SISMO DE 1985 A LA PANDEMIA DE COVID-19

Como hemos visto hasta ahora, la participación ciudadana se ha encontrado con importantes obstáculos a lo largo de la historia nacional, transitando de un sistema democrático, con arraigadas prácticas autoritarias, a uno abierto, con incipientes mecanismos formales con los que en las últimas dos décadas apenas se experimentó.

Según, Jorge Javier Romero, en México:

> [a]demás de la profunda reforma electoral, basamento del nuevo pacto de elites, que finalmente periclitó con la elección federal del año pasado [2018], el cambio institucional de la segunda mitad de la década de 1990 incluyó una transformación profunda de la Suprema Corte de Justicia, para fortalecerla y convertirla en un tribunal de constitucionalidad, con capacidad para dirimir controversias entre poderes y entre órdenes de gobierno –federal, estatales y municipales–. Así emergió un nuevo régimen, que dejó atrás el consolidado en 1946, cuando se consolidó el arreglo de partido prácticamente único, como lo llamó el entonces presidente Ernesto Zedillo (Romero, 2019).

En ese sentido, superando la apatía generada por la cerrazón de un sistema democrático cuya alta concentración del poder facilitó la cleptocracia y la corrupción política, la participación ciudadana trascendió de manera orgánica los escasos y complejos mecanismos que

mantuvieron los costos de participación por el cielo. Esto se observa en la aparición misma de la llamada *sociedad civil organizada* a finales de la década de los años ochenta, particularmente en respuesta al terremoto de septiembre de 1985.

Con la aparición de nuevos mecanismos de participación y la reforma antes referida al tribunal supremo, la sociedad civil de la década de los años noventa adquirió una serie de nuevas habilidades y estrategias para incidir en los pesos y contrapesos del sistema democrático. La profesionalización de dicha participación se reflejó en esos años en la aparición de organizaciones dedicadas a temas específicos de interés público o a la especialización en algún proceso de incidencia en lo público.

Aunado al litigio estratégico, las herramientas de pedagogía y presión parlamentaria se multiplicaron con las plataformas que a partir de este siglo significaron las redes sociales, las nuevas tecnologías y la Internet como acelerador de la organización social. De hecho, sobra mirar algunos de los ejemplos que 30 años después produjo el terremoto de 2017 para entender la gigantesca evolución que la participación ciudadana tuvo en el país, ya sea en su cantidad, su calidad o los mecanismos y la efectividad que tienen las acciones realizadas.

El 19 de septiembre de 2017, tras un fuerte sismo en el centro del país, un grupo de ciudadanos (entre quienes se encontraban diversos activistas, periodistas y programadores) lanzaron el hashtag #Verificado19s para recuperar datos útiles. Según recuenta Sophia Hernández:

> Mientras algunos se enfocaron en la creación de un mapa digital que registrara derrumbes, edificios en riesgo de colapso, refugios y centros de acopio; otros trabajaron para crear una base de datos con información detallada sobre las necesidades y riesgos en tiempo real de cada ubicación, recopilando información con el apoyo de redes sociales. Esto llevó a la creación del hashtag #Verificado19s, en referencia a información verificada... (Hernández, 2017).

En un segundo momento, algunos grupos ciudadanos consolidaron esfuerzos de presión política con el objetivo de integrar un fondo único que, con los principios de transparencia y eficiencia, permitiera hacer frente a la duplicidad de funciones, al uso

clientelar de los programas sociales, a la corrupción y a la ausencia de coordinación entre los principales actores relevantes que participarían en los procesos de reconstrucción. La organización civil Nosotrxs convocó a colectivos de damnificados para trabajar en conjunto con las autoridades por una reedificación efectiva. El movimiento se convirtió rápidamente en un referente de organización de damnificados para externar los problemas y retos que enfrentaban diferentes grupos de personas afectadas por desastres naturales.

Ejercicios como los antes mencionados muestran con claridad una vibrante participación ciudadana que explota los recursos tecnológicos a la mano y trasciende los mecanismos formales de participación, para organizarse, incidir y movilizar a más personas. En otras latitudes, la mirada comparada nos recuerda las experiencias del Instituto Update (www.institutoupdate.org.br) y Nossas Cidades (www.nossas.org) en Brasil, o Ciudadanía Inteligente (www.ciudadaniai.org) en Chile.

Tras la facilidad que plataformas como Avaaz o Change.org ofrecieron a la ciudadanía para exigir atención o generar presión, las tres organizaciones antes mencionadas son experiencias de la intersección entre información, nuevas tecnologías y sistematización de metodologías para la movilización, la organización y la incidencia. Al observar su propia experiencia reiterada, estos órganos funcionan como plataformas de tecnología cívica que permiten agilizar y mejorar el impacto, con objetivo, de resultados.

En ese sentido, la innovación en la participación ciudadana desborda por fuera de los mecanismos formales de participación y promueve nuevas dinámicas en el sistema democrático. Esto se observa, más recientemente, en la respuesta que distintos grupos civiles tuvieron ante la pandemia de Covid-19 en México. La plataforma #MiBarrioMeRespalda (www.eldiadespues.mx) retoma el ejercicio de agregación de información y redireccionamiento de ayuda a nodos ciudadanos críticos o prioritarios, una experiencia que ya había probado ser efectiva en el sismo de 2017.

Mientras tanto, la plataforma VerifiCovid (www.verificovid.mx) diariamente publicó pequeñas cápsulas de audio identificando y corrigiendo noticias falsas que se transmiten en los medios nacionales. Serendipia (www.serendipia.digital), por su parte, retoma

los datos oficiales de las autoridades de salud y los convierte en *OpenData* agregada en archivos disponibles para la libre descarga de ciudadanos, analistas y periodistas.

Estas experiencias, apenas ejemplos dentro de un mar de acciones de participación, ofrecen una pequeña muestra del rico ecosistema que componen individuos, grupos civiles formales e informales, activistas, programadores y periodistas. Enfrentados ante un aparente rezago institucional que mantiene altos costos de entrada para la participación ciudadana, la reacción ante la emergencia y/o la oportunidad muestra la capacidad creativa que existe hoy en el espacio cívico en México.

SECCIÓN 3: RETOS A LA PARTICIPACIÓN CIUDADANA

Participación y democracia en el mundo digital

Los que hacen imposible una revolución pacífica
harán inevitable una revolución violenta
John F. Kennedy

El desarrollo y la adopción de herramientas digitales ha influido irreversiblemente en casi todos los ámbitos de las relaciones humanas. Desde la educación, hasta la salud o la agricultura, la tecnología ha sido integrada para cumplir con muchos objetivos, incluyendo facilitar el flujo de procesos para mejorar almacenamiento y tratamiento de información. Como revisamos, al hablar de "tecnología cívica", el impacto en la democracia y la participación no ha sido menor y esto aporta componentes positivos en respuesta.

Por un lado, se amplió la cantidad, calidad, accesibilidad y funciones de las herramientas asociadas a la participación. Empezando por el nivel más básico de acceso a la información, se han desarrollado diversas plataformas para obtener, entender y procesar datos; para hacerlos comprensibles. Con el avance de la tecnología, también se ha ampliado la capacidad de registro, memoria y difusión de hechos de interés público.

Cada vez es más sencillo recoger evidencia (fotos, videos, testimonios) sobre sucesos que puedan ser relevantes, y mostrarlos públicamente para denunciar, generar conciencia o simplemente promover la información de primera mano. Igualmente, se ha simplificado la construcción de herramientas que faciliten el acceso a registros históricos permitiendo, a su vez, dar seguimiento al avance de procesos o casos.

Para facilitar los ejercicios de toma de decisión, también se han diseñado diversas herramientas, algunas de las cuales incorporan espacios de deliberación para facilitar el intercambio de ideas. Otras permiten comentar o editar sobre propuestas o indicaciones existentes, y unas más habilitan la posibilidad de elegir entre diversas opciones y/o proveen información sencilla con el afán de facilitar la toma de decisiones. Desde esta perspectiva, la mayoría de los mecanismos tradicionales de participación –las asambleas, las elecciones, la colaboración, los debates, entre otros– tienen un correlato digital.

Una de las grandes promesas de la relación entre tecnología y democracia es la reducción de las barreras de entrada. La visión planteaba que con tan sólo un dispositivo electrónico y una conexión a Internet, cualquier persona podría participar en el debate público de manera directa y desde cualquier lugar. Si bien, efectivamente, la tecnología ha habilitado muchos y muy diversos espacios, en una serie de análisis de casos como el de Tiago Peixoto y Micah Sifry (2017), se ha identificado que más no necesariamente significa mejor participación o participación más diversa.

Con la llegada de plataformas digitales para recibir denuncias ciudadanas o para fomentar el diálogo entre ciudadanía y autoridades, se ha documentado que, si bien ha aumentado la cantidad total de personas que se involucran, el perfil de quien más participa y la voz que más peso tiene suele venir primordialmente de hombres con altos niveles de educación y en zonas urbanas, quienes ya conformaban el grupo de población que participaba con anterioridad. De ahí se desprende, quizá, el aspecto más negativo o peligroso de la infraestructura digital para la participación: que se abran más alternativas con el objetivo de que más personas se involucren, pero que al final sean escuchadas las mismas voces de siempre.

Por ello es importante establecer una serie de pautas al abordar los beneficios y objetivos de las plataformas digitales como parte de esquemas de participación amplios. Algunos puntos por tomar en cuenta son los siguientes:

— **Complemento, no suplemento:** las herramientas digitales han llegado a ampliar la oferta de la participación y ahí está su valor, no en suplir los mecanismos existentes. Incluso es preferible que haya mecanismos redundantes a que haya áreas de la vida pública que sean impenetrables para quien tenga interés en involucrarse.

— **Acercarse a donde está el movimiento:** es común que, cuando hay una iniciativa o entidad interesada en promover algún esquema de participación, se piense que crear una herramienta para ese fin es la mejor idea. Sin embargo, tanto por eficiencia en los recursos por invertir, como por la eficacia en facilitar la interacción, la mejor opción es buscar las herramientas que ya están siendo utilizadas por los grupos objetivo con quien se quiere trabajar, y procurar integrar en ellas los temas con que se pretende fomentar mejor participación. Por ejemplo, si se quiere promover un debate sobre un tema en particular, en lugar de crear una herramienta con la cual se transmita e invite a conocer más, siempre será más eficaz sumarse a las redes sociales, medios o entornos digitales donde la gente ya participa, y abrir el debate ahí.

— **La flexibilidad abre posibilidades:** cuando una reunión o asamblea presencial se extiende más de la cuenta, suele generar agotamiento o hartazgo. Incluso puede desincentivar a que las personas regresen. Sin embargo, en el mundo digital, si una persona quiere pasar de cinco debates de manera simultánea y tiene el interés de participar durante 10 hs seguidas en una discusión, es viable. Las herramientas digitales deben proveer a la persona participante la posibilidad de informarse más o participar más si lo desea, y consultar más si así lo requiere. En ese sentido, claramente tiene que existir la capacidad instalada para administrar esta diversidad, pero permitir un involucramiento a la medida, interés y capacidad. Como elemento adicional, es importante

entender que, a medida en que las generaciones son cada vez más nativas digitales, el consumo de información se vuelve insuficiente ante la capacidad y necesidad de asumir el protagonismo en la generación de contenido. Si existe desconocimiento de la cultura digital de las poblaciones a quienes se pretende incluir, probablemente no se aproveche todo el potencial disponible.

— **Retorno de la inversión participativa:** si una persona participa algunas veces y su inversión de tiempo y dedicación no genera ninguna respuesta, probablemente termine con frustración y desinterés de regresar a involucrarse en el espacio cívico. Una de las grandes virtudes de las herramientas digitales es su capacidad para automatizar todos, varios o algunos de sus procesos. En ese sentido, las herramientas digitales de participación deben contar con avisos que le permitan a la gente saber en qué se está convirtiendo el tiempo e ímpetu que le ha dedicado a su causa, y saber, asimismo, cuáles son los siguientes pasos, incluso si los resultados pudieran no ser favorables.

— **La ciudadanía perfecta es un unicornio:** uno de los grandes objetivos de la tecnología es simplificar la complejidad y reducir las barreras de entrada a la construcción y fortalecimiento de las democracias. Si al diseñar herramientas o procesos digitales imaginamos que quien participe será una persona ejemplar, informada, con tiempo disponible y voluntad en cuantas etapas sea necesario, probablemente nos encontremos con que esas personas en la realidad sean muy pocas. Es imperativo abrir los espacios digitales con lo más básico e ir abriendo otros más a medida que el interés de las personas lo impulse. Si tenemos que dar una serie de talleres para explicar cómo se utilizan las herramientas de participación, lo más probable es que caigan en desuso antes de ser adoptadas.

— **Transparencia en todo el proceso. Todo:** es importante que, si se pretende fomentar una democracia más activa, con una mejor distribución del poder, las herramientas digitales que acompañen esta inquietud deben ser transparentes al clarificar desde su objetivos, hasta su proceso de diseño, los algoritmos que utiliza y los resultados que obtiene. Si una persona que participa es incapaz de ver cómo se procesa la información que genera y en qué deriva, será imposible reconocer que la democracia en realidad se está fortaleciendo y sólo se seguirá reproduciendo el modelo de "todos participamos, pero sólo los mismos de siempre deciden". Además, es importante, siempre, asegurar a quien participe que sus datos personales serán protegidos según las regulaciones pertinentes.

— **Atender la brecha digital:** se entiende por ésta la relación entre las personas que tienen acceso y conocimiento de las tecnologías de información y comunicación (incluyendo la conectividad) y quienes no. Si bien cada día hay más personas vinculadas, la realidad es que existen muchas brechas en las que se profundiza esta diferencia. En México, un país con profundas y diversas desigualdades, la diferencia no puede verse únicamente en el número absoluto de personas conectadas, sino en las diferencias por sector. Existe una brecha profunda entre los sectores urbano y el rural, así como brechas generacionales. Con esa comprensión en la complejidad, es importante diseñar procesos que atiendan todas las variables y que ofrezcan mecanismos capaces de incluir a las mayorías y las minorías.

— **Atender la brecha democrática:** en seguimiento a varios de los puntos anteriores, es importante reconocer que en una población siempre existirán diferentes niveles de conocimiento y capacidad respecto del funcionamiento de las democracias, sus estructuras y las decisiones que están en juego. Lejos de ver esto como una condición de exclusión en la que únicamente las personas más informadas puedan participar, debe ser la pauta para el diseño de herramientas –digitales y no– capaces de recoger la diversidad de conocimientos e inquietudes, y de procurar una constante capacitación en cultura cívica.

Si una herramienta digital restringe más que habilitar, si desincentiva más que motivar, si aliena más que integrar, entonces no está cumpliendo su objetivo más esencial. En ese sentido, es importante

reconocer que no hay una herramienta o mecanismo de participación que sea una *bala de plata* y que sea capaz de satisfacer todas las necesidades para todos los grupos en todas las ocasiones.

Con ese reconocimiento, es importante establecer que el mejor modelo de participación es aquel que abre los escenarios suficientes para recoger la mayor cantidad de las voces de una sociedad, ya sea presencial o digitalmente, para poblaciones con más o menos conocimiento. Además, se debe reconocer que la diversidad de raza, género y etnia, en la participación, siempre será condición de mayor riqueza, legitimidad y confianza, y definirá la base de una sociedad capaz de escucharse y entenderse.

DESAFÍOS ADICIONALES

A medida que este texto se escribe, nuevos desafíos van surgiendo, asociados a una tecnología que evoluciona cada segundo. Por eso, más allá de establecer pautas o reflexiones detalladas sobre aspectos o aplicativos puntuales, consideramos clave puntualizar algunas de las tendencias más influyentes de los últimos años.

Veracidad de la información y papel de los medios

Ante diversas situaciones de interés público que van desde elecciones, hasta plebiscitos de relevancia nacional o el manejo de una pandemia, hemos visto incontables casos en los cuales las noticias falsas y/o engañosas generan una influencia considerable. Según un estudio del Instituto Reuters, de la Universidad de Oxford, en Reino Unido, la infodemia de noticias falsas es una mezcla de diversos fenómenos: primero, la creación de notas que van desde las recontextualizadas o ligeramente falseadas, hasta las noticias fabricadas completamente. Luego, para la difusión, además de los medios efímeros creados para difundir ese tipo de noticias, los principales agentes de resonancia son las figuras públicas de gran número de seguidores. De ahí, los medios tradicionales retoman las notas y vuelven a difundir. Finalmente, las redes sociales han sido incapaces de generar filtros suficientes para ello y las noticias identificadas como falsas se mantienen en las plataformas aun a pesar de ser denunciadas.[3]

Ante eso, primero es necesario aceptar que hoy día las herramientas y medios para adecuar, truquear o crear notas falsas enfocadas a desinformar, son más accesibles que nunca. De ahí, es importante reconocer la importancia de contar con una cultura de la verificación, ya sea promovida por instituciones dedicadas a ello, como Chequeado, en Argentina, por medios tradicionales que tengan espacios dedicados a ello para contrastar o sencillamente por las personas usuarias que tengan mayor cautela de la información que comparten, y que se fomente una verificación ciudadana.

En ese sentido, es vital que las personas que tengan acceso a audiencias grandes asuman mayor responsabilidad respecto del contenido que se difunde, al igual que los medios tradicionales, quienes deben aumentar el estándar de su verificación de información y evitar a toda costa la difusión de cualquier tipo de noticia no veraz.

Datos y más datos

El caso de Cambridge Analytica exhibió a una entidad con la capacidad de realizar un análisis profundo de los datos de amplios sectores de la población estadounidense y construir, a partir de ello, una serie de estrategias para influir en las decisiones asociadas a una campaña electoral. Es importante aclarar que dichos datos fueron obtenidos de manera engañosa, sin el consentimiento de las personas usuarias. Con este caso se puso de manifiesto una serie de factores por considerar:

Primero, la importancia de una regulación detallada y rigurosa respecto del uso y aprovechamiento de los datos, y en particular la información privada de las personas, así como su propiedad. Además, es fundamental que la ciudadanía cuente con el conocimiento suficiente sobre el valor de su información y la necesidad de cuidarla. Segundo, reconocer que hoy en día se generan más datos por segundo que en ningún otro momento en la historia de la humanidad y que contar con la capacidad para analizar y procesar grandes cantidades de información es algo que se debe hacer de

[3] Types, Sources, and Claims of Covid-19 Misinformation Authors: J. Scott Brennen, Felix M. Simon, Philip N. Howard, y Rasmus Kleis Nielsen. Disponible en https://bit.ly/3MqPIWf19-misinformation

manera responsable y transparente, y que debe existir una trazabilidad respecto de cómo, quién y por qué se utilizan los datos, poniendo al centro la integridad de la ciudadanía, su privacidad y sus derechos.

Inteligencia artificial, IA

Los avances tecnológicos en materia de IA son veloces, contundentes e impactantes en cuanto a las funcionalidades que habilitan: desde bots capaces de conversar, atender y resolver dudas, hasta el desarrollo de modelos probabilísticos para predecir enfermedades, crímenes o tendencias de consumo. Las posibilidades son infinitas y, una vez más, quien cuenta con la capacidad para desarrollar los algoritmos que alimentan la IA, tienen el poder para "educar" a esta inteligencia para que analice, desarrolle y produzca aquello que le es encomendado, pero también para discriminar y filtrar con sesgos.

Ninguna tecnología es absolutamente neutral, ya que adquiere la mirada y posicionamiento de quien la desarrolla. Al respecto, el AI Institute generó un estudio que identifica una profunda crisis de falta de diversidad en el ecosistema de especialistas de IA tanto en materia de género, como de raza, y cómo las consecuencias de ello genera una serie de sistemas discriminatorios (West *et al.*, 2019). Frente a ello, hay una urgencia de fomentar mayor diversidad en los equipos de desarrollo, mayor transparencia de los algoritmos, y una reevaluación y rediseño de los sistemas de IA encargados de clasificar, detectar y predecir situaciones en relación con la raza y el género.

La IA puede ayudar y potenciar, en gran medida, la capacidad de las instituciones para ser más responsivas, generar una mejor y más pertinente atención. Pero sólo será posible si quien lo impulsa es capaz de imprimir una mirada basada en la justicia y la equidad, y si la sociedad implicada tiene la posibilidad de fiscalizar el diseño *motor*.

CONCLUSIONES: INNOVACIÓN EN LA PARTICIPACIÓN CIUDADANA EN MÉXICO

Como hemos elaborado hasta aquí, las características de participación ciudadana en un lugar y un momento determinados son el reflejo de las tensiones entre una sociedad, sus necesidades y la fluidez con las cuales se cumplen los acuerdos de esta sociedad con sus instituciones. Los mecanismos que facilitan la participación ciudadana en México, además de burocráticos y con altos costos de entrada, se encuentran hoy rebasados por mecanismos informales de presión y movilización.

Si bien eso no es suficiente, es importante reconocer que la aparición de dichos mecanismos es también reflejo de una evolución democrática en el sistema político mexicano, fruto de importantes esfuerzos de reforma, transparencia y pluralidad (incluyendo la dimensión de género) durante las últimas tres décadas. En ese sentido, la participación no ocurre en un limbo.

Por un lado, una importante época de *profesionalización* y *especialización* de la sociedad civil, a pesar de los retos sistémicos al *asociativismo*, han permitido que el día de hoy exista gran número de grupos ciudadanos organizados que están incidiendo en temas clave de la agenda pública, así como laborando en la promoción y defensa de los derechos humanos. Entre dichos grupos se encuentran también algunos que han profundizado en torno al derecho mismo de participación reconocido por la Constitución.

Por otro lado, los avances tecnológicos y la velocidad de la comunicación han permitido una importante evolución en el ejercicio de la participación ciudadana. En ocasiones, la sistematización de metodologías de movilización y organización han, incluso, permitido consolidar nuevas tecnologías cívicas, así como cambios reales e importantes en el marco legal y/o el avance de los derechos humanos. Es decir, los vehículos de participación contribuyen a la forma que ocupa la participación.

En ese sentido, es importante anotar al menos tres principales retos a la participación. Primero, la agenda para simplificar el asociativismo en México y promover una filantropía local, transparente y responsable, ha estado virtualmente abandonada durante los últi-

mos años. Fuera de loables esfuerzos de ciudadanos ejemplares que publicaron guías para navegar en el complejo proceso hoy vigente, no existe una visión política seria para promover las diferentes formas de la participación ciudadana.

Esto se empantana incluso más, toda vez que el presidente López Obrador establece una narrativa oficial sobre *las organizaciones fifí*, que demuestra un profundo desconocimiento y/o un desprecio incomprensible de la importante labor y aporte a lo público que hacen una muy diversa y amplia red de organizaciones. En un país donde los periodistas y los defensores de derechos humanos son asesinados impunemente, polemizar con su figura a la ligera es una irresponsabilidad absoluta.

Segundo, los mecanismos formales de participación no pueden ni deben caer en la simulación política que se vislumbra en algunos. Para ello, es necesario afinar las reglas de operación y reducir los costos de participación que algunos mantienen. Además, es necesaria una revisión de fondo a la regulación de los partidos políticos, con el objetivo de promover mayor pluralidad en el equilibrio del poder público.

Tercero, los ciudadanos deben reconocer que las herramientas de organización, comunicación, activismo e incidencia están más disponibles que nunca antes. Sin embargo, todas ellas sólo serán de utilidad únicamente si existe un tejido social capaz de soportar el impulso de las causas que emerjan. Incluso con sistemas sólidos de organización ciudadana equipados con capacidad operativa, la relación entre autoridades y sociedad, puede generar nuevos balances menos enfocados en la dependencia y más asociados a un sistema de contrapesos realmente democrático.

Como vimos en los casos de emergencia debido a desastres naturales o crisis de salud pública, las y los mexicanos son ejemplo de innovación en la participación ciudadana, así como en lo que se refiere a su uso de la Internet para organizar, movilizar e incidir en los asuntos de interés público. Sin embargo, la desconexión que ello tiene de la credibilidad de la que gozan partidos políticos e instituciones del Estado, debe llamar nuestra atención urgente.

Los mecanismos formales de participación son hoy rancios y burocráticos, además de establecer altísimos costos de participación. En muchas ocasiones, por si no fuera suficiente, son instrumentos

de simulación política y clientelismo, que dan como resultado una sociedad aparentemente desinteresada o apática –nada más lejos de la verdad–. Sin embargo, para que el uso de estos mecanismos se expanda, es necesario que quienes participan puedan ver el impacto de sus acciones.

Esta necesidad de transparencia se facilita en la medida en la que la Internet facilita y acelera la comunicación. Esto es, las plataformas digitales son una avenida que funciona en dos sentidos. Por un lado, promueven nuevos métodos y caminos para la participación, que desbordan por fuera de los mecanismos formales mencionados. Por el otro, representan una oportunidad para que los funcionarios públicos complementen, mejoren y amplíen su relación con quienes participan y con la sociedad en su conjunto.

Por ello, es vital que se vuelvan comprometidos aliados de la cultura de la participación ciudadana, y guardianes de su buena salud y dinamismo. Con ello, para decirlo en pocas palabras, todos ganamos. Porque para cambiar la política, necesitamos hacerla, y hacer de la política una herramienta accesible y ajustable.

Una sociedad con la capacidad de organizarse de manera autónoma, de resolver aspectos importantes sobre la toma de decisiones en función del bienestar colectivo o el interés público, será una sociedad libre, capaz de participar políticamente y de modificar, exigir y presionar al sistema de gobierno que le rige. Esta es la base de la democracia plena que México tiene el potencial de alcanzar.

BIBLIOGRAFÍA

Arnstein, S. (1969). A ladder of citizen participation. *Journal of the American Institute of Planners, 35*(4), 216-224.

Barczak, M. (2001). Representation By Consultation? The Rise of Direct Democracy in Latin America. *Latin American Politics and Society, 43*(3), 37-60.

Brager, G. y H. Specht (1973). *Community Organizing*. Nueva York: Columbia University Press.

Brennen, J.S., Simon, F.M., Howard, P.N. y Kleis Nielsen, R. (2020). Types, Sources, and Claims of Covid-19 Misinformation Authors. Recuperado de https://bit.ly/3pFFWWt

Congreso de la Ciudad de México (2019). *Ley de Participación Ciudadana de la Ciudad de México*. Ciudad de México: Instituto Electoral de la Ciudad de México. Recuperado de https://bit.ly/3KbZIAy

Dahl, R. (2000). *La democracia y sus críticos*. Barcelona: Paidós.

García, I. (2019). "OSCS: La incertidumbre". *Reporte Índigo*. Recuperado de https://bit.ly/3CsMVY5/

Guillen, A., Sáenz, K., Badii, M.H. y Castillo, J. (2009). Origen, espacio y niveles de participación ciudadana (Origin, space and levels of participation). *Daena: International Journal of Good Conscience*, *4*(1), 179-193.

Hambleton, S. y Hoggett, P. (1994). A framework for understanding area-based decentralization. *Local Goverment. Policy Marketing*, *20*(4), 5-12.

Hernández, S. (2017). Verificado 19s: Ayuda de la tecnología después del sismo en México. *Ford Foundation*. Recuperado de https://bit.ly/3IZIZ4F

Innerarity, D. (2020). *Una teoría de la democracia compleja. Gobernar en el siglo XXI*. Barcelona: Galaxia Gutenberg.

Lehmbruch, G. (1967). *Proporzdemokratie: Politisches System und politische Kultur in der Schweiz und in Österreich*. Tübingen: Mohr (Siebeck).

Lehmbruch, G. (1992). Konkordanzdemokratie. En M.G. Schmidt (ed.). *Die westlichen Länder. Lexikon der Politik. vol. 3 (206-211).* München: C.H.Beck.

Lehmbruch, G. (1996). Die korporative Verhandlungsdemokratie in Westmitteleuropa. *Schweizerische Zeitschrift für Politische Wissenschaft*, *2*(4), 19-41.

Lehmbruch, G. (2003). *Verhandlungsdemokratie. Beiträge zur vergleichenden Regierungslehre*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Lehmbruch, G. (2012). Die Entwicklung der vergleichenden Politikforschung und die Entdeckung der Konkordanzdemokratie: eine historisch-institutionelle Perspektive. En S. Köppl & U. Kranenpohl (eds.), *Konkordanzdemokratie: Ein Demokratietyp der Vergangenheit?* (33-50). Baden-Baden: Nomos.

Lijphart, A. (1977). *Democracy in plural societies. A comparative exploration*. New Haven, CT: Yale University Press.

Lijphart, A. (1984). *Democracies. Patterns of majoritarian and consensus government in twenty-one countries*. New Haven, CT: Yale University Press.

Lijphart, A. (1999). *Patterns of democracy. Government forms and performance in thirty-six countries*. New Haven, CT: Yale University Press.

Lijphart, A. (2008a). Introduction: Developments in power sharing theory. En A. Lijphart (ed.). *Thinking about democracy. Power sharing and majority rule in theory and practice* (pp. 3-22). Londres: Routledge.

Martínez Colín, M.A., Gallardo González, G.P. y Pizano Martínez, A.C. (2012). Intervención de la Asociación de Vecinos Jardines del Country Segunda Sección, en el Rescate y Manejo del Parque Hundido. Recuperado de https://bit.ly/3tq6sEe

Peixoto, Tiago y Sifry, Micah L. (2017). *Civic Tech in the Global South: Assessing Technology for the Public Good*. Washington, DC: World Bank and Personal Democracy Press. Recuperado de https://bit.ly/3Mm2DbL

Pogrebinschi, Thamy, (2013). El giro pragmático de la democracia en América Latina. *Nueva sociedad*. Recuperado de https://bit.ly/3CixDoG

Poppert, D. (2018). Navigating the field of civic tech. A guide for newcomers and explorers. Recuperado de https://bit.ly/3CmVbc0

Romero, J.J. (2019). El Estado como botín de políticos. *Sin Embargo*. Recuperado de https://bit.ly/3IW7iPq

Rowley, J. (2016). Civic Tech Faces Uphill Battle In Work To Build A Better Government And Society. Recuperado de https://bit.ly/3MmRiZ2

Shand, D. y Arnberg, M. (1996). Backgroung Paper in Responsive Government: Service Quality Initiatives. Paris: OECDE.
Schneider, V. y Eberlein, B. (2015). *Complex Democracy: Varieties, Crises, and Transformations*. Suiza: Springer.
West, S.M., Whittaker, M. y Crawford, K. (2019). Discriminating Systems: Gender, Race and Power in AI. *AI Now Institute*. Recuperado de https://b.gatech.edu/3Ke4EFa

CAPÍTULO 10

TRES ÁREAS DE OPORTUNIDAD QUE OFRECE LA ECONOMÍA DIGITAL PARA CONTRIBUIR AL DESARROLLO EN MÉXICO

JAIME ARTURO DEL RÍO MONGES
JOSÉ LUIS CLAVELLINA MILLER*

* Ambos autores se desempeñan en el Instituto Belisario Domínguez.

La economía es la ciencia que se encarga de la optimización de recursos escasos para diversos fines. La economía digital permite la utilización de las nuevas tecnologías de la información y comunicación (TIC) para administrar de mejor forma dichos recursos escasos.

Las TIC proporcionan instrumentos para el procesamiento, administración y distribución de información por medio de diferentes dispositivos tecnológicos, tales como: computadoras, teléfonos móviles, tabletas, televisiones, videojuegos, entre otros, que utilizan la Internet como plataforma para la producción, distribución y consumo de bienes y servicios que satisfacen necesidades de la sociedad. De acuerdo con Hernández (2018), para que este tipo de economía funcione, se requiere tanto de TIC como de usuarios y una infraestructura de red que permita la conexión entre ellos; además, involucra un gran número de agentes como el gobierno, empresas energéticas y de telecomunicaciones, proveedores de servicios de negocios y comercio, derechos de propiedad, capital humano, entre otros.

Entre los principales atributos que debe tener la economía digital destacan que debe ser: *i)* digitalizada y rastreable (para analizar el comportamiento de los usuarios); *ii)* conectada (para vincular a proveedores, consumidores, trabajadores, por mencionar algunos); *iii)* compartida (se comparte una gran cantidad de información para la creación de campañas exitosas de mercadeo); *iv)* personalizada (para la creación de productos específicos y optimización logística); *v)* directa (permite eludir intermediarios); y *vi)* globalizada (no importa la procedencia del comercio dada la gran cobertura de Internet) (Hernández, 2018).

El acceso a diferentes mercados de forma sencilla a precios competitivos, el crecimiento escalable de las organizaciones con modelos basados en las TIC, que generan menores costos; el trabajo remoto y mayor flexibilidad de horarios son algunas de las ventajas de la llamada economía digital (Hernández, 2018). Adicionalmente, las TIC tienen interacción con varios sectores, posibilitan innovaciones, incrementan la productividad y promueven el desarrollo de destrezas, incluso pueden elevar la participación política de los ciudadanos y hacer que los gobiernos rindan más cuentas. La capacidad que tiene una economía de beneficiarse del uso de las TIC está determinada por el medio ambiente empresarial y de regulación. En general los países avanzados son los que tienen un mejor aprovechamiento de las TIC y de la economía digital (BBVA Research, 2015).

Por otro lado, entre algunas de las desventajas de la economía digital se encuentra que aún existe gran cantidad de personas que no tiene acceso a esas tecnologías, así como la menor necesidad de fuerza de trabajo, lo que eleva el desempleo; también puede generar importantes barreras a la entrada de nuevos competidores y algunas empresas pueden obtener poder de mercado e incluso generar tensiones sociales y, como se verá más adelante, erosión de la base impositiva.

La economía digital representa, además, un reto para las empresas, pues deben innovar y cambiar sus procesos de producción, ventas, publicidad, entrega, marketing, entre otros. Para que la mayor parte de la población participe de los beneficios que representa la economía digital, la Organización para la Cooperación y el Desarrollo Económicos (por sus siglas en inglés, OECD, 2019) señala que se requiere de políticas que reduzcan las barreras al comercio y a la inversión; que promuevan la competencia, simplifiquen trámites e impulsen la conectividad en áreas remotas y rurales. También se necesita que cada vez mayor número de empresas de todos tamaños realicen análisis de datos, lo cual requiere del desarrollo de habilidades. Las distintas economías también necesitarán de mayor inversión en innovación digital (software y patentes, por ejemplo), promover emprendimientos, facilitar el financiamiento, apoyar la investigación básica, la difusión del conocimiento, la ciencia y los datos abiertos por parte del gobierno.

De acuerdo con datos de la OECD (2019), alrededor de 14% de los empleos en los países de la organización enfrenta la posibilidad de automatización y otro 32% lo hará en los próximos 10-20 años. Sin embargo, también señala que en la última década cuatro de cada 10 empleos se crearon en sectores digitales y que han emergido nuevas formas de trabajo. Para asegurar que existan oportunidades de empleo para todos se requerirá de un entrenamiento masivo de la población. Al mismo tiempo, deben atenderse problemas como la protección social en un entorno de mayor movilidad y flexibilidad laborales. Otros problemas por atenderse en la nueva era digital se relacionan con la inclusión social y con la seguridad, privacidad y protección de datos e información.

En el presente capítulo se analizan tres de las áreas de oportunidad que ofrece la economía digital para contribuir al desarrollo en México. En primer lugar, se muestra el potencial de la economía digital para facilitar el acceso a los servicios financieros por parte de población que habita en zonas con baja penetración financiera, incluyendo áreas rurales con distintos niveles de marginación. Un mayor acceso a servicios financieros digitales (i.e. ahorro, crédito) podría facilitar el impulso de actividades productivas que aumenten las oportunidades de desarrollo en regiones marginadas. Los servicios financieros asociados a la economía digital tienen el potencial de contribuir a la creación de proyectos productivos y, con el tiempo, de polos de desarrollo regional, lo cual podría ayudar a la reducción de la pobreza.

En segundo lugar, se analiza el potencial de la economía digital para contribuir al fortalecimiento de los ingresos públicos. La adecuación de la legislación fiscal para facilitar el pago de impuestos por parte de empresas digitales y otros servicios que forman parte de la economía digital, puede ayudar a elevar la competencia en ciertos sectores y contribuir al aumento de la base gravable y al fortalecimiento de las finanzas públicas.

En tercer lugar, se analiza la creciente penetración de mercado de los servicios asociados a la economía digital, así como las oportunidades de negocio que esto representa. Las compras por Internet son uno de los servicios que ofrece la economía digital. Si bien las compras en línea ya presentaban una tendencia creciente, la actual pandemia de Covid-19 y las perspectivas que se vislumbran para cuando esta sea superada, han acelerado el crecimiento de la demanda de estos servicios. Los datos de la Encuesta Mensual de Empresas Comerciales (EMEC), actualizados al mes de marzo de 2020, muestran que las ramas de actividad económica que han reportado significativos incrementos en ingresos ante el impacto de la actual pandemia han sido las de: *i)* comercio al por menor exclusivamente por Internet y catálogos impresos, televisión y similares; *ii)* tiendas de autoservicio; y *iii)* artículos de cuidados para la salud. Cabe destacar que el impacto de la pandemia en las ventas por Internet puede estar implícito también en los ingresos de las ramas de tiendas de autoservicio, y artículos de cuidados para la salud, pues es factible que una parte significativa de sus ventas (y de las farmacias) se esté llevando a cabo por Internet en el actual contexto de la pandemia, y es probable que esta tendencia se mantenga en el futuro.

LOS SERVICIOS FINANCIEROS DIGITALES COMO ALTERNATIVA PARA AUMENTAR LA INCLUSIÓN FINANCIERA Y REDUCIR LA POBREZA Y LA VULNERABILIDAD ECONÓMICA

El acceso a servicios financieros como el ahorro, el crédito, los seguros, entre otros, permite a las personas incrementar sus posibilidades para emprender negocios y reducir y diversificar riesgos. Por lo que la adecuada utilización de dichos servicios puede contribuir a la reducción de la pobreza y la vulnerabilidad económica. En el presente apartado se analiza cómo los servicios financieros digitales pueden contribuir a incrementar la inclusión financiera en México y ser parte de los elementos de una estrategia integral de reducción de la pobreza.

Servicios financieros digitales e inclusión financiera

En septiembre de 2019, Arturo Herrera, secretario de Hacienda y Crédito Público, en su comparecencia ante el Senado, explicó que una de las barreras que deben superarse para facilitar un cambio estructural positivo en la tendencia de crecimiento de mediano y largo plazos en México es la reducida profundidad del sistema financiero (Canal del Congreso, 2019). Tan sólo 27% de los mexicanos en la parte baja de la distribución del ingreso tiene una cuenta bancaria, y en general la baja penetración financiera que prevalece en el país implica que no se está recurriendo al sistema financiero para ahorrar o financiar inversiones y, por tanto, México opera en gran medida a partir del efectivo (Canal del Congreso, 2019).

La inclusión financiera se refiere en este caso a la proporción de la población que usa servicios financieros formales, de acuerdo con Demirguc-Kunt y Klapper (2013). Los resultados de la Encuesta Nacional de Inclusión Financiera (ENIF) 2018 señalan que cerca de la mitad de la población del país recurre al ahorro informal. Asimismo,

la población que ahorra en México en una mayor proporción tiene activos, cuenta con un ingreso fijo y un empleo formal, en comparación con la que no ahorra; en ese sentido, la capacidad de ahorrar puede asociarse con la vulnerabilidad económica. En la ENIF 2018 se encuentra que las personas que no tienen capacidad de ahorrar en el país son también las que cuentan con mayores dificultades para que su ingreso mensual les sea suficiente para cubrir sus gastos. Destaca que entre quienes cuentan con un empleo formal, las mujeres, en general, ahorran más que los hombres.

El tamaño de la localidad también influye en dicha capacidad de las personas en México. Las localidades con una reducida población, en general se asocian con niveles altos o muy altos de marginación, lo cual dificulta la generación de economías de escala y reduce la probabilidad de que los intermediarios financieros bancarios y no bancarios establezcan sucursales en dichas localidades. Los resultados de la ENIF 2018 permiten observar que la capacidad de ahorrar para las personas en las localidades menores a 15 000 habitantes es menor respecto a localidades con una población mayor.

La mayor capacidad de ahorrar en localidades con mayor tamaño de población se mantiene tanto en productos de ahorro formales, como informales. Las personas que ahorran en localidades de menor población cuentan con menos activos y empleos formales respecto de las personas que ahorran en localidades más grandes. Sin embargo, independientemente del tamaño de la población, en general se mantiene que las mujeres que cuentan con un trabajo formal ahorran más que los hombres.

Por otro lado, de acuerdo con la ENIF 2018, se puede observar que en el nivel nacional los hombres tienen en mayor proporción al menos un producto financiero formal respecto de las mujeres. Sin embargo, las ellas tienen en mayor proporción un sólo producto financiero formal respecto de los hombres, y este resultado se mantiene independientemente del tamaño de la población de la localidad. En el ámbito nacional los hombres suelen contar con más de un producto financiero formal, este resultado se mantiene independientemente del tamaño de la población de las localidades, con excepción del caso cuando se tienen dos o tres productos financieros formales en localidades de 15 000 o más habitantes.

CUADRO 01. ALGUNOS INDICADORES ASOCIADOS AL AHORRO EN MÉXICO

	NIVEL NACIONAL					
	TOTAL		MUJERES		HOMBRES	
Indicadores	**Tiene cuenta de ahorro**	**No tiene cuenta de ahorro**	**Tiene cuenta de ahorro**	**No tiene cuenta de ahorro**	**Tiene cuenta de ahorro**	**No tiene cuenta de ahorro**
Saber que existen cuentas básicas	56.1%	43.9%	52.2%	47.8%	60.3%	39.7%
Tiene ahorro informal	49.6%	50.6%	49.6%	50.4%	51.2%	48.8%
Tiene productos financieros formales	62.8%	37.2%	62.8%	37.2%	63.1%	36.9%
En el último año, el ingreso mensual que recibió no fue suficiente para cubrir sus gastos	43.2%	56.8%	43.6%	56.4%	42.6%	57.4%
Tiene propiedad de activos	56.5%	43.5%	59.8%	40.2%	54.2%	45.8%
Peribe ingresos variables	42.3%	57.7%	48.7%	51.3%	38.7%	61.3%
Tiene trabajo formal	52.4%	47.6%	58.6%	41.4%	48.8%	51.2%

FUENTE:
elaboración propia con base en datos de la ENIF 2018.

Las mujeres en México tienen en mayor proporción que los hombres cuenta o tarjeta de ahorro, independientemente del tamaño de población de la localidad en la que viven. Sin embargo, los hombres tienen más créditos, seguros y cuenta de ahorro para el retiro.

CUADRO 02.

ALGUNOS INDICADORES ASOCIADOS AL AHORRO EN LOCALIDADES CON POBLACIONES MENORES A 15 000 HABITANTES EN MÉXICO

	LOCALIDADES CON MENOS DE 15 000 HABITANTES					
	TOTAL		MUJERES		HOMBRES	
Indicadores	**Tiene cuenta de ahorro**	**No tiene cuenta de ahorro**	**Tiene cuenta de ahorro**	**No tiene cuenta de ahorro**	**Tiene cuenta de ahorro**	**No tiene cuenta de ahorro**
Saber que existen cuentas básicas	46.6%	53.4%	45.5%	54.5%	47.9%	52.1%
Tiene ahorro informal	42.3%	57.7%	45.1%	54.9%	39.2%	60.8%
Tiene productos financieros formales	57.1%	42.9%	57.1%	42.9%	57.2%	42.8%
En el último año, el ingreso mensual que recibió no fue suficiente para cubrir sus gastos	37.4%	62.6%	40.8%	59.2%	33.3%	66.7%
Tiene propiedad de activos	44.0%	56.0%	55.1%	44.9%	38.1%	61.9%
Percibe ingresos variables	35.3%	64.7%	45.2%	54.8%	30.3%	69.7%
Tiene trabajo formal	39.0%	61.0%	45.4%	54.6%	36.2%	63.8%

Cuando las personas en México cuentan con un máximo de escolaridad de nivel secundaria, es más probable que no conozcan las cuentas básicas de ahorro. Mientras que, con niveles de escolaridad superiores a dicho grado, es más probable que conozcan

FUENTE:
elaboración propia con base en datos de la ENIF 2018.

CUADRO 03.

ALGUNOS INDICADORES ASOCIADOS AL AHORRO EN LOCALIDADES CON POBLACIONES DE 15 000 O MÁS HABITANTES EN MÉXICO

	LOCALIDADES CON 15 000 O MÁS HABITANTES					
	TOTAL		MUJERES		HOMBRES	
Indicadores	**Tiene cuenta de ahorro**	**No tiene cuenta de ahorro**	**Tiene cuenta de ahorro**	**No tiene cuenta de ahorro**	**Tiene cuenta de ahorro**	**No tiene cuenta de ahorro**
Saber que existen cuentas básicas	60.1%	39.9%	55.1%	44.9%	65.1%	34.9%
Tiene ahorro informal	54.8%	45.2%	52.2%	47.8%	57.6%	42.4%
Tiene productos financieros formales	64.9%	35.1%	64.8%	35.2%	65.1%	34.9%
En el último año, el ingreso mensual que recibió no fue suficiente para cubrir sus gastos	46.8%	53.2%	45.3%	54.7%	48.7%	51.3%
Tiene propiedad de activos	63.4%	36.6%	61.9%	38.1%	64.5%	35.5%
Percibe ingresos variables	47.4%	52.6%	50.9%	49.1%	45.2%	54.8%
Tiene trabajo formal	59.0%	41.0%	63.5%	36.5%	55.9%	44.1%

FUENTE:
elaboración propia con base en datos de la ENIF 2018.

las cuentas básicas de ahorro. Este resultado se mantiene como predominante, independientemente del género de las personas y del tamaño de la población de las localidades.

NÚMERO DE PRODUCTOS FINANCIEROS FORMALES QUE TIENEN LAS PERSONAS EN MÉXICO

CUADRO 04.

FUENTE: elaboración propia con base en datos de la ENIF 2018.

	NIVEL NACIONAL			LOCALIDADES CON MENOS DE 15 000 HABITANTES			LOCALIDADES CON 15 000 O MÁS HABITANTES		
Número de productos financieros	**Total**	**Mujeres**	**Hombres**	**Total**	**Mujeres**	**Hombres**	**Total**	**Mujeres**	**Hombres**
Sí tiene al menos 1 producto financiero formal	68.3%	65.2%	71.8%	57.1%	58.0%	56.1%	74.4%	69.0%	80.3%
1 producto	34.4%	37.9%	30.9%	46.1%	52.4%	38.9%	29.6%	31.5%	27.9%
2 a 3 productos	39.2%	38.9%	39.6%	37.8%	35.0%	41.0%	39.8%	40.6%	39.0%
4 a 5 productos	15.2%	14.0%	16.4%	10.7%	8.7%	12.9%	17.1%	16.4%	17.7%
6 o más productos	11.1%	9.1%	13.2%	5.4%	3.9%	7.2%	13.5%	11.5%	15.4%
No tiene productos financieros formales	31.7%	34.8%	28.2%	42.9%	42.0%	43.9%	25.6%	31.0%	19.7%

TIPO DE PRODUCTOS FINANCIEROS FORMALES QUE TIENEN LAS PERSONAS EN MÉXICO

CUADRO 05.

FUENTE: elaboración propia con base en datos de la ENIF 2018.

	NIVEL NACIONAL			LOCALIDADES CON MENOS DE 15 000 HABITANTES			LOCALIDADES CON 15 000 O MÁS HABITANTES		
Tipo de productos financieros	**Total**	**Mujeres**	**Hombres**	**Total**	**Mujeres**	**Hombres**	**Total**	**Mujeres**	**Hombres**
Cuenta o tarjeta de ahorro	68.9%	70.4%	67.5%	68.4%	71.7%	64.6%	69.2%	69.8%	68.6%
Crédito	45.6%	44.8%	46.4%	38.4%	37.0%	40.1%	48.5%	48.3%	48.8%
Seguro	37.2%	35.5%	38.9%	31.7%	31.5%	32.0%	39.4%	37.2%	41.5%
Cuenta de ahorro para el retiro	57.9%	47.6%	68.2%	43.4%	27.5%	61.6%	63.8%	56.7%	70.6%

CUADRO 06. NIVEL DE ESCOLARIDAD Y CONOCIMIENTO DE CUENTAS BÁSICAS DE AHORRO EN EL NIVEL NACIONAL

	NIVEL NACIONAL					
	TOTAL		MUJERES		HOMBRES	
Nivel de escolaridad	**Sí tiene** **	**No tiene** ***	**Sí tiene** **	**No tiene** ***	**Sí tiene** **	**No tiene** ***
Sin primaria	2.1%	5.5%	2.6%	6.0%	1.6%	5.0%
Primaria	15.8%	27.6%	16.1%	27.7%	15.6%	27.4%
Secundaria	24.2%	29.8%	24.9%	28.5%	23.4%	31.2%
Preparatoria o bachillerato	20.8%	18.4%	21.3%	18.2%	20.2%	18.6%
Profesional (licenciatura o ingeniería)	34.0%	17.8%	32.2%	18.6%	35.9%	16.9%
Maestría o Doctorado	3.1%	0.8%	2.9%	0.9%	3.3%	0.7%
TOTAL	100%	100%	100%	100%	100%	100%

** Sí tiene conocimiento de la existencia de cuentas básicas
*** No tiene conocimiento de la existencia de cuentas básicas

FUENTE:
elaboración propia con base en datos de la ENIF 2018.

Una de las innovaciones más disruptivas[1] en el sector financiero han sido las instituciones de tecnología financiera, llamadas Fintech, que promueven la colaboración, la vigilancia distribuida y la transparencia. Las Fintech han creado distintos modelos de negocio, como plataformas de plago electrónico, modelos de financiamiento colectivo y préstamos, criptomonedas y el uso de inteligencia artificial (Canal del Congreso, 2019). Las Fintech son importantes para la inclusión digital, porque permiten que servicios financieros lleguen con mayor facilidad a cualquier lugar que cuente con una conexión a Internet, de ahí la importancia de continuar con los esfuerzos de

CUADRO 07. NIVEL DE ESCOLARIDAD Y CONOCIMIENTO DE CUENTAS BÁSICAS DE AHORRO EN LOCALIDADES MENORES A 15 000 HABITANTES

	LOCALIDADES DE MENOS DE 15,000 HABITANTES					
	TOTAL		MUJERES		HOMBRES	
Nivel de escolaridad	**Sí tiene** **	**No tiene** ***	**Sí tiene** **	**No tiene** ***	**Sí tiene** **	**No tiene** ***
Sin primaria	4.2%	9.5%	4.9%	9.6%	3.4%	9.4%
Primaria	27.3%	38.9%	24.9%	37.7%	30.2%	40.1%
Secundaria	30.3%	30.0%	33.1%	31.1%	27.0%	28.8%
Preparatoria o bachillerato	17.1%	13.3%	18.0%	12.9%	16.1%	13.6%
Profesional (licenciatura o ingeniería)	19.1%	8.0%	16.7%	8.2%	21.9%	7.8%
Maestría o Doctorado	1.9%	0.4%	2.3%	0.5%	1.4%	0.3%
TOTAL	100%	100%	100%	100%	100%	100%

FUENTE:
elaboración propia con base en datos de la ENIF 2018.

** Sí tiene conocimiento de la existencia de cuentas básicas
*** No tiene conocimiento de la existencia de cuentas básicas

1 La senadora Alejandra Lagunes explicó que la innovación disruptiva se refiere a las tecnologías accesibles con modelos de negocios innovadores y que crean una cadena de valor en la que todos los participantes puedan estar mejor. Asimismo, explicó que México ocupa el séptimo lugar en el ámbito mundial en adopción de Fintech, con un porcentaje de usuarios de este tipo de empresas como proporción de la población digitalmente activa de 36%, contra 69% de China, que ocupa el primer lugar, lo cual ubica a México por encima de países como Alemania, Estados Unidos y Corea del Sur. También explicó que en México prevalecían 238 empresas Fintech y 540 000 usuarios activos, lo que implicó un crecimiento de 50% sólo entre 2016 y 2017; señaló que, de acuerdo con el estudio de la OCDE de 2018, "Plataformas Digitales y Competencia", México es uno de los líderes en Latinoamérica en el sector, sólo detrás de Brasil.

CUADRO 08.

NIVEL DE ESCOLARIDAD Y CONOCIMIENTO DE CUENTAS BÁSICAS DE AHORRO EN LOCALIDADES DE 15 000 O MÁS HABITANTES

	LOCALICADES DE 15 000 O MÁS HABITANTES					
	TOTAL		MUJERES		HOMBRES	
Nivel de escolaridad	**Sí tiene** **	**No tiene** ***	**Sí tiene** **	**No tiene** ***	**Sí tiene** **	**No tiene** ***
Sin primaria	1.3%	3.0%	1.6%	3.8%	0.9%	2.0%
Primaria	11.1%	20.1%	12.1%	21.6%	10.0%	18.4%
Secundaria	21.6%	29.7%	21.2%	27.0%	22.1%	33.0%
Preparatoria o bachillerato	22.3%	21.8%	22.8%	21.5%	21.7%	22.2%
Profesional (licenciatura o ingeniería)	40.2%	24.2%	39.1%	25.0%	41.2%	23.3%
Maestría o Doctorado	3.6%	1.1%	3.1%	1.1%	4.1%	1.1%
TOTAL	100%	100%	100%	100%	100%	100%

** Sí tiene conocimiento de la existencia de cuentas básicas
*** No tiene conocimiento de la existencia de cuentas básicas

FUENTE:
elaboración propia con base en datos de la ENIF 2018.

conectividad, ya que inclusión digital e inclusión financiera van de la mano (Canal del Congreso, 2019).

El secretario de Hacienda explicó que las regiones más pobres del país son, además, las más aisladas y que lo que permiten las Fintech es cerrar esa brecha, porque no se requiere de un banco para hacer transacciones financieras. Explicó también que el recién lanzado código digital (CoDi), herramienta impulsada principalmente por el Banco de México, que dará la posibilidad de hacer pagos digitales de teléfono a teléfono o de teléfono a un QR en cualquier miscelánea, tortillería, entre otros, sin requerir que una institución

financiera tenga una presencia física en esa localidad. Este tipo de herramientas permitiría cambiar de una economía que, sobre todo en lugares remotos opera fundamentalmente en efectivo, a una economía que funcione por medios digitales.[2]

Los servicios financieros digitales tienen el potencial de aumentar el uso de productos formales entre la población de México, sobre todo aquella que habita en zonas aisladas del medio rural que dificultan la instalación de sucursales de intermediarios financieros bancarios y no bancarios. Estos servicios pueden contribuir a incrementar la inclusión financiera, y con ello aumentar las posibilidades de emprender negocios y reducir riesgos entre la población que tradicionalmente no ha tenido acceso a servicios financieros o estos han sido limitado.

Servicios financieros digitales y reducción de la pobreza

La inclusión financiera puede contribuir a la reducción de la pobreza y a la equidad de género, ya que permitiría a las personas incrementar distintos tipos de capital (i.e. financiero, físico, natural, humano) (Manji, 2010; Levenson, 2016). Sin embargo, el aprovechamiento de dicha inclusión depende del nivel de educación de la población (Arora, 2012). En ese sentido, esa inclusión puede ser uno de los elementos de una estrategia integral de reducción sostenible de la pobreza que considere el fortalecimiento de la educación, entre otras líneas de acción, orientadas a incidir en distintas dimensiones y dinámicas de la pobreza.

Con la finalidad de estimar la posible correlación entre los servicios financieros digitales, el nivel de educación y la pobreza de ingresos, se desarrollaron distintos modelos estadísticos del tipo panel-data,[3] a partir de datos del Banco Mundial. La información disponible permitió construir una base de datos de 64 países, con tres observaciones

[2] El secretario de Hacienda señaló que los beneficiarios inmediatos de este tipo de innovaciones serían los clientes del Banco del Bienestar, principalmente los habitantes del sector rural. Asimismo, estas tecnologías permitirán reducir los elevados costos e incluso riesgos de llevar a cabo la dispersión de recursos en la operación del Banco.

[3] Los modelos panel-data combinan observaciones de sección cruzada (i.e. distintos países) y de series de tiempo.

de tiempo correspondientes a los promedios de los periodos 2010-2012, 2013-2015, y 2016-2018. La posesión de una cuenta en instituciones financieras o con un proveedor de servicios de dinero mediante teléfono celular fue utilizada como una variable *proxy* de los servicios financieros digitales. Se diferenciaron dos grupos: *i)* máximo de estudios en educación primaria; *ii)* mínimo de estudios en educación secundaria. Se consideraron tres grados de pobreza absoluta: *i)* ingreso diario igual o menor a 5.50 dólares PPP constantes (año base 2011), denominado nivel I de pobreza; *ii)* ingreso diario igual o menor a 3.20 dólares PPP constantes (año base 2011), definido como nivel II de pobreza; *iii)* ingreso diario igual o menor a 1.90 dólares PPP[4] constantes (año base 2011), cataogado nivel III de pobreza. Una de las variables implica el uso de pobreza relativa al considerar a 40% de la población con menores ingresos, lo cual en algunos casos puede coincidir con que ese porcentaje de población también padezca pobreza en términos absolutos.[5]

En el primer grupo se estimó la correlación entre "40% de la población con menores ingresos que tiene una cuenta en instituciones financieras o con un proveedor de servicios de dinero vía teléfono celular" (variable independiente), y "el porcentaje de la población que padece un nivel de pobreza absoluta en términos de ingreso" (variable dependiente). A partir de los resultados obtenidos, se estimó que la variable *proxy* de servicios financieros digitales tiene una correlación negativa estadísticamente significativa con el nivel de la pobreza absoluta. En ese sentido, mientras una mayor proporción de la población con menores ingresos tenga acceso a esa variable *proxy* de servicios financieros digitales, menor será el porcentaje que padece un grado de pobreza absoluta en términos de ingreso. Así, se observa que cuando la variable *proxy* de servicios financieros digitales aumenta 1%, el porcentaje de población en nivel de pobreza absoluto I disminuye en 0.50 puntos porcentuales; el porcentaje de población en grado de pobreza absoluto II disminuye en 0.21 puntos porcentuales y el porcentaje de población en nivel de pobreza absoluto III disminuye 0.07 puntos porcentuales.

En el segundo grupo se estimó la correlación entre "el porcentaje de la población con una edad igual o mayor a 15 años que tiene un máximo de escolaridad en el nivel primaria y que tiene una cuenta en instituciones financieras o con un proveedor de servicios de dinero vía teléfono celular" (variable independiente), y "el porcentaje de la población que padece un grado de pobreza absoluta en términos de ingreso" (variable dependiente). Se encontró que la variable *proxy* de servicios financieros digitales asociada a un máximo de escolaridad de nivel primaria tiene una correlación negativa estadísticamente significativa con el grado de la pobreza absoluta. En ese sentido, mientras una mayor proporción de la población económicamente activa (con un máximo de escolaridad de nivel primaria) tenga acceso a esa variable *proxy* de servicios financieros digitales, menor será el porcentaje de la población que padece un grado de pobreza absoluta en términos de ingreso. Así, cuando la variable independiente aumenta 1% (variable *proxy* de servicios financieros digitales), el porcentaje de población en nivel de pobreza absoluto I disminuye en 0.42 puntos porcentuales; el porcentaje de población en grado de pobreza absoluto II disminuye en 0.17 puntos porcentuales y el porcentaje de población en nivel de pobreza absoluto III disminuye 0.05 puntos porcentuales.

En un tercer grupo se estimó la correlación entre "el porcentaje de la población con una edad igual o mayor a 15 años que tiene un mínimo de escolaridad en el nivel secundaria y con una cuenta en instituciones financieras o con un proveedor de servicios de dinero vía teléfono celular" (variable independiente), y "el porcentaje de la población que padece un grado de pobreza

4 Las siglas PPP corresponden a poder de paridad de compra, la cual es una forma de expresar el dinero en términos reales, con la finalidad de facilitar la comparación entre países.

5 Los países que conforman la base de datos empleada en los modelos tipo panel-data son: Argentina, Armenia, Austria, Bielorrusia, Bélgica, Brasil, Bolivia, Bulgaria, Chile, China, Colombia, Costa Rica, Croacia, Chipre, República Checa, Dinamarca, República Dominicana, Ecuador, Egipto, El Salvador, Estonia, Finlandia, Francia, Georgia, Alemania, Grecia, Honduras, Hungría, Indonesia, Irlanda, Israel, Italia, Kazajistán, Kosovo, Kirguistán, Letonia, Lituania, Luxemburgo, Malta, México, Moldavia, Mongolia, Países Bajos, Macedonia del Norte, Panamá, Perú, Polonia, Portugal, Rumania, Rusia, Ruanda, Serbia, Eslovaquia, Eslovenia, España, Suecia, Tailandia, Turquía, Ucrania, Reino Unido, Estados Unidos, Uruguay y Vietnam.

absoluta en términos de ingreso" (variable dependiente). A partir de los resultados obtenidos, se estimó que la variable *proxy* de servicios financieros digitales asociada a un mínimo de escolaridad de nivel secundaria tiene una correlación negativa estadísticamente significativa con el grado de la pobreza absoluta. En ese sentido, mientras una mayor proporción de la población económicamente activa con un mínimo de escolaridad de nivel secundaria tenga acceso a esa variable *proxy* de servicios financieros digitales, menor será el porcentaje de la población que padece un grado de pobreza absoluta en términos de ingreso. Así, se obtuvo que cuando la variable independiente aumenta 1%, el porcentaje de población en nivel de pobreza absoluto I disminuye en 0.59 puntos porcentuales; el porcentaje de población en grado de pobreza absoluto II disminuye en 0.23 puntos porcentuales y el porcentaje de población en nivel de pobreza absoluto III disminuye 0.07 puntos porcentuales.

Los resultados del segundo y tercer grupo permiten inferir que un mayor nivel de escolaridad en las personas que tienen acceso a la variable *proxy* de servicios financieros digitales podría tener un mayor impacto en la reducción de la pobreza absoluta. Sin embargo, el impacto de la educación tenderá a ser menor mientras más profunda sea la pobreza absoluta de la población. Ahora bien, ya se estimó el posible impacto de una variable *proxy* de los servicios financieros digitales sobre el porcentaje de población en condiciones de pobreza absoluta, y también del posible impacto de esa misma variable asociada al nivel de educación sobre el porcentaje de población en condiciones de pobreza absoluta. Sin embargo, vale el esfuerzo efectuar el análisis a la inversa, es decir, al considerar el porcentaje de población en condiciones de pobreza absoluta como variable independiente de las demás. En ese sentido, se buscaría evaluar si el porcentaje de población en condiciones de pobreza absoluta puede ser en sí mismo un obstáculo para que las personas puedan acceder a los servicios financieros digitales; los siguientes modelos se enfocan en ese análisis.

En un cuarto grupo se estimó la correlación entre "el porcentaje de la población que padece un nivel de pobreza absoluta en términos de ingreso" (variable independiente), y "la proporción de

40% de la población con menores ingresos que tiene una cuenta en instituciones financieras o con un proveedor de servicios de dinero vía teléfono celular" (variable dependiente). A partir de los resultados obtenidos, se estima que el grado de la pobreza absoluta tiene una correlación negativa estadísticamente significativa con la variable *proxy* de servicios financieros digitales. En ese sentido, mientras mayor sea el porcentaje de la población que padece un nivel de pobreza absoluta en términos de ingreso, menor será la proporción de la población con menores ingresos que tenga acceso a esa variable de servicios financieros digitales. Así, se obtuvo que cuando el porcentaje de población en grado de pobreza absoluto I aumenta 1%, la variable *proxy* de servicios financieros digitales disminuye en 1.06 puntos porcentuales. Cuando el porcentaje de población en nivel de pobreza absoluto II aumenta 1%, la variable *proxy* de servicios financieros digitales disminuye en 1.26 puntos porcentuales. Y cuando el porcentaje de población en grado de pobreza absoluto III aumenta 1%, la variable *proxy* de servicios financieros digitales disminuye en 1.19 puntos porcentuales.

En el quinto grupo se estimó la correlación entre "el porcentaje de la población que padece un nivel de pobreza absoluta en términos de ingreso" (variable independiente), y "el porcentaje de la población con una edad igual o mayor a 15 años que tiene un máximo de escolaridad de nivel primaria y que tiene posesión de una cuenta en instituciones financieras o con un proveedor de servicios de dinero vía teléfono celular" (variable dependiente). A partir de los resultados obtenidos, se encuentra que el nivel de la pobreza absoluta tiene una correlación negativa estadísticamente significativa con la variable *proxy* de servicios financieros digitales asociada con un máximo de escolaridad de nivel primaria. En ese sentido, mientras mayor sea el porcentaje de la población que padece pobreza absoluta en términos de ingreso, menor será el porcentaje de la población económicamente activa (con un máximo de escolaridad de nivel primaria) que tenga una cuenta en instituciones financieras o con un proveedor de servicios de dinero vía teléfono celular. Así, cuando el porcentaje de población en grado de pobreza absoluto I aumenta 1%, la variable dependiente disminuye en 0.89 puntos porcentuales.

Cuando el porcentaje de población en nivel de pobreza absoluto II aumenta 1%, la variable dependiente disminuye 1.01 puntos porcentuales; y cuando el porcentaje de población en grado de pobreza absoluto III aumenta 1%, la variable dependiente disminuye en 0.84 puntos porcentuales.

En el sexto grupo se estimó la correlación entre "el porcentaje de la población que padece un nivel de pobreza absoluta en términos de ingreso" (variable independiente), y "el porcentaje de la población con una edad igual o mayor a 15 años que tiene un mínimo de escolaridad de nivel secundaria y que tiene una cuenta en instituciones financieras o con un proveedor de servicios de dinero vía teléfono celular" (variable dependiente). A partir de los resultados obtenidos, se encuentra que el grado de la pobreza absoluta tiene una correlación negativa estadísticamente significativa con la variable *proxy* de servicios financieros digitales asociada a un mínimo de escolaridad de nivel secundaria.[6] Así, se obtiene que cuando el porcentaje de población en grado de pobreza absoluto I aumenta 1%, la dependiente disminuye en 0.83 puntos porcentuales. Cuando el porcentaje de población en nivel de pobreza absoluto II aumenta 1%, la variable dependiente disminuye en 0.93 puntos porcentuales; y cuando el porcentaje de población en grado de pobreza absoluto III aumenta 1%, la variable dependiente disminuye en 0.73 puntos porcentuales.

Los resultados obtenidos permiten inferir que el porcentaje de población en condiciones de pobreza absoluta podría ser en sí mismo un obstáculo para que las personas, independientemente de su nivel de escolaridad, puedan acceder a servicios financieros digitales. En ese sentido, si bien los servicios financieros digitales podrían contribuir a la reducción de la pobreza absoluta, también la reducción de dicha pobreza absoluta podría contribuir a facilitar el acceso a los servicios financieros digitales, sobre todo entre la población con menores ingresos (los resultados indican también que podría existir una doble causalidad entre dichas variables).

6 En ese sentido, mientras mayor sea el porcentaje de la población que padece un nivel de pobreza absoluta en términos de ingreso, menor será el porcentaje de la población económicamente activa con un mínimo de escolaridad de nivel secundaria que tenga posesión de una cuenta en instituciones financieras o con un proveedor de servicios de dinero vía teléfono celular.

La base de datos empleada para desarrollar los modelos tipo panel-data anteriores permiten ubicar a México en el ranking de las variables analizadas en el subconjunto de países que pertenecen a la OCDE. En el grupo de 27 países que la conforman, México se ubicó en la última posición en el ranking de la variable "porcentaje de 40% de la población con menores ingresos que tiene 15 años o más y tiene cuenta en una institución financiera o con un proveedor de servicios de dinero vía teléfono celular". Similarmente, México se ubicó en la última posición en el ranking de la variable "porcentaje de la población que tiene 15 años y más con estudios máximos a nivel primaria y que tiene cuenta en una institución financiera o con un proveedor de servicios de dinero vía teléfono celular" y de igual forma, en la última posición en el ranking de la variable "porcentaje de la población que tiene 15 años o más con estudios mínimos a nivel secundaria y que tiene cuenta en una institución financiera o con un proveedor de servicios de dinero vía teléfono celular".

Mientras tanto, también en el grupo de la OCDE, pero ordenando los países de menor a mayor porcentaje de población en condiciones de pobreza absoluta, se observa lo siguiente. México se ubicó como el país con el mayor porcentaje promedio de pobreza absoluta durante el periodo 2010-2018 al considerar las tres líneas de pobreza analizadas: *i)* 1.90 dólares PPP constantes (año base 2011); *ii)* 3.20 dólares PPP constantes (año base 2011); y *iii)* 5.50 dólares PPP constantes (año base 2011).

El diseño de una estrategia integral de reducción de la pobreza requiere considerar las distintas dimensiones y las dinámicas de dicha situación. La medición multidimensional de la pobreza en México que lleva a cabo el Consejo Nacional de Evaluación de la Política de Desarrollo Social (Coneval) podría contribuir a un diseño y monitoreo adecuado de una estrategia integral de reducción de la pobreza, dentro de la cual los servicios financieros digitales podrían ser uno de sus elementos.

Con los resultados que se tienen hasta ahora, podría generarse una sinergia positiva en ambas direcciones, entre la reducción de la pobreza y el mayor aprovechamiento de una herramienta como los servicios financieros digitales. Esto es, los servicios financieros digitales podrían contribuir a la reducción de la pobreza.

CUADRO 09.

PROPORCIÓN DE 40% DE LA POBLACIÓN CON MENORES INGRESOS, DE 15 AÑOS O MÁS QUE TIENE CUENTA EN UNA INSTITUCIÓN FINANCIERA O CON UN PROVEEDOR DE SERVICIOS DE DINERO VÍA TELÉFONO CELULAR

Ranking	País	Promedio 2010-2012	Promedio 2013-2015	Promedio 2016-2018	Promedio 2010-2018
1	Dinamarca	99.8	100.0	100.0	**122.8**
2	Finlandia	99.9	100.0	99.5	**99.8**
3	Países Bajos	99.5	99.0	99.8	**99.4**
4	Suecia	98.0	99.3	99.7	**99.0**
5	Alemania	98.1	97.0	98.1	**97.7**
6	Bélgica	93.8	98.6	98.9	**97.1**
7	Reino Unido	96.6	98.1	94.5	**96.4**
8	Austria	94.7	96.3	97.9	**96.3**
9	Estonia	94.3	97.2	96.2	**95.9**
10	Eslovenia	94.8	95.7	95.5	**95.3**
11	Luxemburgo	92.0	95.2	98.3	**95.2**
12	Francia	95.7	94.5	93.5	**94.5**
13	España	91.9	96.6	93.1	**93.9**
14	Irlanda	93.1	92.3	92.9	**92.8**
15	Letonia	84.6	86.5	88.5	**86.5**
16	Israel	84.4	85.1	85.7	**85.1**
17	EE.UU.	78.6	87.7	85.2	**83.8**
18	Portugal	73.4	80.2	87.5	**80.3**
19	Italia	62.4	82.6	90.6	**78.5**
20	Rep. Checa	73.7	77.1	70.6	**73.8**
21	Eslovaquia	72.8	69.9	77.9	**73.5**
22	Polonia	62.2	71.3	84.2	**72.6**
23	Lituania	69.3	69.1	77.9	**72.1**
24	Hungría	67.8	66.6	67.7	**67.4**
25	Turquía	47.1	51.1	56.4	**51.5**
26	Chile	30.4	53.8	66.9	**50.4**
27	**México**	**13.4**	**29.4**	**25.8**	**22.9**

FUENTE: elaboración propia con base en datos del Banco Mundial.

CUADRO 10.

PORCENTAJE DE LA POBLACIÓN QUE TIENE 15 AÑOS O MÁS CON ESTUDIOS MÁXIMOS A NIVEL PRIMARIA Y QUE TIENE CUENTA EN UNA INSTITUCIÓN FINANCIERA O CON UN PROVEEDOR DE SERVICIOS DE DINERO VÍA TELÉFONO CELULAR

Ranking	País	Promedio 2010-2012	Promedio 2013-2015	Promedio 2016-2018	Promedio 2010-2018
1	Dinamarca	100.0	100.0	100.0	**100.0**
2	Finlandia	99.2	100.0	99.2	**99.5**
3	Países Bajos	96.3	100.0	100.0	**98.8**
4	Suecia	98.5	100.0	96.9	**98.5**
5	Alemania	97.2	97.6	100.0	**98.3**
6	Bélgica	87.3	100.0	100.0	**95.8**
7	Luxemburgo	88.9	98.9	95.7	**94.5**
8	Austria	88.9	96.4	96.0	**93.8**
9	Reino Unido	89.9	100.0	90.2	**93.4**
10	Eslovenia	94.5	90.6	94.4	**93.2**
11	Estonia	87.8	91.6	94.4	**91.3**
12	España	87.6	93.2	89.0	**89.9**
13	Israel	91.1	83.7	88.3	**87.7**
14	Francia	97.7	83.4	79.8	**86.9**
15	Portugal	74.9	80.3	87.6	**80.9**
16	Irlanda	83.2	71.0	84.2	**79.5**
17	Italia	64.3	79.5	92.0	**78.6**
18	Letonia	74.4	74.3	79.4	**76.0**
19	EE.UU.	47.2	59.9	64.6	**57.2**
20	Turquía	50.9	47.5	57.4	**51.9**
21	Polonia	34.7	50.7	65.5	**50.3**
22	Lituania	47.4	40.1	61.3	**49.6**
23	Hungría	46.3	45.0	55.8	**49.0**
24	Rep. Checa	48.7	50.0	36.8	**45.2**
25	Eslovaquia	49.2	24.0	49.2	**40.8**
26	Chile	24.4	36.7	54.2	**38.4**
27	**México**	**13.4**	**30.0**	**24.5**	**22.6**

FUENTE: elaboración propia con base en datos del Banco Mundial.

CUADRO 11. PORCENTAJE DE LA POBLACIÓN DE 15 AÑOS O MÁS CON ESTUDIOS MÍNIMOS DE SECUNDARIA QUE TIENE CUENTA EN UNA INSTITUCIÓN FINANCIERA O CON UN PROVEEDOR DE SERVICIOS DE DINERO VÍA TELÉFONO CELULAR

Ranking	País	Promedio 2010-2012	Promedio 2013-2015	Promedio 2016-2018	Promedio 2010-2018
1	Finlandia	99.9	100.0	100.0	**100.0**
2	Dinamarca	99.7	100.0	99.9	**99.9**
3	Suecia	99.1	99.8	100.0	**99.6**
4	Países Bajos	99.0	99.2	99.6	**99.3**
5	Estonia	99.0	99.6	99.0	**99.2**
6	Alemania	98.6	98.8	99.3	**98.9**
7	Eslovenia	97.7	99.1	98.5	**98.5**
8	Bélgica	98.6	97.8	98.8	**98.4**
9	Reino Unido	98.5	98.8	97.8	**98.4**
10	Austria	98.3	96.9	98.5	**97.9**
11	Luxemburgo	95.8	96.2	99.4	**97.1**
12	Francia	96.8	97.3	97.2	**97.1**
13	España	95.2	98.1	95.8	**96.4**
14	Irlanda	95.6	97.3	96.2	**96.4**
15	Letonia	94.2	94.9	97.2	**95.4**
16	EE.UU.	89.9	94.3	94.4	**92.9**
17	Portugal	86.1	95.6	95.5	**92.4**
18	Israel	90.8	90.2	93.0	**91.3**
19	Italia	82.7	94.6	96.3	**91.2**
20	Rep. Checa	90.2	89.3	91.2	**90.2**
21	Eslovaquia	87.8	89.2	92.0	**89.7**
22	Polonia	81.4	83.7	90.0	**85.0**
23	Lituania	77.8	89.4	87.3	**84.8**
24	Hungría	83.6	83.5	82.8	**83.3**
25	Chile	51.1	71.3	80.9	**67.8**
26	Turquía	65.2	60.9	74.0	**66.7**
27	**México**	**37.9**	**46.2**	**43.8**	**42.6**

FUENTE: elaboración propia con base en datos del Banco Mundial.

CUADRO 12. PORCENTAJE DE LA POBLACIÓN EN CONDICIONES DE POBREZA MONETARIA DEBAJO DE UNA LÍNEA DE POBREZA DE 1.90 DÓLARES PPP CONSTANTES (AÑO BASE 2011)

Ranking	País	Promedio 2010-2012	Promedio 2013-2015	Promedio 2016-2018	Promedio 2010-2018
1	Rep. Checa	0.0	0.0	0.0	**0.0**
2	Alemania	0.0	0.0	0.0	**0.0**
3	Eslovenia	0.0	0.0	0.0	**0.0**
4	Finlandia	0.0	0.1	0.1	**0.1**
5	Francia	0.1	0.1	0.1	**0.1**
6	Países Bajos	0.1	0.1	0.1	**0.1**
7	Bélgica	0.2	0.1	0.1	**0.1**
8	Luxemburgo	0.0	0.2	0.2	**0.1**
9	Dinamarca	0.0	0.2	0.2	**0.2**
10	Reino Unido	0.2	0.2	0.2	**0.2**
11	Polonia	0.3	0.4	0.3	**0.3**
12	Turquía	0.5	0.3	0.2	**0.3**
13	Irlanda	0.4	0.5	0.1	**0.3**
14	Israel	0.4	0.5	0.2	**0.4**
15	Chile	0.6	0.4	0.3	**0.4**
16	Suecia	0.5	0.5	0.3	**0.4**
17	Austria	0.5	0.4	0.5	**0.5**
18	Portugal	0.4	0.6	0.4	**0.5**
19	Hungría	0.2	0.4	1.0	**0.5**
20	Estonia	0.8	0.8	0.4	**0.7**
21	Eslovaquia	0.4	0.5	1.4	**0.8**
22	Letonia	1.2	0.8	0.7	**0.9**
23	España	0.9	1.0	1.0	**0.9**
24	Lituania	1.1	0.9	1.2	**1.1**
25	EE.UU.	1.0	1.0	1.2	**1.1**
26	Italia	1.2	1.5	1.5	**1.4**
27	**México**	**4.3**	**3.8**	**2.0**	**3.3**

FUENTE: elaboración propia con base en datos del Banco Mundial.

CUADRO 13.

PORCENTAJE DE LA POBLACIÓN EN CONDICIONES DE POBREZA MONETARIA DEBAJO DE UNA LÍNEA DE POBREZA DE 3.20 DÓLARES PPP CONSTANTES (AÑO BASE 2011)

Ranking	País	Promedio 2010-2012	Promedio 2013-2015	Promedio 2016-2018	Promedio 2010-2018
1	Eslovenia	0.0	0.0	0.0	**0.0**
2	Francia	0.1	0.1	0.1	**0.1**
3	Finlandia	0.1	0.1	0.1	**0.1**
4	Alemania	0.1	0.0	0.2	**0.1**
5	Rep. Checa	0.2	0.1	0.1	**0.1**
6	Países Bajos	0.1	0.1	0.2	**0.2**
7	Bélgica	0.2	0.2	0.2	**0.2**
8	Dinamarca	0.0	0.3	0.3	**0.2**
9	Luxemburgo	0.1	0.2	0.3	**0.2**
10	Reino Unido	0.3	0.3	0.3	**0.3**
11	Irlanda	0.7	0.6	0.4	**0.5**
12	Austria	0.6	0.5	0.7	**0.6**
13	Suecia	0.7	0.7	0.4	**0.6**
14	Polonia	0.9	0.9	0.6	**0.8**
15	Israel	1.0	1.0	0.7	**0.9**
16	Hungría	0.4	1.0	1.5	**1.0**
17	Portugal	0.9	1.5	0.7	**1.0**
18	Estonia	1.6	1.3	0.7	**1.2**
19	Eslovaquia	0.9	1.0	1.8	**1.2**
20	EE.UU.	1.2	1.2	1.5	**1.3**
21	España	1.4	1.6	1.4	**1.5**
22	Chile	2.6	1.3	0.7	**1.5**
23	Italia	1.6	2.1	2.1	**1.9**
24	Lituania	2.3	2.1	1.9	**2.1**
25	Letonia	3.1	2.0	1.5	**2.2**
26	Turquía	4.0	2.7	1.7	**2.8**
27	**México**	**12.5**	**12.0**	**7.3**	**10.6**

FUENTE: elaboración propia con base en datos del Banco Mundial.

CUADRO 14.

PORCENTAJE DE LA POBLACIÓN EN CONDICIONES DE POBREZA MONETARIA DEBAJO DE UNA LÍNEA DE POBREZA DE 5.50 DÓLARES PPP CONSTANTES (AÑO BASE 2011)

Ranking	País	Promedio 2010-2012	Promedio 2013-2015	Promedio 2016-2018	Promedio 2010-2018
1	Finlandia	0.1	0.1	0.2	**0.1**
2	Eslovenia	0.2	0.2	0.1	**0.1**
3	Francia	0.3	0.2	0.2	**0.2**
4	Alemania	0.2	0.2	0.5	**0.3**
5	Países Bajos	0.2	0.3	0.4	**0.3**
6	Bélgica	0.4	0.3	0.3	**0.3**
7	Luxemburgo	0.2	0.4	0.5	**0.4**
8	Dinamarca	0.3	0.6	0.3	**0.4**
9	Reino Unido	0.6	0.6	0.5	**0.6**
10	Rep. Checa	0.7	0.5	0.5	**0.6**
11	Austria	0.9	0.7	1.0	**0.9**
12	Suecia	1.1	1.1	0.6	**0.9**
13	Irlanda	1.2	1.0	0.7	**1.0**
14	EE.UU.	2.0	2.0	2.0	**2.0**
15	Polonia	3.0	2.8	1.6	**2.5**
16	Estonia	3.9	3.0	1.3	**2.7**
17	España	2.7	3.1	2.7	**2.8**
18	Italia	2.6	3.0	3.2	**3.0**
19	Eslovaquia	2.5	3.1	3.3	**3.0**
20	Portugal	3.1	3.7	2.4	**3.1**
21	Hungría	3.2	3.4	2.9	**3.2**
22	Israel	4.4	3.5	2.7	**3.5**
23	Lituania	6.6	4.7	4.2	**5.2**
24	Letonia	8.6	5.2	3.5	**5.8**
25	Chile	12.4	6.1	3.7	**7.4**
26	Turquía	14.2	11.1	9.4	**11.6**
27	**México**	**32.8**	**33.6**	**24.4**	**30.2**

FUENTE: elaboración propia con base en datos del Banco Mundial.

INDICADORES DE POBREZA Y CARENCIAS SOCIALES EN MÉXICO

CUADRO 15.

Año	Pobreza	Pobreza moderada	Pobreza extrema	Rezago educativo	Carencia por acceso a los servicios de salud	Carencia por acceso a la seguridad social	Carencia por calidad y espacios de la vivienda	Carencia por acceso a los servicios básicos en la vivienda	Carencia por acceso a la alimentación
2008	44.4	33.3	11.0	21.9	38.4	65.0	17.7	22.9	21.7
2010	46.1	34.8	11.3	20.7	29.2	60.7	15.2	22.9	24.8
2012	45.5	35.7	9.8	19.2	21.5	61.2	13.6	21.2	23.3
2014	46.2	36.6	9.5	18.7	18.2	58.5	12.3	21.2	23.4
2016	43.6	35.9	7.6	17.4	15.5	55.8	12.0	19.3	20.1
2018	41.9	34.5	7.4	16.9	16.2	57.3	11.1	19.8	20.4

FUENTE: elaboración propia con base en datos de CONEVAL.

También debe tenerse en cuenta que el impulso a la inclusión financiera digital tiene como condición necesaria una adecuada conectividad y cobertura para teléfonos celulares, principalmente en áreas rurales, lo que a su vez necesita de una suficiente inversión en la infraestructura conveniente; asimismo, se requiere un marco regulatorio apropiado que asegure la protección de los datos de consumidores e inversionistas, y de igual forma necesita el fomento del uso de pagos digitales (Ketterer, 2019; Bin, 2019).

CONTRIBUCIÓN AL FORTALECIMIENTO DE LOS INGRESOS PÚBLICOS MEDIANTE EL COBRO DE IMPUESTOS A PLATAFORMAS DIGITALES EN MÉXICO

Como se mencionó anteriormente, la digitalización reduce los costos de transporte y de comunicación y permite a las empresas alcanzar e interactuar con consumidores en un mercado de forma remota o a través de una presencia física limitada. También existen negocios establecidos que realizan intermediación de consumidores y compañías altamente digitalizadas (OECD, 2019b). Mientras los consumidores pasan más tiempo en línea, las empresas también necesitan hacerlo, lo cual reduce la necesidad de la presencia física y con ello los derechos de cobro de impuestos en las distintas jurisdicciones. Hace años, para establecerse de forma exitosa en un mercado externo era necesario desarrollar una base de consumo y crear valor a través de la presencia física y la proximidad a los mercados, situación que no necesariamente ocurre actualmente. Las ventas y el mercadeo pueden llevarse a cabo de forma remota y a través de embarques, con riesgos limitados y cumpliendo con requisitos legales (OECD, 2019b).

Como argumentan Olbert y Spengel (2017), la digitalización de la economía es un conductor clave de la innovación, el crecimiento económico, y el cambio social; sin embargo, representa un gran reto para el cobro de impuestos en el ámbito mundial, pues muchas compañías transnacionales usan transacciones de la economía digital y toman ventaja de vacíos internacionales en materia fiscal para eludir el pago de impuestos, lo que conlleva a la erosión de la base gravable (Peng, 2016). Los marcos fiscales tradicionales están diseñados para bienes y servicios asociados con una presencia física o a una actividad; sin embargo, la economía digital es intangible y no se ajusta a los supuestos anteriores, lo que implica la necesidad de adaptar los entornos regulatorios al

contexto actual (Li, 2018). Como señala Gerooms (2019), una de las alternativas para abordar el cobro de impuestos a intangibles, como es el caso de la economía digital, es la propuesta de Estados Unidos de América (EUA) sobre el cobro de impuestos a las ganancias obtenidas por las compañías en el mercado nacional, independientemente del lugar en el que esté registrada la empresa que obtiene dichas ganancias.[7]

Varias empresas digitales cuentan con la capacidad de generar ingresos en distintos países sin tener presencia física en ellos (pues cuentan con activos intangibles que son difíciles de localizar y valuar).[8] Cabe señalar que América Latina se encuentra atrasada en el desarrollo de economía digital y es importadora neta de este tipo de bienes y servicios (Seira *et al.*, 2019).

Las empresas digitales son aquellas que usan la tecnología del Internet como parte fundamental de su negocio, entre las que destacan (*idem*):

- Mercados en línea. Intermediarios entre compradores y vendedores (Ebay, Amazon, Airbnb, Uber, entre otros, son ejemplos de estos intermediarios).
- Plataformas de redes sociales. Permiten conectar usuarios entre sí y anunciantes con usuarios (entre ellos se encuentra Google +, Facebook, Instagram, Twitter). Se caracterizan porque el contenido es provisto por los mismos usuarios.
- Buscadores de Internet. Son compañías que permiten a los usuarios buscar contenidos a través de algoritmos (Google, Yahoo y Bing, son ejemplos de ellos).

De esta forma, la digitalización y algunos de los modelos de negocios que facilita, representan importantes retos para la política tributaria en el ámbito internacional. En particular, es importante tener una idea de la forma en que deberían asignarse entre países los impuestos cobrados a las actividades que generan ingresos transfronterizos en la era digital. La gran dependencia en activos intangibles restringe las reglas de asignación de ingresos de este tipo de activos entre las diferentes partes del grupo de una multinacional, lo que crea incertidumbre y oportunidades para la elusión de impuestos. Lo anterior se presenta, principalmente, en negocios altamente digitalizados en los cuales no existe contenido imponible en la jurisdicción donde los usuarios residen (OECD, 2019b).

Ante ello, la OECD (2019b) establece que debe reconocerse en los distintos ordenamientos legales el valor creado por la actividad de un negocio (sin presencia física en un país), la participación en una jurisdicción de un mercado o usuario, para la asignación de ganancias. Este tipo de empresas permite una participación remota en la economía doméstica a través de medios digitales, pero sin una presencia física imponible. Actualmente el Proyecto de Erosión de la Base Fiscal y Redireccionamiento de Ganancias (BEPS, por sus siglas en inglés), se encuentra analizando propuestas relacionadas con la asignación de utilidades en respuesta a los retos impuestos por la digitalización. A continuación, se describen algunas de las principales propuestas:

1. **Participación del usuario.** Esta propuesta se basa en el valor creado por negocios altamente digitalizados a través del desarrollo de una base activa de usuarios. En este caso, las plataformas de *social-media* incorporan contenido generado por los propios usuarios, donde el volumen y la actividad de los mismos es un factor clave para generar utilidades, mediante los usuarios que pagan por ver ese contenido o por publicidad. Esta propuesta también abarca los motores de búsqueda y los mercados en línea.[9]
2. **Mercadeo de intangibles.** A diferencia de la propuesta anterior, este se aplicaría a un rango más amplio de la economía digital. Las jurisdicciones de mercado tendrían el derecho de cobrar impuestos a las actividades altamente digitalizadas, incluso en la ausencia de lo que causa el impuesto (intangibles), debido a la importancia de ese tipo de bienes en esos negocios (OECD, 2019b).

7 En el mismo sentido, Seira *et al.*, (2019) señalan que en la actualidad existen compañías digitales con tasas efectivas de pago de impuestos muy bajas, lo cual erosiona la base gravable y los ingresos públicos.

8 Si existe un establecimiento permanente, se dice que la empresa tiene un *nexus* en el país y eso le permite a este cobrar impuestos a la empresa (aunque sólo sobre los ingresos generados en ese país). Si la producción se hace en varios países, existen tratados internacionales para determinar la fracción del impuesto que les corresponde.

9 Una limitante de esta propuesta es la dificultad de cálculo de los precios de transferencia, por lo que se requiere estimaciones de ganancia residuales y porcentajes preestablecidos (OECD, 2019b).

3 **Presencia económica significativa.** Se refiere a la situación en la cual una empresa digital está envuelta en la vida económica de una jurisdicción, pero no tiene una presencia física significativa. Con esta propuesta, los derechos de cobro de impuestos emergen cuando una compañía no residente tiene una presencia económica significativa basada en una interacción relevante en una jurisdicción a través de la tecnología digital y otros medios automáticos. Además de los ingresos obtenidos en una jurisdicción, estos deben interactuar con otros factores para considerar la presencia económica significativa y los derechos del cobro de impuestos. Entre dichos factores se encuentran: la existencia de una base de usuarios; el volumen de contenido digital; el cobro en moneda local o a través de formas locales de pago; mantener un sitio web en el idioma local; la responsabilidad de la entrega final de bienes y servicios y la provisión de servicios de posventa (como reparación y mantenimiento); y actividades de mercadeo y venta (en línea u otros) para atraer consumidores (OECD, 2019b).

Por otro lado, de acuerdo con Seira *et al.* (2019), las dificultades en el cobro de impuestos a empresas digitales tienen su origen en el marco tributario internacional vigente, basado en tres pilares fundamentales: *1)* el cobro de impuestos en el país fuente; *2)* transacciones valuadas en valor de mercado; y *3)* bilateralidad de los acuerdos internacionales. Estos pilares, sin embargo, generan vacíos legales que las compañías utilizan para reasignar ganancias y reducir su tasa de tributación efectiva (algunas multinacionales, por ejemplo, encuentran la forma de registrar sus dividendos en países con menores tasas de impuestos).

El que algunas empresas digitales eludan gravámenes genera problemas de eficiencia económica, pues las compañías no digitales pagan mayores tasas y se encuentran en desventaja. Se genera, además, menor justicia distributiva, pues las empresas que pagan menos impuestos también usan bienes y servicios públicos para generar valor (por lo que deberían contribuir al fisco) e, incluso, pueden generar inestabilidad política y ganar poder de mercado (compañías muy grandes como Facebook o Netflix podrían tener demasiada influencia política y riesgos a la democracia, o bien limitar la competencia en el sector) (Seira *et al.*, 2019).

Con el fin de reducir la elusión y generar mayores ingresos fiscales, los países deben modificar sus leyes tributarias, así como incluir nuevos conceptos y decidir si gravarán ganancias, insumos o ventas. Cada operación debe ser estudiada para tratar de generar las menores distorsiones posibles en el mercado, se requiere además que exista cooperación internacional al respecto (Seira *et al.*, 2019).

Lo anterior resulta relevante, pues México ha ocupado tradicionalmente el último lugar en los países que conforman la OCDE en relación con la proporción que representan los ingresos tributarios respecto del producto interno bruto (PIB). Durante el periodo 2013-2017, los ingresos tributarios de México representaron en promedio 15.1% de su PIB, mientras que la media de la OCDE fue de 33.8%. Aun después de que México impulsó una reforma fiscal recientemente, su recaudación tributaria en 2017 apenas representó 16.2% del PIB, mientras que la media de la OCDE en dicho año fue de 34.2%. En ese sentido, la brecha entre los ingresos tributarios como proporción del PIB en México respecto del promedio de los países que integran la OCDE es de 18.0 puntos porcentuales del PIB en el último año del periodo analizado.

La eliminación de un factor que erosiona la base gravable de México, al cobrar impuestos ya existentes a las plataformas digitales, contribuiría al fortalecimiento de los ingresos públicos.

Cambios en la normatividad fiscal en México

En la presentación del paquete económico para el ejercicio fiscal 2020, el Ejecutivo federal incluyó diversos cambios en materia de economía digital.[10] En cuanto al ISR, se actualizó el concepto de establecimiento permanente, de acuerdo con las recomendaciones del BEPS. Esta figura de establecimiento permanente, tanto en la legislación interna, como en los Convenios para Evitar la Doble

10 Durante su comparecencia ante el Senado de la República en septiembre de 2019, el secretario de Hacienda indicó que en los últimos años ha habido una revolución digital extraordinariamente importante que ha disminuido los costos transaccionales y ha hecho que las cosas sean más rápidas, más seguras, y que van desde la descarga de contenidos, como en Netflix y Spotify, hasta el transporte mediante el uso de plataformas electrónicas como Uber y Didi (Canal del Congreso, 2019). También explicó que este sector, por su propia naturaleza, es el que más está creciendo en el mundo, en

CUADRO 16.

PROMEDIO DE INGRESOS TRIBUTARIOS COMO PROPORCIÓN DEL PIB EN PAÍSES DE LA OCDE, 2013-2017

	PROMEDIO 2013-2017				
País	**Total**	**Nivel de gobierno federal o central**	**Nivel de gobierno estatal o regional**	**Nivel de gobierno municipal o local**	**Fondos de seguridad social**
Dinamarca	46.5	34.1	0.2	12.3	0.0
Francia	45.6	15.3	0.1	6.0	24.1
Bélgica	44.7	24.2	3.9	2.2	14.4
Finlandia	43.7	20.8	0.1	10.3	12.6
Suecia	43.3	22.1	0.1	15.6	5.4
Italia	43.1	23.2	0.1	6.9	13.0
Austria	42.5	28.3	0.8	1.3	12.1
Islandia	39.9	30.3	0.0	9.6	0.0
Noruega	38.8	33.0	-0.0	5.8	0.0
Hungría	38.3	23.3	0.1	2.2	12.7
Luxemburgo	37.9	25.9	0.1	1.4	10.6
Países Bajos	37.5	21.4	0.4	1.3	14.4
Grecia	37.2	25.5	0.1	0.9	10.7
Alemania	37.1	11.3	8.7	3.1	14.0
Eslovenia	36.3	18.2	0.2	3.6	14.3
Portugal	34.4	25.1	0.1	2.5	6.7
República Checa	33.9	18.7	0.2	0.4	14.7
Promedio OCDE	**33.8**	**20.2**	**1.5**	**3.7**	**8.4**
España	33.4	14.0	4.9	3.3	11.1
Estonia	32.8	26.9	0.2	0.3	5.4
Polonia	32.7	15.9	0.1	4.2	12.5
Reino Unido	32.4	24.6	0.2	1.6	6.1
Canadá	32.0	13.1	12.7	3.3	2.9
Eslovaquia	31.8	17.4	0.2	0.7	13.5
Israel	31.5	23.8	0.0	2.5	5.2
Nueva Zelanda	31.4	29.2	-0.0	2.1	0.0
Japón	30.1	10.9	-0.1	7.2	12.1
Letonia	29.5	15.2	0.2	5.7	8.4
Lituania	28.6	16.4	0.3	0.4	11.6
Australia	27.5	22.0	4.6	1.0	0.0
Suiza	27.5	9.8	6.8	4.2	6.7
Estados Unidos	26.2	11.2	5.1	3.7	6.2
Corea del Sur	25.4	14.4	-0.0	4.3	6.7
Irlanda	25.2	20.7	0.2	0.6	3.6
Turquía	25.0	15.5	0.0	2.4	7.2
Chile	20.0	17.4	-0.0	1.5	1.1
México	**15.1**	**12.1**	**0.6**	**0.2**	**2.2**

FUENTE:

elaboración propia con base en datos de la OCDE.

Imposición, es fundamental para determinar cuándo un residente extranjero debe pagar impuesto sobre la renta (ISR) en nuestro país (SHCP, 2019 y 2019b; IBD, 2019).

En cuanto a los ingresos sujetos a regímenes fiscales preferentes que obtienen entidades extranjeras controladas, se propuso combatir las planeaciones fiscales agresivas que utilizan organismos residentes en el extranjero, cuyos ingresos se encuentran sujetos a un régimen fiscal preferente. La propuesta atendió gran parte de las recomendaciones del BEPS y uno de los cambios principales fue el supuesto para determinar cuándo el contribuyente tiene control sobre la entidad extranjera. Las propuestas buscaron aclarar que para determinar si los ingresos de una entidad extranjera se encontraban sujetos a un régimen fiscal preferente, se tenían que considerar todos los impuestos sobre la renta pagados.

En lo que se refiere a la limitación a la deducción de intereses, la iniciativa señaló que, de acuerdo con el BEPS, una de las técnicas más sencillas para trasladar utilidades como parte de una planeación fiscal internacional es el pago de intereses entre partes relacionadas e independientes. Por lo que se propuso un ratio de 30%. Adicionalmente, se otorgó la facultad al Servicio de Administración Tributaria (SAT) para regular los supuestos en los cuales el contribuyente no tenga una utilidad neta ajustada de conformidad con la regla propuesta.

En cuanto al tratamiento fiscal a los ingresos por la prestación de servicios o enajenación de bienes a través de Internet, mediante plataformas tecnológicas, aplicaciones informáticas y similares, la iniciativa reconoció que resulta complicado determinar

2017 representaba 4.6% del PIB en México; para 2019, se estimaba en 5.2% del PIB. Herrera explicó que en México las plataformas digitales han comenzado a pagar los impuestos tradicionales que son el impuesto al valor agregado (IVA) y el impuesto sobre la renta (ISR); sin embargo, enfatizó que no se trata de haber creado un impuesto específico para dichas actividades, como sí se ha hecho en países como Francia o España. Señaló, además, que el marco tributario de México está diseñado para bienes tangibles, y que no se requiere crear nuevos impuestos para las actividades relacionadas con la economía digital, sino encontrar la forma de retener el pago de los impuestos existentes (Canal del Congreso, 2019). Explicó que se habían creado una serie de mecanismos y acuerdos bilaterales con las plataformas de transporte, con Netflix, entre otros, y que se llevarán a cabo retenciones de impuestos a dichas plataformas. Asimismo, señaló que cobrar impuestos a plataformas digitales de transporte era un tema de equidad, ya que los taxistas tradicionales que no usan dichas plataformas tienen que pagar ISR, mientras los choferes de Uber, Didi, entre otros, no lo estaban pagando.

la jurisdicción en la cual tiene lugar la creación de valor y que recientemente, han surgido diversas plataformas tecnológicas que, a través de la red, interconectan a las personas para poder realizar un intercambio comercial de bienes y servicios; por ejemplo, de transporte privado de personas, reparto de bienes o comida, incluso la prestación del servicio de hospedaje. Se propuso que las plataformas digitales residentes en México y las residentes en el extranjero, con o sin establecimiento permanente en el país, tengan la obligación de retener y enterar el impuesto correspondiente, teniendo el carácter de pago provisional de la retención respecto de cada persona física que preste servicios o enajene bienes a través de las plataformas tecnológicas, aplicaciones informáticas y similares.

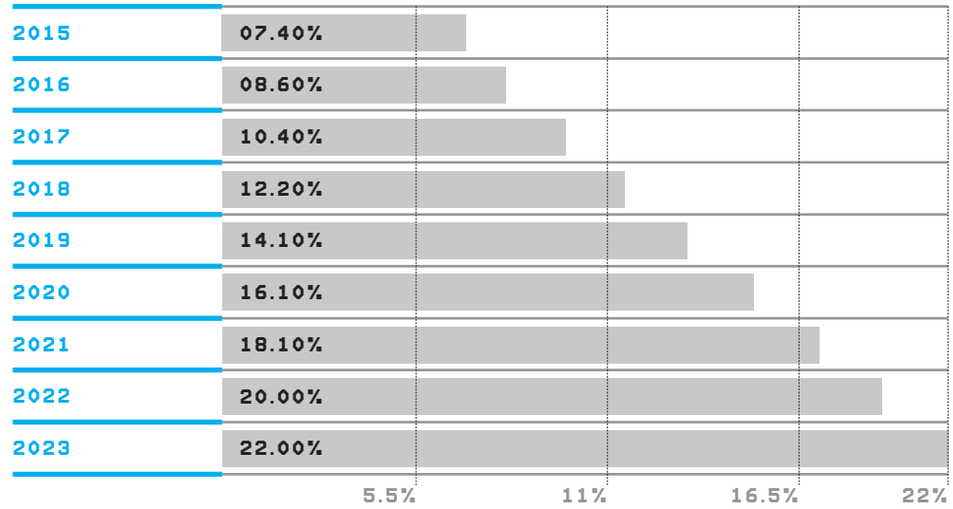
En lo que se refiere al IVA, la iniciativa reconoció la existencia de un área de oportunidad importante para establecer medidas orientadas a incrementar la eficiencia en la recaudación del IVA. También que, en materia de economía digital, el marco legal y tributario del país se encontraba desactualizado por el avance tecnológico de la última década y se propuso que, tratándose de servicios digitales prestados por residentes en el extranjero sin establecimiento en México, se considere que el servicio se presta en territorio nacional, cuando el receptor del servicio se encuentre en el territorio mencionado.

La propuesta no sería aplicable a todos los servicios digitales, sino exclusivamente a la categoría que generalmente son de consumo final en los hogares o utilizados por las personas para consumo individual, como son: la descarga o acceso a imágenes, películas, texto, información, video, audio, música, juegos, entre otros (servicios de streaming de audio o video para ver películas o escuchar música).

Finalmente, en lo referente a servicios de transporte particular, se propuso aclarar que cuando se presta el servicio de transporte de personas y se contrata mediante plataformas digitales de intermediación entre terceros y cuando los vehículos con los que se proporcione el servicio sean de uso particular, no se trata de transporte público y no procede exención.

Estas propuestas fueron aprobadas y entraron en vigor a partir del 1 de junio de 2020.

GRÁFICA 01. PARTICIPACIÓN DE MERCADO DEL COMERCIO ELECTRÓNICO EN EL COMERCIO AL POR MENOR EN EL NIVEL MUNDIAL, 2015-2023



FUENTE:
elaboración propia con datos de Statista.

Oportunidades de negocio que ofrece el comercio electrónico en México

A partir de datos de Statista, se observa que el comercio electrónico ha mantenido una creciente participación de mercado en el comercio al por menor en el nivel mundial. En 2019, dicha participación fue de 14.1%, y para 2023 se estima que será de 22.0 por ciento.

Como explica la Organización Mundial del Comercio (OMC; WTO por sus siglas en inglés), las medidas de aislamiento social y confinamiento instrumentadas para hacer frente a la pandemia de Covid-19 han derivado en que los consumidores recurran aún más a las compras por Internet, particularmente de artículos para el cuidado de la salud, artículos de primera necesidad para el hogar, y productos alimenticios (WTO, 2020). Asimismo, se ha incrementado el uso de redes sociales, los servicios de telefonía por Internet y las teleconferencias, así como la transmisión de películas y videos en línea (WTO, 2020).

A partir de datos de la Encuesta Mensual de Empresas Comerciales (EMEC) que reporta Inegi, se observa que la rama de actividad comercial del comercio al por menor que mayor crecimiento tuvo tanto en 2019, como en el periodo 2015-2019 fue la de "comercio al por menor exclusivamente a través de Internet, y catálogos impresos,

CUADRO 17. CRECIMIENTO REAL EN LOS INGRESOS POR LA VENTA DE BIENES Y SERVICIOS EN RAMAS DE LA ACTIVIDAD COMERCIAL EN EL COMERCIO AL POR MENOR EN MÉXICO

Rama de la actividad comercial	Crecimiento anual real en 2019	Tasa media de crecimiento anual (TMCA) durante el período 2015-2019
Comercio al por menor exclusivamente a través de Internet, y catálogos impresos, televisión y similares	**36.8%**	**34.3%**
Motocicletas y otros vehículos de motor	9.7%	8.8%
Artículos de perfumería y joyerí	9.2%	3.3%
Tiendas departamentales	7.2%	4.5%
Calzado	6.4%	4.7%
Partes y refacciones para automóviles, camionetas y camiones	5.3%	1.6%
Muebles para el hogar y otros enseres domésticos	4.7%	5.8%
Combustibles, aceites y grasas lubricantes	4.3%	-0.3%
Tiendas de autoservicio	3.6%	2.7%
Ropa, bisutería y accesorios de vestir	3.2%	4.5%
Artículos para la decoración de interiores	3.2%	4.8%
Artículos de cuidados para la salud	2.5%	3.7%
Bebidas, hielo y tabaco	-0.5%	3.6%
Abarrotes y alimentos	-0.7%	-0.1%
Mascotas, regalos, artículos religiosos, desechables y otros artículos de uso personal	-1.4%	2.3%
Artículos para el esparcimiento	-1.7%	1.8%
Artículos de ferretería, tlapalería y vidrios	-1.7%	2.2%
Mobiliario, equipo y accesorios de cómputo, teléfonos y otros aparatos de comunicación	-4.1%	4.7%
Productos textiles, excluyendo ropa	-4.5%	2.2%
Papelería, libros, revistas y periódicos	-5.1%	-2.2%

FUENTE: elaboración propia con base en datos de la Encuesta Mensual de Empresas Comerciales, de Inegi.

CUADRO 18. CRECIMIENTO REAL EN LOS INGRESOS POR LA VENTA DE BIENES Y SERVICIOS EN RAMAS DE LA ACTIVIDAD COMERCIAL EN EL COMERCIO AL POR MENOR EN MÉXICO (MARZO, 2020)

Rama de la actividad comercial	Crecimiento real mensual en marzo 2020	Crecimiento real anual (marzo 2020 *vs* marzo 2019	Tasa media de crecimiento anual (TMCA) durante el período marzo 2016 - marzo 2020
Comercio al por menor exclusivamente a través de Internet, y catálogos impresos, televisión y similares	**14.1%**	**42.9%**	**33.2%**
Tiendas de autoservicio	21.9%	16.3%	7.0%
Motocicletas y otros vehículos de motor	-4.2%	-10.9%	4.2%
Artículos de cuidados para la salud	10.4%	6.3%	3.7%
Muebles para el hogar y otros enseres domésticos	-1.0%	-5.8%	2.4%
Artículos de ferretería, tlapalería y vidrios	7.0%	1.6%	1.0%
Partes y refacciones para automóviles, camionetas y camiones	-1.6%	-9.2%	-0.2%
Combustibles, aceites y grasas lubricantes	2.7%	3.4%	-0.7%
Tiendas departamentales	-5.1%	-15.7%	-1.0%
Mobiliario, equipo y accesorios de cómputo, teléfonos y otros aparatos de comunicación	0.1%	-15.5%	-1.9%
Artículos usados	-15.6%	-21.6%	-2.3%
Calzado	-16.5%	-18.9%	-2.5%
Abarrotes y alimentos	-4.0%	-9.4%	-2.7%
Artículos para la decoración de interiores	-22.3%	-18.1%	-3.0%
Productos textiles, excluyendo ropa	-7.0%	-11.8%	-3.1%
Mascotas, regalos, artículos religiosos, desechables y otros artículos de uso personal	-13.8%	-16.3%	-3.4%
Automóviles y camionetas	-9.4%	-15.8%	-4.1%
Artículos para el esparcimiento	-22.8%	-22.3%	-4.1%
Bebidas, hielo y tabaco	-5.0%	-19.3%	-4.6%
Artículos de perfumería y joyería	-15.0%	-32.0%	-5.2%
Ropa, bisutería y accesorios de vestir	-25.4%	-30.3%	-5.4%
Papelería, libros, revistas y periódicos	-17.3%	-17.8%	-8.1%

FUENTE: elaboración propia con base en datos de la Encuesta Mensual de Empresas Comerciales, de Inegi.

televisión y similares". El último dato actualizado por Inegi de la EMEC corresponde al mes de marzo de 2020, en el cual ya se refleja el impacto de la pandemia de Covid-19. Las ramas de la actividad comercial en el comercio al por menor que reportaron en dicho mes el mayor crecimiento real respecto del mes anterior fueron: *i)* tiendas de autoservicio; *ii)* comercio al por menor exclusivamente a través de Internet, y catálogos impresos, televisión y similares; y *iii)* artículos de cuidados para la salud. Como mencionó la OMC, las medidas de aislamiento social y confinamiento instrumentadas durante la pandemia actual, han derivado en un incremento significativo de las compras por Internet. Así, es de esperarse que una proporción significativa de las ventas de las tiendas de autoservicio y de las farmacias se hayan llevado a cabo mediante Internet desde que dichas medidas comenzaron a instauarse para hacer frente a la pandemia.

Se anticipa que durante la etapa posterior a la pandemia podría mantenerse una mayor proclividad a realizar en línea actividades como realizar compras, tener reuniones laborales o sociales, tomar cursos, entre otras, con relación a la etapa previa a dicha pandemia. En ese sentido, se anticipan crecientes oportunidades de negocio vinculadas a ciberseguridad, servicios financieros digitales, teletrabajo, capacitación en línea, análisis de *Big Data*, realidad aumentada, inteligencia artificial, comercio electrónico, logística y cadena de suministros, y en general, a las áreas que pertenecen o están estrechamente asociadas a la economía digital (Gómez, 2017; Innovación Económica, 2020).

COMENTARIOS FINALES

La Internet ha revolucionado múltiples áreas de la actividad humana. La economía digital continuará su expansión y, con ella, las diversas áreas de oportunidad que ofrece para impulsar el desarrollo y el bienestar.

El uso de herramientas digitales para elevar la inclusión financiera en zonas rurales y para la población en situación de pobreza y vulnerabilidad económica puede formar parte de una estrategia integral de combate a dicha situación.

La existencia de bienes y servicios intangibles, gracias a la economía digital ante la falta de presencia física en un mercado o jurisdicción, dificultan el cobro de impuestos a las compañías digitales. Sin embargo, la OECD se encuentra analizando diversas propuestas encaminadas a reducir la elusión impositiva.

México realizó diversas modificaciones a su marco legal para que a partir de 2020 se comenzara a atender esta problemática haciendo que impuestos ya existentes como el IVA y el ISR fueran retenidos y pagados por estas empresas digitales.

La actual pandemia de Covid-19 ha acentuado algunas de las áreas de oportunidad asociadas con la economía digital. El impacto de dicha pandemia puede ser tal que incluso cuando esta sea superada de forma sostenible, con la disponibilidad para todo el que lo necesite, de un tratamiento o vacuna, diversos hábitos de consumo e interacción humana podrían verse modificados.

Es tan vasto el campo de acción de la economía digital que, como ha sido argumentado en la presente investigación, puede asociarse de forma directa o indirecta a la inclusión financiera, la reducción de la pobreza y la vulnerabilidad económica, el fortalecimiento de los ingresos públicos, y a gran número de oportunidades de negocio.

BIBLIOGRAFÍA

Arora, R. (2012). Financial Inclusion and Human Capital in Developing Asia: the Australian connection. *Third World Quarterly*, (33)1, Taylor & Francis, Ltd.

Bin, H. (2019). Digital Financial Inclusion. En Andrade, G. (ed.) (2019). Shaping the Future of Financial Services in the Digital Economy. Proceedings from the Fourth Policy and Knowledge between Latin America and the Caribbean and China. Institutions for Development Sector. Connectivity, Markets and Finance Division. Discussion Paper No. IDB-DP-694. International Development Bank.

BBVA Research (2015). Medición de la economía digital. Abril de 2015.

Canal del Congreso (2019). Sesión Ordinaria de la H. Cámara de Diputados. Comparecencia del Titular de la Secretaría de Hacienda y Crédito Público, Canal del Congreso, 26 de septiembre de 2019. Recuperado de https://bit.ly/3Mo1Dns

Demirguc-Kunt, A. y Klapper, L. (2013). Measuring Financial Inclusion: Explaining Variation in Use of Financial Services across and within Countries. *Brookings Papers on Economic Activity*. Spring 2013. Brookings Institution Press.

Gerooms, M. (2019). *Taxation of the Digital Economy*, KPMG Tax & Legal Advisors.

Gómez, A. (2017). 6 Future trends in e-commerce that you can't lose sight of, ECN. Recuperado de https://bit.ly/35uEFdS

Heath, J. (2019). *¿Recesión?*, Jonathan Heath, Análisis y Perspectivas Económicas de México. Recuperado de https://bit.ly/3vGeEmn

Hernández, H. (2018). *Economía digital, claves y retos de la era del Internet*. Recuperado de https://bit.ly/3pGgYGt

IBD (2019), Aspectos relevantes de las modificaciones en materia de ISR, IVA, IEPS y CFF propuestas en el paquete económico 2020. Recuperado de https://bit.ly/3KfX7FQ

Innovación Económica (2020). Diez ideas de negocios post pandemia, Innovación Económica. Recuperado de https://bit.ly/3HCW2X3

Ketterer, J. (2019). Digital Finance in Latin America: Trends and Challenges. En Andrade, G. (ed.). Shaping the Future of Financial Services in the Digital Economy. Proceedings from the Fourth Policy and Knowledge between Latin America and the Caribbean and China. Institutions for Development Sector. Connectivity, Markets and Finance Division. Discussion Paper IDB-DP-694. International Development Bank.

Levenson, G. (2016). *Capital and the Common Good*. Columbia University Press.

Li, J. (2018). Protecting the Tax Base in a Digital Economy. Research Paper 78. Legal Studies Research Paper Series, Osgoode Hall Law School.

Manji, A. (2010). Eliminating Poverty? "Financial Inclusion", Access to Land, and Gender Equality in International Development. *The Modern Law Review*, Wiley on behalf of the Modern Law Review.

OECD (2019b). Addressing the tax challenges of the digitalization of the economy. Public consultation document. Base Erosion and Profit Shifting Project (BEPS).

OECD (2019). Going Digital: Shaping policies, improving lives. Paris: OECD publishing.

Olbert, M. y Spenger, C. (2017). International Taxation in the Digital Economy: Challenge Accepted? *World Tax Journal*. February. IBFD.

Peng, W. (2016). Multinational Tax Base Erosion Problem of the Digital Economy. *Modern Economy*, 2016 (7). Scientific Research Publishing.

Seira, E., Pineda, E. y Rasteletti, A., (2019). Retos para el cobro del impuesto sobre la renta en la economía digital. Causas y propuestas para enfrentarlos. Banco Interamericano de Desarrollo. Documento para discusión no. IBD-DP-723.

SHCP (2019). Iniciativa de Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Ley del Impuesto sobre la Renta, de la Ley del Impuesto al Valor Agregado, de la Ley del Impuesto sobre Producción y Servicios y del Código Fiscal de la Federación. Recuperado de https://bit.ly/3IJ78Li

SHCP (2019b), Iniciativa de Ley de Ingresos de la Federación para el Ejercicio Fiscal de 2020. Recuperado de https://bit.ly/3sIiJVj

World Trade Organization (2020). E-Commerce, Trade and the Covid-19 Pandemic, World Trade Organization (WTO). Recuparado de https://bit.ly/375r2Cn

SITIOS WEB CONSULTADOS

Coneval: https://www.coneval.org.mx/Paginas/principal.aspx
Inegi, Encuesta Nacional de Inclusión Financiera (enif) 2018: https://www.inegi.org.mx/programas/enif/2018/
Inegi, Banco de Información Económica (BIE): https://www.inegi.org.mx/sistemas/bie/
Inegi, Sistema de Indicadores Cíclicos: https://www.inegi.org.mx/app/saladeprensa/noticia.html?id=5678
OECD, Database: http://stats.oecd.org/
Statista: https://www.statista.com/statistics/534123/e-commerce-share-of-retail-sales-worldwide/
World Bank, World Development Indicators: http://databank.worldbank.org/data/views/variableSelection/selectvariables.aspx?-source=world-development-indicators

CAPÍTULO 11

ACCESO A INTERNET E INCLUSIÓN FINANCIERA: TEORÍA Y EVIDENCIA ACERCA DEL ROL DE LA INNOVACIÓN TECNOLÓGICA

MARÍA FERNANDA VIECENS*

* La autora es investigadora del Conicet en la Universidad de San Andrés, Argentina, donde además ejerce la docencia.

La importancia del acceso a Internet como fuente de crecimiento, e inclusión social, ha sido tema de un importante cuerpo de literatura académica y de difusión. A partir de esta premisa, luego de la crisis de 2008, muchos gobiernos en todo el mundo desarrollaron importantes proyectos de despliegue de redes de banda ancha frente a un convencimiento de la importancia del acceso a Internet para promover la productividad y la innovación.[1]

Para determinar en qué medida la evidencia empírica daba soporte al entusiasmo de los gobiernos a la hora de invertir en infraestructura de comunicaciones, en Galperin y Viecens (2016; 2017) se buscó establecer un vínculo teórico entre la adopción del uso de Internet y la reducción de la pobreza a través de una revisión de la literatura y la evidencia disponible. Se destacó la distancia existente en la literatura entre expectativa y evidencia en relación con el impacto que el acceso a Internet tiene en el crecimiento y, por consiguiente, en la reducción de la pobreza. Se identificaron, en particular, los canales microeconómicos que podrían explicar el impacto (si lo hubiera) y se realizó una revisión sistemática de la evidencia disponible en relación con los mismos. Específicamente, se buscó contrastar la hipótesis de dos tipos de efectos vinculados a la tecnología de Internet: un efecto sobre el crecimiento de la economía y un efecto distributivo de los ingresos. En relación con el primer efecto, se identificó un impacto positivo, aunque modesto e incierto en el caso de los países en desarrollo. En relación con los efectos distributivos, la evidencia encontrada resultó ambigua. Mientras que algunos estudios destacan un efecto que lleva a aumentar las desigualdades como resultado de sesgos en las habilidades de los trabajadores en los mercados laborales, otros destacan el efecto de integración de zonas geográficamente aisladas gracias al acceso a Internet.

Uno de los aportes realizados en Galperin y Viecens (2016; 2017) fue el de teorizar una serie de mecanismos microeconómicos a través de los cuales se canaliza el impacto de Internet, mismo que luego se refleja en los efectos de crecimiento y desigualdad. Las hipótesis se construyeron en función de la revisión de literatura y la evidencia disponible. Para el caso de efectos sobre el crecimiento se identificaron cuatro mecanismos: *i)* aumento de productividad de las firmas; *ii)* coordinación de los mercados (reducción de fallas de mercado: reducción de asimetrías de información, facilitación de *matchs*, etcétera); *iii)* fortalecimiento del capital humano y social (adquisición de habilidades TIC, redes sociales como facilitadoras de la inmigración, entre otros); *iv*) promoción de instituciones inclusivas (mayor transparencia gubernamental, mayor participación ciudadana, etcétera).

Desde hace ya algunos años, la inclusión financiera es una meta presente en el nivel global en un importante número de países en desarrollo.[2] Destaca particularmente el hecho de que las poblaciones más pobres representan un porcentaje desproporcionado entre los no bancarizados (Global Findex, 2017). Ante los desafíos que enfrenta Latinoamérica en este sentido, la mayoría de los países de la región han planteado Estrategias Nacionales de Inclusión Financiera (ENIF).[3]

En este trabajo se llevará a cabo una revisión de la literatura existente, con especial énfasis en aquella que proporciona análisis empírico para la región. Recientemente, ha surgido cierto optimismo en relación con el rol que las Fintech (abreviado de *Financial Technology*) pueden jugar en el abordaje de esta problemática.[4] Se buscará evidencia que dé soporte, o no, a este optimismo. Si las Fintech juegan un rol importante frente al desafío de la inclusión financiera, se habrá identificado un mecanismo microeconómico adicional de impacto del acceso a Internet sobre el desarrollo y la desigualdad, complementario con Galperin y Viecens (2016; 2017).

1 Véase Galperín, Mariscal y Viecens (2019) para una revisión de estos planes de banda ancha en América Latina.

2 Se entiende por inclusión financiera el acceso y uso de un conjunto de servicios financieros por parte de los adultos (Demirguc-Kunt, Klapper y Singer (2017). Para una discusión sobre definiciones de inclusión financiera, véase AFI (2017).

3 Véase Trivelli y Caballero (2018) para un análisis de las Estrategias Nacionales de Inclusión Financiera (ENIF) en 11 países de la región hasta 2018. En 2019, Argentina lanzó también su ENIF ((https://bit.ly/3KtCiXB).

4 Véase, por ejemplo (CAF, 2019).

El objetivo final de este capítulo es identificar instrumentos de éxito para promover la inclusión financiera.

La siguiente sección discute brevemente las principales conclusiones de la literatura sobre la relación entre pobreza e inclusión financiera. La sección tres analiza el éxito de un conjunto de políticas públicas enfocadas en promover la inclusión financiera, lo que permite elaborar un conjunto de lecciones aprendidas. La sección cuatro aborda la literatura con evidencia sobre el vínculo entre nuevas tecnologías e inclusión financiera. Allí se presentan los hechos estilizados que posicionan a las Fintech como actores relevantes en la discusión. La sección cinco concluye con un marco de herramientas de las que disponen los gobiernos para avanzar en inclusión financiera.

POBREZA Y LAS CONSECUENCIAS DE LA EXCLUSIÓN FINANCIERA

En el celebrado trabajo de Banerjee y Duflo (2007) sobre la vida económica de la gente en situación de extrema pobreza, los autores marcaron un hito en el análisis y la importancia de la relación entre pobreza y el acceso a servicios financieros. A partir de encuestas en hogares, llevadas a cabo en trece países, los autores destacaron ciertas observaciones sobre el acceso al crédito y el ahorro de las poblaciones de bajos recursos. En relación con el crédito, los autores mostraron que muy pocos pobres tienen créditos provenientes de un recurso formal de préstamos como bancos comerciales o cooperativas, más bien provienen de conocidos, amigos, familiares, prestamistas y comercios. Estos créditos provenientes de fuentes informales suelen ser muy caros, por los altos costos que conlleva el logro del cumplimiento de los contratos. En relación con el ahorro, los autores reportaron que un porcentaje muy bajo de pobres tiene cuentas de ahorro seguras y con rentabilidades razonables.

Recientes revisiones de la literatura sobre el impacto de la inclusión financiera en el desarrollo económico muestran resultados poco contundentes en relación con estas dos variables. Demirguc-Kunt, Klapper y Singer (2017), así como Martinez Pera y Shin (2020) coinciden en sus conclusiones. En cuanto al acceso al crédito, los autores documentan un fervor inicial en relación con el impacto positivo de los microcréditos en reducción de la pobreza, desarrollo humano y empoderamiento de las mujeres. Sin embargo, literatura posterior con pruebas controladas aleatorizadas muestra resultados menos optimistas, con efectos insignificantes, cuando no negativos. Esencialmente, las evaluaciones más recientes no encuentran mejoras en los indicadores socioeconómicos, ni un aumento en la creación de nuevas empresas, como resultado de un mayor acceso al crédito. En relación con el ahorro, la literatura muestra efectos positivos del acceso al ahorro formal. Tales efectos provendrían de la mayor seguridad que implica el ahorro en una cuenta que en el hogar, frente a riesgos de robos y mejor gestión de los gastos de las familias. Por su parte, las mediciones del impacto sobre el ahorro en sí mismo muestran algunos resultados contradictorios, ya que varios trabajos no encuentran impacto alguno.[5]

Complementariamente, tanto Demirguc-Kunt *et al.* (2017) como Martinez Pera y Shin (2020) documentan importantes efectos positivos en relación con el uso de pagos y transacciones digitales. Se identifican altos beneficios en presencia de largas distancias y cuando el valor de los pagos es alto; además de disminuciones de costos administrativos y de manipulación para usuarios, gobiernos y empresas. El uso de cuentas bancarias aumenta la seguridad, la transparencia y asegura que los beneficiarios reciban completas las transferencias de los gobiernos. Asimismo, el uso de cuentas bancarias y pagos digitales tiende también a reducir incidentes vinculados a criminalidad.

La importancia del uso de pagos y transacciones digitales ha sido contrastada con la experiencia que nos deja la pandemia de Covid-19. La necesidad de aislamiento social ha demostrado más que nunca la importancia de contar con una sociedad bancarizada y con acceso a medios de pagos digitales.[6] En particular, una de las debilidades con las que debieron enfrentarse algunos gobiernos de América Latina fue precisamente la alta tasa de uso de dinero

5 Demirguc-Kunt *et al.* (2017) reportan cierto potencial para los seguros, en particular en la agricultura.

6 Se observa un aumento importante en el uso de medios de pagos sin transacciones físicas y algunos de los nuevos actores reportan un crecimiento sin precedentes. Véase (Ámbito, 2020; *Perfil*, 2020).

físico para realizar transacciones.[7] Así, la posibilidad de hacer compras de manera sencilla y remota y acceder a servicios en línea resultó más valorada, cuando no indispensable. Por el lado de la oferta, la situación trajo desafíos y oportunidades para empresas y personas que pudieran ofrecer y vender servicios en línea. Nuevos productos y servicios surgieron como resultado de un despliegue de estrategias creativas, generado por la necesidad de que las familias se mantuvieran en sus hogares.[8] Pero este escenario de nuevas oportunidades ha estado restringido a personas y empresas que se encontraban digitalizadas, bancarizadas y con acceso a plataformas de pago digitales. En este sentido, la pandemia ha profundizado las consecuencias de asimetrías preexistentes.

Se deduce entonces, de manera estilizada, que el canal por el cual la inclusión financiera podría impactar de manera inmediata en el desarrollo y en la calidad de vida de las personas de bajos recursos, es el vinculado a la posibilidad de realizar y recibir pagos en formato digital. Esta posibilidad reduce distancias y riesgos de hechos criminales, así como también aumenta el tamaño de los mercados y la transparencia en la entrega de transferencias de los gobiernos a sus beneficiarios.

EVIDENCIA EMPÍRICA EN AMÉRICA LATINA: IMPACTO DE POLÍTICAS PÚBLICAS E INTERVENCIONES

En esta sección se revisan experiencias de políticas públicas desarrolladas en países de la región con el objetivo de avanzar en la inclusión financiera. Para esto se ha llevado a cabo una selección de trabajos que documentan algún tipo de evaluación de impacto.

7 En Argentina, largas filas de espera en las puertas de los bancos para el retiro de dinero de jubilaciones, o de subsidios a sectores desfavorecidos, se transformaron en pesadillas para adultos mayores y poblaciones de bajos recursos acostumbradas a utilizar dinero físico a la hora de realizar pagos (Infobae, 2020; *Clarín*, 2020a).

8 La pandemia puso en evidencia un potencial mundo virtual para una gran cantidad de productos básicos, así como para otros que generan nuevas experiencias atractivas en la situación de aislamiento (*Clarín*, 2020b).

El cuadro 1 resume los casos identificados. La primera columna de la misma presenta a los autores, la segunda indica el o los países donde se ha llevado a cabo la evaluación, con una breve descripción de la situación previa a la misma. La tercera explica el tratamiento aplicado y la cuarta muestra los resultados posteriores.

El cuadro muestra un conjunto de estudios que han evaluado el éxito o potencial de ciertas políticas públicas llevadas a cabo en países de la región. El común de estas intervenciones ha sido intentar comprender qué instrumentos funcionan o podrían funcionar a la hora de promover el uso de mecanismos de pagos distintos del efectivo y servicios financieros en poblaciones no acostumbradas a esto. Dupas, Karlan, Robinson y Ubfal (2018) concluyen que las cuentas bancarias tradicionales, aun subsidiadas, no son atractivas para las poblaciones no bancarizadas de tres países analizados (Chile, Malawi y Uganda). Sostienen, además, que en Malawi y Uganda el no uso de las cuentas se explica porque la población es de bajísimos recursos como para tener qué ahorrar y las cuentas bancarias no se adecuan a sus necesidades o hábitos. Por consiguiente, los autores argumentan que políticas públicas que implican sólo una apertura subsidiada de cuentas bancarias tienen pocas chances de ser efectiva.[9] En este sentido, Dupas *et al.* (2018) consideran que las cuentas de ahorro vinculadas a *mobile money* o *savings-led microfinance groups* resultarían productos más atractivos para poblaciones no bancarizadas. Estas conclusiones son consistentes con las de Castellanos, Jimenez Hernández, Mahajan y Seira (2018), quienes sostienen, luego del estudio llevado a cabo en México, que las grandes instituciones financieras formales carecen de eficacia para expandir el acceso al crédito.

En Argentina, Carballo y Bartolini (2019) llevaron a cabo una encuesta en un barrio de población vulnerable de la Ciudad de Buenos Aires, luego de que allí se implementara una estrategia por parte del gobierno de la ciudad para impulsar el uso de pagos digitales. Como parte del programa se entregaron terminales de pago a los comercios y se fomentó el uso de tarjetas con reintegros

9 Esta observación surge también en Maldonado y Moreno Sánchez (2018), quienes advierten que hay un salto importante entre la adquisición de un producto financiero y el uso del mismo.

CUADRO 01.

CONTINÚA

Autores	Países/Estado previo	Tratamiento	Resultados
Dupas, Karlan, Robinson y Ubfal (2018)	2010 Chile, Malawi, Uganda Hogares sin cuenta bancaria antes del tratamiento: Malawi: 85% Uganda: 77% Chile: 26%	En 2011 bajaron los costos para el acceso a una cuenta bancaria en colaboración con bancos. En Malawi y Uganda se eliminaron costos de apertura y mantenimiento por dos años y se dio asistencia para completar la documentación requerida para abrir una cuenta. En Chile se dio sólo la asistencia, ya que los bancos de la colaboración ya ofrecían cuentas sin costos.	2012-2013 Porcentaje de apertura de cuenta entre hogares del tratamiento Malawi: 69% Uganda: 54% Chile: 17% Porcentaje de uso de la cuenta (al menos cinco depósitos) Malawi: 10% Uganda: 17% Chile: 3%
Castellanos *et al.* (2018)	México	2007-2010 Experimento aleatorio a 162 000 clientes de "Banco A" para testear si tasas de interés más bajas con pagos mínimos más altos podrían mitigar el *default*.	1/3 de nuevos tomadores de préstamos entran en *default* o abandonan antes de los 26 meses (muestra de un millón de clientes de buró de crédito). Los cambios en la tasa de interés tienen efectos limitados en el nivel de *default*. Los cambios en los niveles de pagos mínimos no tienen impacto.
Carballo y Bartolini (2019)	Argentina Barrio Padre Mujica (ex Villa 31). Asentamiento urbano en la Ciudad Autónoma de Buenos Aires.	2018-2019 Entrevistas a 104 comerciantes del barrio luego de las medidas: - Se entregaron 62 terminales de pago electrónico - Apertura de cuentas bancarias gratuitas con la sola presentación de DNI - Talleres de educación financiera - Se colocó un cajero automático	2019 24% de los comercios acepta pagos digitales 87% tiene un smartphone. Se identifican motivaciones para aceptación y uso de pagos digitales: capacidades tecnológicas, seguridad (frente al alto nivel de siniestralidad en relación con el efectivo), expectativas de mejoras en el nivel de ventas.

CUADRO 01.

		- Sucursales de Banco Ciudad y BBVA (atendida por jóvenes estudiantes del barrio) - Reintegros de 50% para pagos con tarjeta del Banco Ciudad	
Mariscal y Rojas-Lozano (2020)	México En 2017 80% de los beneficiarios del programa Prospera (cerca de 7 millones de familias) recibía sus pagos en efectivo.	2017 se implementaron 3 intervenciones: 1) Encuesta aleatoria a 19 000 beneficiarios de Prospera en 34 localidades de los estados de México, Puebla, Chiapas y Yucatán. 2) En 28 localidades se implementaron medidas para acercar la información de los servicios que los beneficiarios tenían disponibles, en colaboración con Yastas, una red de comercios pequeños que comenzó a funcionar como agente de servicios bancarios. 3) Tres semanas antes del cambio de cobro en efectivo a cuenta bancaria, se enviaron mensajes sms a 2 870 mujeres a través de RapidPro (una plataforma de comunicación). Al grupo de tratamiento se le enviaron mensajes (tres o cuatro por semana) con: 1) recordatorio de las fechas de pago, 2) información y consejos sobre ahorro.	44% de los encuestados respondió que usaría una aplicación de pagos si le fuera ofrecida. Los beneficiarios de Prospera son clientes de Bansefi, pero pocos de ellos saben que disponen de una cuenta bancaria. Cierta preocupación por el funcionamiento de una solución de pagos móviles. Aumentaron las transacciones en Yastas y se triplicó la probabilidad de que beneficiarios de Prospera usen Yastas al menos una vez. Las mujeres respondieron proactivamente a los mensajes, dejando saber que desconocían la información de sus cuentas.

CUADRO 01.

Tejerina *et al.* (2014)	Honduras Los pagos del Programa Bono 10 000 se realizaban mediante entregas de efectivo en eventos masivos , convocados para una fecha y horario específico, lo que implicaba largas filas de espera para las beneficiarias.	En 2013 se implementaron pilotos con tres modalidades: 1) A través de telefonía móvil con el servicio Tigo Money: en un municipio, retiro total y parcial, beneficiario debe presentarse dentro de los 30 días. 2) Utilizando red de agencias de Banadesa (Banco Nacional de Desarrollo Agrícola): en ocho municipios, retiro total dentro de los seis u once días. 3) A través de la Red de la FACACH (Federación de Cooperativas de Ahorro y Crédito): en dos municipios, retiro total dentro de los siete días. Tigo Money resultó el mecanismo mejor valorado. Mientras que 91.89% dijo preferir este mecanismo al tradicional, en el caso de la red de la FACACH y las agencias Banadesa los respectivos porcentajes fueron 67% y 51%. 93% de las usuarias de Tigo Money considera que este método es más seguro que el tradicional. En el caso de las agencias del Banadesa y de las sucursales de la FACACH, los porcentajes respectivos fueron 52% y 74%.

FUENTE:
elaboración de la autora.

a las compras y descuentos en adquisiciones con la tarjeta del Banco Ciudad. De esta manera se facilitó el uso por parte de los comercios y se dieron incentivos por el lado de la demanda. Uno de los principales resultados de Carballo y Bartolini (2019) es que, si bien casi la totalidad de los comerciantes tiene y usa un teléfono móvil, es muy bajo el porcentaje de uso de los mismos para hacer operaciones financieras (7% utilizó una Billetera Digital, 5% cobró con un mPos y 2% cobró con códigos QR).[10] 62% informó sentirse "más o menos" o que "no se sentía seguro" para entender y utilizar la tecnología de su teléfono; dentro de este grupo, 19% incorporó pagos digitales en su comercio. Resulta llamativo que del restante 38% que "se sentía muy seguro" en el uso de la tecnología, sólo 31% había adoptado pagos digitales. Al respecto, Carballo y Bartolini (2019) señalan que una intervención pública para fomentar el uso de pagos digitales en comercios de barrios vulnerables deberá estar acompañada de educación financiera y de educación digital a fin de generar confianza en la utilización de la tecnología.

De acuerdo con los resultados que emergen de las revisiones de literatura mencionadas en la sección dos, de la encuesta de Carballo y Bartolini (2019) surge que 72% de los comercios que aceptan pagos digitales consideran que es más seguro que el efectivo. Entre los que no aceptan, 51% estaría interesado en aceptar y, de estos, 73% dijo que una de las razones sería mejorar la seguridad en su actividad económica. Nótese que 62% de los comerciantes encuestados había sufrido en los últimos tres años un siniestro delictivo en relación con el dinero en efectivo.

10 El código QR (Quick Response) es la evolución del código de barras y permite acceder de manera rápida a cierta información. Tiene un amplio abanico de funcionalidades. Una de ellas es que el código qr se integra con las billeteras electrónicas y se utiliza para realizar pagos presenciales con el teléfono móvil.

Mariscal y Rojas-Lozano (2020) y Tejerina *et al.* (2014) son proyectos piloto en el marco de los programas de transferencias condicionadas de dinero (CCT por sus siglas en inglés) en México y Honduras respectivamente.[11] Las CCT han sido estudiadas ya como mecanismos para acercar las primeras herramientas financieras a sectores vulnerables, dado que las CCT suelen conllevar la apertura de una cuenta bancaria y una tarjeta de débito a nombre del beneficiario. Maldonado y Moreno Sánchez (2018) señalan que los sistemas de pago utilizados en las CCT (tanto públicos como privados) no estarían funcionando como productos y servicios adecuados a las necesidades de las poblaciones receptoras de los mismos. Los autores señalan que el uso muy limitado en la región de cuentas bancarias podría estar explicado por limitaciones propias de las cuentas, como también por el desconocimiento, la autoexclusión y la desconfianza frente al sistema financiero de los beneficiarios de las CCT. Maldonado y Moreno Sánchez (2018) señalan que las cuentas de ahorro ofrecen mayores oportunidades para la inclusión financiera cuando se vinculan con aplicaciones de banca móvil.

Mariscal y Rojas-Lozano (2020) argumentan que Prospera, el que ha sido el programa CCT de México durante muchos años, se caracterizaba por una alta ineficiencia en la distribución del dinero a los beneficiarios, quienes debían recorrer largas distancias para recibirlo y quedaban expuestos a riesgos por la tenencia en efectivo. En ese contexto surgió Prospera Digital, para llegar a los beneficiarios a través de una plataforma de dinero móvil. Desafortunadamente la plataforma nunca llegó a implementarse, pero la experiencia descripta en el trabajo de Mariscal y Rojas-Lozano (2020) pone en relieve la importancia de dos aspectos en particular. En primer lugar, la pertinencia de incluir mecanismos de información adecuada y adaptada a las circunstancias de los beneficiarios de los programas. Las intervenciones pusieron en evidencia que los beneficiarios de Prospera desconocían que disponían de cuentas bancarias, el eslabón más básico de cualquier intención de inclusión financiera. En segundo lugar, el papel de Yastas, la red de comercios pequeños con alta capilaridad, que

[11] Las CCT son programas sociales a través de los cuales los gobiernos transfieren dinero a poblaciones desfavorecidas, condicionadas al cumplimiento de acciones vinculadas a educación o salud.

aparece como un agente de alta relevancia para el éxito en la implementación de los cambios. Ambos aspectos van de la mano con la impresión ya mencionada de que grandes agentes tradicionales no aparecen por sí solos como los más efectivos para llevar a cabo estrategias de inclusión financiera.

Las encuestas de Mariscal y Rojas-Lozano (2020), como las de Carballo y Bartolini (2019), señalan la manifiesta inseguridad de los usuarios frente al uso de la tecnología. Sin embargo, ambos trabajos destacan la altísima capilaridad de la telefonía móvil y su llegada a poblaciones vulnerables, inclusive a aquellas no bancarizadas, y que este hecho debe ser interpretado como una oportunidad para que la tecnología sea un canal de inclusión financiera.[12] Mariscal y Rojas-Lozano (2020) destacan también la importancia de incorporar al sector privado (bancos y Fintech) en el esquema de distribución digital de las CCT.

Tejerina *et al.* (2014) presentan también resultados tendientes a favorecer sistemas de *mobile money* para la distribución de las CCT, dado que el piloto con una empresa de telefonía móvil resultó mejor valorado que aquellos con otras dos grandes instituciones.[13] Asimismo, la mejora en seguridad que implicó recibir la CCT vía el servicio de la empresa móvil, fue también un elemento altamente valorado por las participantes en el piloto.

La revisión de casos llevada a cabo en esta sección permite inferir algunas lecciones de política pública:

- Los problemas de siniestralidad vinculados con el uso de efectivo que se vive en barrios y poblaciones vulnerables denotan la urgencia por promover la aceptación y el uso de pagos digitales.
- La mera puesta a disposición de cuentas bancarias no resulta como mecanismo efectivo de fomento al uso de servicios financieros.

[12] En Global Findex (2017) se sostiene que el acceso a Internet, junto con el uso de teléfonos móviles, podría ayudar a superar barreras que hoy encuentran algunas personas para acceder a servicios financieros. Véase también Aker *et al.* (2016).

[13] Aker *et al.* (2016) encuentran evidencia sobre beneficios de los sistemas de transferencias móviles (*m-transfer*) en Nigeria. En particular, aquellos hogares que recibieron la CCT vía transferencia móvil mejoraron la calidad y variedad de su dieta. Los resultados se explicarían, al menos en parte, por el ahorro en tiempo a la hora de recibir la transferencia.

- Grandes instituciones formales tradicionales podrían no ser los agentes mejor preparados para los desafíos que implica la inclusión financiera.
- La alta tasa de uso de teléfonos móviles en poblaciones no bancarizadas representa una oportunidad como puerta de entrada.
- La educación financiera y la digital aparecen como elementos complementarios, fundamentales en cualquier estrategia tendiente a fomentar el uso de pagos y servicios financieros digitales entre poblaciones vulnerables.

Cualquier estrategia de inclusión financiera debe ser diseñada con mecanismos que aseguren la llegada de la información adecuada y pertinente a las poblaciones objeto de la estrategia.

Debe ser evaluada la identificación e incorporación de agentes privados ya cercanos a las poblaciones objeto que ayuden a proporcionar la información necesaria y a generar confianza entre los nuevos usuarios de los servicios digitales.

EL ROL DE LA TECNOLOGÍA FINANCIERA FRENTE AL DESAFÍO DE LA INCLUSIÓN FINANCIERA

El sistema bancario ha dejado de ser una red de sucursales físicas para convertirse en un sector digitalizado, con alta tecnología de la información y uso de datos. Esta transformación ha supuesto el ingreso de nuevos actores, en particular, las Fintech, (acrónimo de *Financial Technology*) aquellas empresas que usan tecnología innovadora en servicios financieros.[14]

[14] La definición de la Cámara Argentina de Fintech es: "Las Fintech son empresas de origen digital cuya actividad principal es brindar servicios financieros mediante el uso de la tecnología", Cámara Argentina de Fintech (2018). El Financial Stability Board (FSB) define Fintech como "innovación financiera posibilitada por la tecnología que puede resultar en nuevos modelos de negocio, aplicaciones, procesos o productos con un efecto material asociado sobre los mercados e instituciones financieras y la provisión de servicios financieros" (traducción de la autora) ((https://bit.ly/3Cvuvpn).)

Aker y Mbiti (2010) es uno de los primeros estudios de impacto del uso de nuevas tecnologías financieras luego de que, desde 2005, aplicaciones de *m-money*, *m-banking* y *e-money* proliferaran en los países en desarrollo.[15] En particular, los autores analizaron el impacto de adopción de teléfonos móviles en África y cómo estos evolucionaron de ser un instrumento de comunicación a plataformas de provisión de servicios financieros. Tales plataformas comenzaron posibilitando algunos servicios sencillos como pagos de facturas, transferencias entre individuos y alguna posibilidad de cuenta de ahorro accesible desde el equipo móvil, lo que generó gran optimismo en torno de estos desarrollos.[16] Sin embargo, Aker y Mbiti (2010) encontraron para el caso M-Pesa en Kenya, que la población que usaba estos servicios estaba compuesta mayormente por personas de altos ingresos y nivel educativo, urbana y que ya estaba bancarizada.[17]

Indicadores recientes para Latinoamérica evidencian una situación similar presente en la región. De acuerdo con información en Andrade, Bagolle y Tejerina (2020), en Latinoamérica operan hoy más de 150 empresas que proveen servicios de pagos móviles y billeteras electrónicas, pero una gran parte de las mismas son de baja escala o están enfocadas en consumidores que ya están bancarizados o ya accedieron a tarjetas de débito (Andrade *et al.*, 2020). De acuerdo con datos del Global Findex (2017), sólo 7% de los adultos declaró poseer cuentas de dinero móvil, un porcentaje bajo si se compara con 24% de África subsahariana (Global Findex

[15] Estas son las maneras como se suelen denominar a las aplicaciones financieras a las que se accede y se usan con teléfonos móviles.

[16] Nótese que en 2009 el acceso a Internet estaba limitado al 4.2% de la población de África, por lo que el potencial del teléfono móvil como plataforma de servicios estaba restringido a aplicaciones que no requirieran acceso a Internet. Como remarcan Aker y Mbiti (2010), si bien estos sistemas de *m-money* representaron un valor importante para las comunidades de países en desarrollo por el abanico de opciones que se generó gracias a la posibilidad de hacer transferencias, no implicaron un potencial de bancarización de la población, ya que los mismos no ofrecían intereses al ahorro ni facilitaban el acceso al crédito de instituciones formales.

[17] M-Pesa es un servicio de *mobile money* en Kenya. Munyegera y Matsumoto (2016) encontraron resultados similares en Uganda.

2017).[18] Por consiguiente, la tecnología ha demostrado que puede ofrecer nuevos y mejores servicios, adaptados a las necesidades de los usuarios. Sin embargo, su uso es bajo en la región y se observa mayormente en un perfil de usuarios urbanos con niveles de ingresos y educativos medio-altos (Global Findex 2017). La revisión de los casos analizados en el cuadro 01 muestra esfuerzos por intentar comprender cuáles serían los canales más eficaces para conseguir que poblaciones vulnerables, de bajos ingresos y no urbanas comiencen a utilizar servicios de pago y financieros digitales.

Existe cierto optimismo con el rol que las Fintech pueden jugar en este sentido. Por ejemplo, BID (2018) señala que 46% de los emprendimientos Fintech encuestados para el reporte afirmaron desarrollar una estrategia dirigida a consumidores y pymes subbancarizadas o no bancarizadas. Además, BID (2018) observa que esto sucede primordialmente en aquellos países con mayores tasas de exclusión financiera.[19]

El análisis de la tabla 1 permite dar cuenta de un conjunto de hechos estilizados que dan soporte al optimismo sobre el potencial de las Fintech para llegar a poblaciones que no usan pagos digitales ni servicios financieros.

"Las Fintech nacieron como agentes y productos innovadores capaces de ofrecer servicios y experiencias diferentes a los consumidores". Una característica del modelo de negocios de las firmas digitales es que el mismo está basado en el cliente, en satisfacer sus necesidades y resolver sus problemas (Noya, 2019). En la sección anterior se identificó que la puesta a disposición de productos tradicionales como cuentas bancarias y tarjetas de débito no ha tenido el impacto esperado como mecanismo de inclusión financiera. La capacidad innovadora de las Fintech, con alto potencial para desarrollar productos de tipo *tailor made*, lleva a pensar que podrían ser los agentes adecuados para desarrollar propuestas de nicho específicas para las poblaciones foco de este estudio.

"Las Fintech podrían ser los agentes mejor preparados para operar de manera colaborativa con grandes instituciones". Del cuadro 01 se deduce que las grandes instituciones enfrentan dificultades para lograr por sí solas impulsar el uso de productos (como cuentas bancarias) que sí han puesto a disposición de poblaciones vulnerables. Además, si bien las Fintech brindan servicios independientes, muchas trabajan con elementos del sistema financiero tradicional, tales como la posesión de una cuenta bancaria y el historial crediticio. En este sentido, la colaboración entre Fintech y bancos resulta en beneficio de ambas partes (Cámara Argentina de Fintech, 2018). La colaboración podría derivar en el desarrollo conjunto de soluciones innovadoras con mejores servicios para los clientes. Estas sinergias han llevado al surgimiento del modelo de negocio de banca abierta (*open banking*), que permite a los bancos proveer servicios en asociación con proveedores digitales Fintech mediante aplicaciones. De hecho, este paradigma está en el corazón de la estrategia de complementación entre bancos y Fintech. Los bancos aportan sus ventajas (mayor capital, marca reconocida que brinda confianza a los consumidores, mayor conocimiento de las regulaciones) y retienen como *core business* su licencia bancaria, su base de clientes (CRM) y la actividad de *compliance* (Noya 2019).

"Las aplicaciones Fintech y los teléfonos móviles son complementarios en el uso". Varios de los autores citados en el cuadro 01 proponen el aprovechamiento de cuentas de ahorro vinculadas a *mobile money* así como también la distribución de CCT vía servicios de este tipo para avanzar en la inclusión financiera. Las Fintech nacen liderando aplicaciones de uso en los teléfonos móviles para pagos digitales como la billetera digital, el mPos y el pago con QR, del mismo modo que algunos servicios financieros con mayor nivel de complejidad. Por consiguiente, estas empresas ya están acostumbradas a ofrecer servicios diseñados para las comunicaciones móviles.

18 El segmento Fintech de pagos y remesas es el más importante en la región, registró 24% del total de soluciones en 2018 (BID, 2018).

19 Por ejemplo, El Salvador, Nicaragua y México, donde más del 50% de los emprendimientos Fintech dirigen sus servicios a segmento excluidos financieramente; menos del 40% de los adultos tiene acceso a una cuenta bancaria (BID, 2018).

HERRAMIENTAS DE POLÍTICA PÚBLICA Y CONCLUSIONES FINALES

La literatura que evalúa políticas públicas para promover la inclusión financiera es escasa en Latinoamérica.[20] En este trabajo se ha intentado identificar las lecciones que se deducen de un conjunto de intervenciones llevadas a cabo en países de la región.

Los resultados relevados muestran que los programas impulsados por los gobiernos para bancarizar poblaciones de bajos ingresos se enfrentan con importantes desafíos. Por ejemplo, los de la encuesta llevada a cabo por Carballo y Bartolini (2019) en un barrio vulnerable de la ciudad de Buenos Aires, luego de que el gobierno impulsara una batería de medidas en el barrio, son inicialmente desalentadores. Sin embargo, los mismos son útiles para identificar los elementos que actúan como barreras para que los comercios y compradores empiecen a usar medios de pagos digitales. En ese sentido, de la revisión de casos se dedujeron un conjunto de lecciones para el diseño de estrategias de inclusión financiera que promuevan el salto que lleve a más allá del acceso, al uso de las nuevas tecnologías.

La literatura señala que algunos productos financieros tradicionales no estarían siendo los adecuados para cubrir las necesidades de segmentos de la población alejados de la bancarización. En función del análisis llevado a cabo, se conformó un conjunto de hechos estilizados que sirven para argumentar que las Fintech presentan un alto potencial para cubrir la demanda no satisfecha, o para generar una demanda por parte de quienes hoy no muestran interés por la oferta existente. En este sentido, es fundamental que se satisfagan una serie de condiciones complementarias vinculadas al acceso a Internet y la disponibilidad de redes de conexión de buena calidad. Entonces, si las Fintech tienen un rol frente a la inclusión social, las nuevas tecnologías financieras son un mecanismo a través del cual el acceso a la banda ancha y a Internet implica crecimiento y menos desigualdad.

Finalmente, a continuación se explican cuatro herramientas de política económica de las que disponen los gobiernos para promover la inclusión financiera, en contexto con los elementos identificados en la revisión de casos del cuadro 01 y los hechos estilizados que favorecen la participación de las Fintech en programas de inclusión. La implementación de acciones en línea con estas recomendaciones permitiría asegurar una infraestructura de pagos electrónicos y digitales con acceso a toda la población, el primer escalón básico que hoy aparece como más urgente en la agenda de inclusión financiera. Establecer las bases en este sentido facilitará el abordaje de un segundo escalón de servicios financieros más avanzados por parte de poblaciones vulnerables.

[20] A diferencia de África para cuyos países se encuentra amplio material.

Promover la competencia que facilite la entrada de nuevos actores Fintech y eliminar barreras a la entrada y desarrollo de nuevos competidores.

Para que el potencial de las nuevas tecnologías financieras sea viable y pueda desplegarse, es necesario contar con un entorno competitivo y regulatorio que lo habilite y facilite. En este sentido, las posibilidades de expansión de los medios de pagos digitales y herramientas financieras no deberían estar limitadas por la existencia de barreras que condicionen la entrada de nuevos actores o el desarrollo de estos. Un elemento central a la hora de analizar el desarrollo de nuevos agentes como las Fintech es el hecho de que su ingreso al mercado y su expansión dependen en gran medida de la infraestructura de pago de los incumbentes para ofrecer servicios complementarios o diferenciados (Vives, 2019; OECD, 2020). Es decir, para poder desarrollarse, las Fintech podrían necesitar de la infraestructura de bancos incumbentes. Estas cuestiones, junto con la regulación y la innovación en el sector, son objeto de análisis y de debate en varios foros internacionales, en particular en la Organisation for Economic Cooperation and Development (OECD), que desde 2019 promueve un espacio de discusión titulado Digital disruption in financial markets. Greco y Viecens (2020) documentan y analizan medidas e intervenciones que han llevado a cabo las agencias de competencia de la región para disminuir barreras a la entrada al sector financiero; en muchos casos, motivadas por las demandas que impone la innovación tecnológica, por denuncias de jugadores entrantes o por investigaciones de mercado abiertas de

oficio. En particular, en los últimos años se observa una intensa actividad por parte de las agencias de competencia de América Latina en relación con el sector de medios de pago electrónicos y digitales. De los estudios e investigaciones relevados en los diferentes países de la región, surge un conjunto de potenciales barreras que las agencias han buscado eliminar.

En México, en octubre de 2018, la Autoridad Investigadora de la Comisión Federal de Competencia Económica (Cofece) inició una indagación en el mercado del sistema de pagos cuyo procesamiento involucra una cámara de compensación para pagos con tarjetas, con el fin de determinar la posible existencia de barreras a la competencia y libre concurrencia, o insumos esenciales que puedan generar efectos anticompetitivos.[21] Al respecto, Cofece señala que, de existir problemas de competencia en el mercado investigado, se estaría afectando la bancarización y la inclusión financiera. La investigación permanece en curso y está pendiente su resultado. México cuenta además con la Ley para Regular las Instituciones de Tecnología Financiera (Ley Fintech) que fue promulgada por el Senado de México, en marzo de 2018, con el fin de potenciar la competencia e innovación en el mercado de los servicios financieros. La ley incluye recomendaciones emitidas por la Cofece: *i)* el establecimiento de reglas para clarificar la propiedad y acceso a los datos; *ii)* garantizar la no discriminación por parte de instituciones financieras más grandes hacia las Fintech; y *iii)* eliminar la infraestructura restrictiva o tecnológica que impiden la entrada de participantes.[22]

[21] Extracto del acuerdo publicado en el Diario Oficial de la Federación (2018). Cofece destaca: "Se consideran barreras a la competencia cualquier característica estructural del mercado, así como cualquier hecho o acto de agentes económicos que tenga por objeto o efecto impedir el acceso de competidores, que limite su capacidad para competir o que distorsione el proceso de competencia. También las disposiciones jurídicas de cualquier orden de gobierno cuando indebidamente impidan o distorsionen dicho proceso" (Cofece, 2018).

[22] Véase la opinión por la que Cofece (2017) recibió un premio del Banco Mundial y la Red Internacional de Agencias. La distinción destacó que las recomendaciones emitidas por Cofece promovieron que una de las primeras leyes en el mundo sobre servicios de tecnología financiera facilite el ingreso efectivo al mercado financiero de nuevos competidores (Cofece, 2019).

Planes nacionales de banda ancha y programas para despliegue de redes de comunicaciones en zonas sin cobertura donde la inversión privada no llega.

Luego de la crisis de 2008, muchos gobiernos en todo el mundo desarrollaron importantes proyectos de despliegue de redes de banda ancha con la esperanza de promover la productividad y la innovación. En ese contexto, Galperin, Mariscal y Viecens (2013a; 2013b) analizaron los planes nacionales de banda ancha adoptados en cinco países de la región (Argentina, Brasil, Chile, Colombia y México). A excepción del caso chileno, todos los planes revisados en aquel momento contemplaban extensos despliegues de fibra óptica. En Galperin *et al.* (2013b) se destacaron también las diferencias entre los planes de la región con otros en países más desarrollados. Mientras que Europa, Estados Unidos y países como Australia, Singapur y Nueva Zelanda, estaban focalizados en la provisión de accesos de nueva generación (FTTH, Docsis 3.0), los planes de banda ancha de la región estaban destinados esencialmente al despliegue de redes troncales, con particular énfasis en dar cobertura a zonas no atendidas. Seguramente estos esfuerzos han implicado avances, pero queda aun camino por andar. Al respecto, Cave, Guerrero y Mariscal (2019) alertan sobre el acceso desigual a la banda ancha en México, lo que implica que los beneficios derivados del uso de Internet quedan limitados a los sectores de mayores ingresos. Los autores destacan que a largo plazo estas desigualdades serán un mecanismo de profundización de desigualdades sociales si los gobiernos no implementan medidas y políticas públicas para reducir brechas de acceso y uso de Internet. Un ejemplo de esto ha sido objeto de análisis en este trabajo, esto es el uso de efectivo en las poblaciones de bajos ingresos sin acceso a canales formales de bancarización y pagos digitales. Al mismo tiempo, la brecha digital que implica el solo uso de efectivo refuerza la brecha entre los hogares de bajos recursos y la economía formal (Carballo y Bartolini, 2019). En México, Cave *et al.* (2019) encuentran que casi 20 millones de personas viven en localidades sin cobertura de banda ancha móvil y destacan brechas digitales severas en servicios de banda ancha móvil en los estados más pobres. En particular, en Oaxaca, Chiapas y Guerrero la brecha puede llegar hasta 50% de sus habitantes.

Programas de transferencias condicionadas (CCT), articulados explícitamente con el objetivo de inclusión financiera.

Trivelli y Caballero (2019) destacan que los programas de transferencias condicionadas (CCT) han liderado un avance importante en el ingreso de los grupos tradicionalmente excluidos al sistema financiero formal en la última década, lo que evidencia el gran potencial de estos como parte de un programa integral de inclusión financiera. En este sentido, Maldonado y Moreno Sánchez (2018) señalan que los gobiernos deberían explicitar más efectivamente el objetivo de inclusión financiera en los programas CCT. Mariscal y Rojas-Lozano (2020) documentan ciertos esfuerzos llevados a cabo en México en el contexto de Prospera y Prospera Digital. Las lecciones destacadas por los autores son insumos valiosos para nuevos proyectos en México y otros países de la región.

Estrategias Nacionales de Inclusión Financiera (ENIF).

Las ENIF ayudan a conseguir consensos sobre la importancia de la inclusión financiera y colocan la problemática en la agenda política y de interés público (Trivelli y Caballero, 2018). Sin embargo, Trivelli y Caballero (2018) sostienen que las ENIF, al tener un método de trabajo más bien universal, fallan en el detalle y no consiguen atender a los sectores marginados. La falta de uso de servicios financieros que sí están disponibles y al alcance de estos sectores, aparece como el desafío más fuerte que limita el avance en materia de inclusión financiera. De esta manera, una intervención pública para fomentar, al menos el uso de pagos digitales, deberá estar acompañada de educación financiera y digital con el fin de generar confianza en la utilización de la tecnología y de los productos financieros. Las ENIF precisamente deberían funcionar entonces como un plan de articulación de la amplia cantidad de variables implicadas en el logro del objetivo que las motiva.

BIBLIOGRAFÍA

AFI (2017). *Defining Financial Inclusion*. Guideline Note N°28. Recuperado de https://bit.ly/3tsoHbZ

Aker, J., Boumnijel, R., McClelland, A. y Tierney, N. (2016). Payment mechanisms and antipoverty programs: Evidence from a mobile money cash transfer experiment in Niger. *Economic Development and Cultural Change, 65*(1), 1-37.

Aker, J. C. y Mbiti, I.M. (2010). Mobile Phones and Economic Development in Africa. *Journal of Economic Perspectives, 24*(3), 207-232. Recuperado de https://bit.ly/3KcTLDo

Ámbito (2020). "Se duplicó el uso de billeteras electrónicas como medio de pago por el aislamiento", 12 de abril. Recuperado de https://bit.ly/3tpDOD9

Andrade, G., Bagolle, A. y Tejerina, L. (2020). Los mecanismos de pago digitales. Una guía para los proyectos de protección social durante pandemias, BID. Recuperado de https://bit.ly/34by2fY

Banerjee, A. V. y Duflo, E. (2007). The Economic Lives of the Poor. *Journal of Economic Perspectives, 21*(1), 141-168. doi: 10.1257/jep.21.1.141

BID (2018). *Informe Fintech en América Latina 2018: crecimiento y consolidación*. Recuperado de https://bit.ly/35M7tOD.

CAF (2019). *Las fintech: clave para la inclusión financiera*. Recuperado de https://bit.ly/3sBLCm7

Cámara Argentina de Fintech (2018). *Informe Ecosistema Fintech Argentino*. Recuperado de https://bit.ly/3MfL2SR

Carballo, I.E. y Bartolini, M. (2019). *Pagos Digitales para la Inclusión Financiera de poblaciones vulnerables en Argentina: un estudio empírico en comerciantes del Barrio Padre Carlos Múgica (ex Villa 31-31 bis) de la Ciudad Autónoma de Buenos Aires*. Recuperado de https://bit.ly/3hAduAI

Castellanos, S., Jiménez Hernández, D., Mahajan, A. y Seira, E. (2018). *Financial Inclusion and Contract Terms: Experimental Evidence From Mexico*. NBER WP 24849. Recuperado de https://bit.ly/3MhMeoG

Cave, M., Guerrero, R. y Mariscal, E. (2019). *Cerrando la brecha digital en México: Una visión inside-out y outside-in de competencia y regulación*. CEEG. Recuperado de https://bit.ly/3sBMw1Z

Clarín (2020a). "Coronavirus en Argentina: largas colas en los bancos, que reabrieron para pagar jubilaciones y planes sociales", 3 de abril. Recuperado de https://bit.ly/35JM7S0

Clarín (2020b). "Venta de vino online y catas virtuales: cómo se reinventan las bodegas en cuarentena", 29 de abril. Recuperado de https://bit.ly/35PdUAQ

Cofece (2017). *Opinión a la Lay para Regular Fintech*. Recuperado de https://bit.ly/3hx1wYu

Cofece (2018). *Cofece investiga posibles barreras a la competencia y/o presencia de insumos esenciales en el sistema de pagos con tarjeta*. Recuperado de https://bit.ly/3tnOgLq

Cofece (2019). *Banco Mundial y Red Internacional de Competencia premian a Cofece por la opinión a la Ley para Regular Fintech*. Recuperado de https://bit.ly/3tocdlJ

Demirguc-Kunt, A., Klapper, L. y Singer, D. (2017). *Financial inclusion and inclusive growth. A review of recent empircal evidence*. Policy Research Working Paper 8040. World Bank Group. Recuperado de https://bit.ly/3hBbfNw

Diario Oficial de la Federación (2018). Extracto, 26 de octubre, p.1. Recuperado de https://bit.ly/3HwtBtK

Dupas, P., Karlan, D., Robinson, J. y Ubfal, D. (2018). Banking the Unbanked? Evidence from Three Countries. *American Economic Journal: Applied Economics, 10*(2), 257-297. doi: 10.1257/app.20160597

Galperin, H., Mariscal, J. y Viecens, M.F. (2013). *One Goal, Different Strategies: An Analysis of National Broadband Plans in Latin America. The journal of policy, regulation and strategy for telecommunications, information and media, 15*(3), 25-38.

Galperin, H. y Viecens, M.F. (2016). *Teoría y evidencia acerca de la relación entre Internet y reducción de la pobreza*. México D.F., México: CIDE press.

Galperin, H. y Viecens, M.F. (2017). Connected for development? Theory and evidence about the impact of Internet technologies on poverty alleviation, Development Policy Review.

Global Findex (2017). *Report The Global Findex Database 2017*, Chapter 6. Recuperado de https://bit.ly/3vPYWVV

Greco, E. y Viecens, M.F. (2020). Fintech y BigTech: barreras a la entrada y a la innovación. Estado de situación en América Latina. *Revista Latinoamericana de Economía y Sociedad Digital*, (1), 30-50.

Infobae (2020). "Después de dos horas de fila, algunos jubilados se descompensaron en las puertas de los bancos", 3 de abril. Recuperado de https://bit.ly/3ttQBVn

Maldonado, J.H. y Moreno Sánchez, R.P. (2018). Transferencias Monetarias Condicionadas, inclusión financiera en América Latina y el papel de Proyecto Capital. En Maldonado, J.H. (ed), *Proyecto Capital: diez años vinculando la inclusión financiera con la protección social* (62-120). Perú: Instituto de Estudios Peruanos. Recuperado de https://bit.ly/3C76mVS

Mariscal, J. y Rojas-Lozano, D. (2020). A State-led Model of Financial Inclusion Through Mobile Services. *Information Technologies & International Development,* (16), 20–31.

Martinez Peria, M.S. y Shin, M.Y. (2020). Financial Inclusion and Human Development. *Oxford Research Encyclopedia of Economics and Finance*. Recuperado de https://bit.ly/36ZvYsv

Munyegera, G.K. y Matsumoto, T. (2016). Mobile Money, Remittances, and Household Welfare: Panel Evidence from Rural Uganda. *World Development*, (79), 127-137.

Noya, E. (2019). The Fintech Revolution: Who Are The New Competitors In Banking? *Forbes*. Recuperado de https://bit.ly/3KeJOAq

OECD (2020). *Digital disruption in banking and its impact on competition*. Recuperado de https://bit.ly/3pwNw5w

Perfil (2020). "Las fintech de Argentina crecen en medio de la cuarentena", 23 de abril. Recuperado de https://bit.ly/3IFQfkC

Tejerina, L, P. Ibarrarán, F. Benedetti, Buchbinder. B., (2014). *En busca de eficiencia e inclusión financiera en el pago de transferencias de ingreso. Un estudio sobre la costo efectividad de los mecanismos de pago en el programa Bono 10,000 en Honduras*. Nota Tecnica IDB-TN-625. IDB Washington D.C. Recuperado de https://bit.ly/3vzElW2

Trivelli, C. y Caballero, E. (2018). ¿Cerrando brechas?: las estrategias nacionales de inclusión financiera en América Latina y el Caribe. Documento de Trabajo N°245, Instituto de Estudios Peruanos. Recuperado de https://bit.ly/3tpGSiD

Vives, X. (2019). *Digital Disruption in Banking*, OECD, background for Item 5 at the 131st Meeting of the Competition Committee on 5-7 June 2019. Recuperado de https://bit.ly/3IG9aM7

CAPÍTULO 12

LA INNOVACIÓN BASADA EN DATOS: HOJA DE RUTA PARA LOGRARLA

LINA ORNELAS NÚÑEZ*

* Google.

La imparable espiral de innovación que atestigua la humanidad se funda en desarrollos tecnológicos de distinta índole y cada vez más sofisticados. En las últimas décadas, las nuevas tecnologías basan gran parte de su operación y eficiencia en la utilización y análisis de grandes segmentos de datos (Data Driven Innovation). Lo anterior está posibilitando cada vez más la obtención de resultados y cambios exponenciales (no incrementales) con resultados benéficos para la atención y solución de los problemas más apremiantes de nuestro tiempo, tales como el impacto en el medio ambiente, la pobreza, la educación, el hambre, entre muchos otros. Ahora bien, como su condición de herramienta lo indica, la tecnología aplicada de manera indebida puede tener impactos negativos y de retroceso para el ejercicio de derechos y libertades.

Desde esta misma perspectiva, *la información por sí misma no engendra conocimiento o innovación, por más accesible y útil que sea.* Hace falta combinar los datos con las herramientas adecuadas para poder extraer análisis de tendencias, ideas, inferencias.

Los datos son la savia de la innovación. Es por eso que el acento a la hora de acercarnos a ellos debe estar puesto no tanto en su acumulación, sino en ¿qué podemos hacer con todos esos datos?, ¿cómo podemos ponerlos al servicio de los problemas de la comunidad y la vida de las personas? Los datos son como la luz, renovables y no rivales o no exclusivos. Usándolos bien y de manera anonimizada podemos impulsar la innovación a gran escala en todos los sectores de la economía y el avance científico.

En ese sentido, y dado que los datos son un elemento presente, tanto en lo público, como en lo privado, se abre una conversación que involucra a todos, iniciativa privada, sociedad civil, academia y gobierno.

Entre los actores mencionados, los gobiernos poseen un papel particular, ya que su participación puede presentarse desde dos planos, por una parte, podrían sumarse a la lista de los grandes beneficiarios de la innovación y, por ejemplo, hacer de la función pública un modelo de eficiencia, transparencia y rendición de cuentas y, por la otra, está llamado a constituirse en el catalizador de la transformación digital del Estado.

Un porcentaje importante del éxito para lograr que la innovación pueda permear con todo su potencial y con la mayor extensión posible en la sociedad, dependerá de la existencia de condiciones tecnológicas y culturales en torno al tema. Una plataforma óptima para generar esas circunstancias está en el diseño e instrumentación de políticas públicas orientadas a ese fin.

El desarrollo de este planteamiento se articulará a partir de tres ejes: la innovación en los sectores público y privado, la innovación y los datos personales, y la inteligencia artificial y los datos.

En el primero de los apartados, innovación en los sectores público y privado, se destaca la relevancia de contar con una regulación inteligente y la necesidad de que este principio de actuación se conciba como un tema por permear en el sector público. También se comparten una serie de reglas para promover la innovación entre entes públicos. Otro de los temas que se aborda es el relativo a los datos abiertos como factor fundamental para que la innovación prospere.

Después, en el segundo apartado, se hace un análisis derivado de la correlación entre innovación y datos personales. Al respecto, se hace una reflexión sobre la necesidad de lograr la mayor armonía entre la regulación en materia del procesamiento de datos personales e innovación, de modo que la protección de los datos no sea un límite u obstáculo para la innovación mediante desmedidas o injustificadas cargas regulatorias.

En el tercero de los apartados, inteligencia artificial y datos, se hace una breve reflexión sobre el poder de esta herramienta, la importancia de un uso ético, dado su inconmensurable potencial, así como su incalculable valor ante fenómenos globales, especialmente complejos, como la situación de emergencia sanitaria que se enfrenta.

LA INNOVACIÓN EN LOS SECTORES PÚBLICO Y PRIVADO

Los frutos de la sociedad de la información, hoy más que nunca, están a plena vista en cada dispositivo móvil en un bolsillo, en cada computadora portátil en una mochila, así como en cada plataforma tecnológica funcionando en las oficinas por todas partes. Medio siglo después de que el uso de computadoras personales se propagara entre la población, hasta el uso extendido del cómputo en la nube

para su almacenamiento y utilización de manera inmediata desde cualquier dispositivo y lugar del mundo, los datos no han parado de acumularse y, gracias a ello, está sucediendo algo nuevo y especial. El mundo se sumergió en un proceso de generación de información sin precedentes. El cambio de escala condujo a uno de estado: de lo cuantitativo a lo cualitativo (Mayer-Shönberger y Cukier, 2013: 6-7).[1]

Para dimensionar cuál es la capacidad de generación de datos, comparto una estadística muy ilustrativa: cada día se envían 500 millones de tuits, 294 mil millones de correos electrónicos, se crean 4 petabytes de datos en Facebook, 4 terabytes de datos a partir de cada auto conectado, 65 mil millones de mensajes se envían en WhatsApp, se realizan 5 mil millones de búsquedas y, para 2025, se contempla que se crearán 463 exabytes de datos cada día en todo el mundo, lo que equivale a 212.765.957 DVD por día (Desjardins, 2019).

Más que nunca, se han obtenido beneficios que transformaron la vida de las personas, gracias al uso de los datos. A lo largo de este artículo se describirán diversos ejemplos al respecto.

De algunas décadas a la fecha, se produjo un cambio de perspectiva con relación a la utilidad de los datos, se dejaron de contemplar como algo estático para convertirse, desde la perspectiva adecuada, en un manantial interminable de innovación y de nuevos servicios (Desjardins, 2019: 6).

La innovación es parte del ADN de muchas plataformas tecnológicas que nacieron en la capa superior de Internet.[2] Muchos

1 Consultado en versión electrónica.

2 Internet puede ser conceptualizado de manera sencilla como un conjunto de redes autónomas descentralizadas, que cooperan voluntariamente para implementar como un lenguaje común el Protocolo de Internet (IP) y subsecuentes protocolos y añadidos, de manera superpuesta a las infraestructuras físicas disímiles que conforman las redes de telecomunicaciones en capas inferiores; esto con el objeto de crear una sola red única, globalmente interconectada, que permite ofrecer innovaciones (como servicios digitales diversos) en capas superiores para sus conjuntos de usuarios a quienes dan acceso o conexión, y que se encuentran ubicados en los extremos de la red. Para mayor referencia véase el RFC 1935, RFC 1462, RFC 1958; Internet Invariants, y más reciente el documento The Internet Way of Networking.

de los denominados unicornios nacieron en pequeñas oficinas en las cocheras de casas (muchas ubicadas en Silicon Valley, en California) y en las que la intención de la compañía fue resolver problemas de una manera novedosa, dando vuelo y libertad a quienes forman parte de la empresa, para poner la creatividad al servicio de nuestros desafíos cotidianos.

A fin de cuentas, innovar no es otra cosa que resolver problemas, tradicionales o no, de forma novedosa. En ese sentido, un concepto relevante es el de *Smart Regulation* (regulación inteligente), el cual sostiene que la innovación y la experimentación con las nuevas tecnologías y modelos de negocio se debe permitir por defecto, sin someterla a permisos o autorizaciones previas, a menos que existan razones de peso para justificar una intervención, por ejemplo, para evitar daños a las personas.

Este modelo ha posibilitado el crecimiento del sector dedicado al desarrollo de nuevos servicios, contenidos, plataformas (como los mercados *online marketplaces*) y aplicaciones en Internet, que ha sido capaz de crear nuevos modelos de negocio y revolucionar la prestación de los ya existentes, y es el mejor escenario para innovar en cualquier circunstancia.

Lo primero que se necesita para poder innovar es enmarcar o identificar un problema o una causa. Y esto en muchos sentidos es coincidente con una de las misiones más relevantes del Estado, la del quehacer de la gestión pública: mejorar la vida de las personas.

El aparato gubernamental constantemente necesita reflexionar en torno a ¿qué falta por hacer o mejorar para lograr un Estado que fomente el bienestar de manera más amplia e inclusiva para los ciudadanos? A partir de la revolución tecnológica esa pregunta debería buscar una respuesta a través de la innovación y la tecnología.

La regulación inteligente no debe ser solamente un tema del ámbito privado; por el contrario, se deben impulsar modelos de experimentación en el sector público que den incentivos para innovar y transformar, y para esto se hace necesario flexibilizar las estructuras tradicionales del Estado y cambiar la cultura de la gestión pública.

3 Se define como una compañía tecnológica que alcanza un valor de mil millones de dólares en algún momento de su proceso de levantamiento de capital, sin cotizar en bolsa.

Es relevante mencionar que hay una diferencia básica entre los ámbitos de acción del sector privado *versus* el público, que deriva del marco normativo. En el ámbito privado, en una economía de mercado, un individuo puede realizar cualquier actividad socioeconómica, excepto aquellas expresamente prohibidas, mientras que en el público, un funcionario puede realizar única y exclusivamente aquello que está señalado por las leyes y reglamentos como parte de su función; y actuar fuera de este margen puede conllevar alguna responsabilidad administrativa.

Por ello, es necesario fomentar marcos normativos flexibles que permitan incluir la innovación como parte del actuar cotidiano del servicio público, dotando de atribuciones a las dependencias, entidades, y todo ente estatal, para que la innovación sea una parte "natural" de sus actividades.

Entre las acciones concretas para esta transformación se podrían crear áreas de innovación, donde, conforme a ciertos parámetros de actuación claramente establecidos, resulte factible el uso de recursos públicos para laboratorios de innovación y creación de soluciones *ad hoc,* transversales a todo ente público. Si bien es cierto que la innovación no se puede forzar, sí se puede crear un ambiente propicio para permitirla y fomentarla. Cada vez más muchos países intentan los denominados *sandboxes* regulatorios que proponen espacios de experimentación segura dentro de la regulación para fomentar la innovación. Un ejemplo claro es el de la Ley Fintech para Modelos Novedosos en México.

Por ello, comparto algunas reglas que considero de utilidad para promover la innovación. Se trata de una adaptación formulada teniendo en mente al sector público, a partir de las que se utilizan en distintas compañías digitales:

- Contratar siempre a la mejor gente: el talento cuesta, incluyendo el *expertise* técnico combinado con una voluntad de servir.
- Las ideas vienen de todas partes: un gobierno abierto incluye una cultura más horizontal y menos jerárquica. Se hace necesario romper la cultura de títulos y jerarquías, antesalas y puertas cerradas –que sólo son barreras para la comunicación y puntos de fricción– y fomentar la cultura de colaboración.

- Pensar cómo resolver algo de manera exponencial y no incremental también aprender a fallar rápido y barato: me refiero concretamente a marcos de experimentación e innovación que permitan al Estado repensar las formas de hacer gestión pública, que permitan al funcionario público atreverse a innovar, sin el temor de que con esto pueda contraer alguna responsabilidad, y reduciendo las fricciones que conlleva la burocracia tradicional. Enfocar las políticas de inversión en ciencia y tecnología para atacar directamente problemas de índole público a través de la tecnología: la academia, el gobierno y las empresas pueden ser aliados clave, como lo señala el modelo de colaboración de triple hélice.
- Usar datos, no opiniones: las decisiones deben basarse en datos con calidad y con la certeza de que son la base de la nueva economía digital, y el gobierno tiene un papel de facilitador y colaborador. Impulsar una política de datos abiertos, con una legislación y un marco normativo adecuado, que permita su reutilización e interoperabilidad para la toma de decisiones de todos los sectores con un marcado beneficio para el crecimiento acelerado de la economía digital.
- Enfocarse en los usuarios, no en la competencia: en mayor medida, el "usuario" de los servicios que presta el gobierno es el ciudadano, así como los propios funcionarios públicos, cuando acceden a sus plataformas. El enfoque debe estar en cómo mejorar los servicios que presta el Estado.
- Crear un ambiente en donde tu gente pueda brillar: al igual que repensar la cultura laboral del sector público, el ambiente de trabajo debe estar diseñado para permitir la colaboración y fomentar la innovación mediante el intercambio de ideas. Las oficinas deben ser espacios abiertos que inviten a la interacción.

LA IMPORTANCIA DE LOS DATOS ABIERTOS PARA LA INNOVACIÓN

Un factor determinante para lograr una exitosa implantación de la innovación en la actividad cotidiana tanto de organizaciones públicas, como privadas, lo encontramos en los datos abiertos. Ello, en el sentido de generar las condiciones necesarias para propiciar la innovación.

La Carta Internacional de Datos Abiertos (2015) los define como aquellos datos digitales que son puestos a disposición con las características técnicas y jurídicas necesarias para que puedan ser usados, reutilizados y redistribuidos libremente por cualquier persona, en cualquier momento y en cualquier lugar.[4]

De acuerdo con lo anterior, hago énfasis en que se trata de datos que pueden ser usados, reutilizados y redistribuidos libremente por cualquier persona. Debido a sus características técnicas, no existe limitante jurídica para su utilización, es decir, no se está en presencia de información de personas identificadas o identificables, ya que está debidamente anonimizada.

La citada carta establece seis principios: los datos deben ser abiertos por defecto, oportunos y exhaustivos, accesibles y utilizables, comparables e interoperables, para mejorar la gobernanza y la participación ciudadana, así como para el desarrollo incluyente y la innovación (Carta Internacional de Datos Abiertos, 2015).

El documento también reconoce la importancia de la apertura para estimular la creatividad y la innovación y que entre más gobiernos, ciudadanos, y organizaciones de la sociedad civil utilicen los datos abiertos, mayores serán los beneficios sociales y económicos que se generarán (Carta Internacional de Datos Abiertos, 2015).

También resaltaría de la mencionada carta la referencia de que el papel de los gobiernos para promover la innovación y el desarrollo sostenible no finaliza con la liberación de los datos abiertos, ya que deben desempeñar un papel activo en el apoyo para la reutilización eficaz e innovadora de los mismos, así como asegurar que los funcionarios de gobierno, los ciudadanos y las organizaciones de la sociedad civil tengan la información que necesitan, las herramientas y los recursos para comprender y utilizar esos datos de manera eficaz (Carta Internacional de Datos Abiertos, 2015).

Esto me permite abrir un corto paréntesis para destacar muy brevemente qué se ha hecho en distintos países, desde los gobiernos, para potenciar el uso de las tecnologías. De acuerdo con la Organización para la Cooperación y Desarrollo Económicos (OCDE; por sus siglas en inglés, OECD, 2015), los gobiernos que tengan como objetivo promover el suministro de tecnologías que permitan la "innovación basada en datos" (DDI por sus siglas en inglés) deberían considerar la posibilidad de también financiar inversiones en investigación y desarrollo (I&D) en tecnologías clave como: análisis de macrodatos, computación en la nube y de alto rendimiento e Internet de las cosas (IoT, por sus siglas en inglés), así como las de tecnologías que mejoran la seguridad y la privacidad.

Por ejemplo, Canadá ha financiado proyectos específicos por un valor de 15 millones de dólares canadienses durante tres años para respaldar la investigación de vanguardia y la comercialización de tecnologías cuánticas. Francia tiene la intención de invertir 150 millones de euros para apoyar la I&D en cinco tecnologías identificadas como estratégicas: IoT, supercomputación y computación en la nube, análisis de *big data* y seguridad. La Agenda Digital de Alemania 2014-2017 también prevé la promoción de la supercomputación, la seguridad y el análisis de *big data*, este último en particular a través de dos centros de competencia de *Big Data*. Y la Declaración de Japón para ser la nación de tecnología de información (TI) más avanzada del mundo, tiene como objetivo promover los desarrollos en el análisis de datos, así como en tecnologías relacionadas con sensores y robótica, entre otras (OECD, 2015).

En Reino Unido, la Estrategia de Economía de la Información, por ejemplo, tiene como objetivo promover el uso de las TIC en empresas y organizaciones, especialmente pymes, a través de una serie de actividades específicas que incluyen la sensibilización, un portal web con herramientas en línea y una red de asesoramiento digital, centros que ofrecen formación, tutoría y acceso a programas de cupones (OECD, 2015).

Otros ejemplos de países que han desarrollado agendas digitales novedosas y positivas son: Singapur, Suecia, Corea del Sur, Noruega, Holanda, Suiza. Destaca el caso de Estonia, este país comenzó a construir hace dos décadas la sociedad de la información que ahora la caracteriza. En esa época ni siquiera había una escala de recolección de datos como la hay ahora. La población no contaba con Internet ni dispositivos a través de los cuales acceder a él. El hecho de que esa nación hubiese invertido en soluciones de TIC

[4] La Carta de Datos Abiertos es una colaboración entre más de 100 gobiernos y organizaciones que trabajan para abrir datos basados en un conjunto compartido de principios.

desde aquellos años habla de un país con una visión muy futurista.[5] Otros ejemplos relevantes los tenemos con Colombia, que creó el Ministerio de Tecnologías de la Información y las Comunicaciones (Mintic), y Emiratos Árabes Unidos (EAU), que creó un Ministerio de Inteligencia Artificial como parte de una reestructuración de gabinete: "La próxima ola mundial es la inteligencia artificial y queremos ser el país mejor preparado para ello", escribió el primer ministro, Sheikh Mohammed bin Rashid Al Maktoum.

Finalmente, para cerrar el paréntesis en relación con el papel de los gobiernos y el potenciamiento en el uso de las tecnologías, los gobiernos deben promover el uso responsable de los datos personales para evitar violaciones de la privacidad. Deben considerarse más los esfuerzos para promover tecnologías que mejoren la privacidad y el empoderamiento de las personas a través de una mayor transparencia del procesamiento de información y la portabilidad de los datos a través de iniciativas como *midata* (Reino Unido) y *MesInfos* (Francia). Los gobiernos también deben aumentar la eficacia (es decir, la dotación de recursos y la experiencia técnica) de las autoridades encargadas de hacer cumplir la privacidad. La adopción de marcos de gestión de riesgos de privacidad requiere más estudios para comprender la mejor manera de apoyar los principios de protección de privacidad existentes (OECD, 2015).

Ahora bien, en lo que se refiere a la utilización de la innovación basada en datos, existen ejemplos tangibles, que dan cuenta de los impactos positivos que dicha innovación ha dejado a su paso. Esta ha sido de gran ayuda en espacios fundamentales de la vida de las personas, un buen ejemplo es la iniciativa Mejora Tu Escuela, plataforma colaborativa que publica información sobre el desempeño de las escuelas en México. La información que se pone a disposición está relacionada con aspectos como infraestructura, número de alumnos, desempeño académico, profesores, entre otros. ¿Qué papel desempeña esta plataforma en la comunidad escolar? Permite que madres y padres estén en posibilidades de decidir, con conocimiento de causa, la mejor escuela para sus hijos. Esta plataforma también permite formular inconformidades respecto de áreas de mejora. Sumado a lo anterior, esta herramienta se constituye en un valioso instrumento con el cual se fomenta la rendición de cuentas al facilitar el control por parte de la sociedad (Muente-Kunigami y Serale, 2018).

Otro caso donde la innovación basada en datos ha dejado un balance positivo[6] está en la plataforma Labora. Fue desarrollada por el gobierno mexicano: ofrece a emprendedores cívicos y sociales, herramientas innovadoras para el uso de datos, así como la posibilidad de vincularlos con el ecosistema mundial de empresas para el desarrollo de productos que tengan como modelo de negocio el uso de datos abiertos.

Gracias a esta iniciativa, el gobierno mexicano impulsó la creación de diversas bases de datos sectoriales (Muente-Kunigami y Serale, 2018: 37).

Aunque no es el objetivo de este artículo hacer una descripción del estado que guarda la política de datos abiertos en México, considero de utilidad señalar que el tema presenta buenos avances, por lo que sería muy valioso, no solamente mantener la ruta, sino seguir fortaleciendo el actuar el Estado y demás actores involucrados al respecto. Para mayor información pueden consultarse el Barómetro de Datos Abiertos, el Índice Global de Datos Abiertos, el Inventario de los Datos Abiertos y el Índice OURdata, de la Organización para la Cooperación y el Desarrollo Económico.

Más allá de México, también destacaría el proyecto Por Mi Barrio. Se trata de una plataforma para vecinas y vecinos en Uruguay, la cual permite formular reclamaciones respecto de fallas, desperfectos y problemas, en general, en la ciudad, y mantiene al tanto a las personas usuarias del proceso de reparación. Por Mi Barrio permite geolocalizar el problema, realizar la reclamación y hacerla llegar a la entidad responsable. Una herramienta como esta fortalece los vínculos entre el gobierno y las personas, un ejemplo óptimo sobre

5 The Estonian Information System Authority (RIA) es la autoridad en Estonia responsable de coordinar el desarrollo y la administración de sus sistemas de información, organiza actividades relacionadas con la seguridad de la información y maneja los incidentes de seguridad que han ocurrido en ese país. RIA también aconseja a otras entidades gubernamentales sobre cómo manejar sus sistemas de información y al mismo tiempo los monitorea

6 Las pymes que usan datos abiertos han sido capaces de generar entre quinientos mil y veinticinco millones de pesos anuales.

cómo la innovación facilita esta colaboración en beneficio del bien común (Muente-Kunigami y Serale, 2018: 44).

El motor de la nueva economía digital son los datos y la innovación gubernamental debe estar basada en estos. De hecho, el Estado es un actor muy relevante, porque es un generador de grandes bases de datos únicos: todos aquellos relativos a la interacción con el ciudadano que genera, procesa y almacena sobre distintos temas: seguridad, salud pública, impuestos, finanzas, requerimientos de los ciudadanos.

El Estado a través de la gestión pública, históricamente, ha sido el mayor experto en la acumulación estadística. Esta surge propiamente en el Estado, restringida en sus orígenes a la concentración de data pública. Se considera necesario que el Estado transforme su operación hacia adentro en la forma en la que administra sus recursos (información, personal, insumos, entre otros), y la forma en que hace política pública hacia afuera (políticas de impacto público), y en ambos esté en posibilidades de tomar decisiones basadas en datos, para los siguientes efectos:

- Profundizar la objetividad de la realidad que pintan los datos, y
- Reducir la subjetividad de la toma de decisiones basadas en opiniones.
- Tomar decisiones de mayor alcance, impacto y magnitud.
- Generar valor en la economía, en forma de nuevos productos y servicios innovadores.
- Mejorar la toma de decisiones socioeconómicas, por ejemplo, dónde establecer un negocio, dónde fijar una ruta de distribución, dónde vivir, entre otros.
- Sustentar la toma de decisiones en realidades y no en ideas.

Un cambio fundamental de paradigma en la economía digital es que el Estado ya no es el único generador de datos; la gran mayoría de actores privados también generan información y, por ende, la innovación se vuelve un camino de colaboración en dos vías.

Expuestas las consideraciones anteriores cabe preguntarse, ¿cuál sería el camino por seguir por los gobiernos para aprovechar la innovación basada en datos? Comparto algunas ideas para una hoja de ruta que permita innovar basándose en datos:

- Iniciar y/o concretar la transformación en su operación: al interior, por lo que refiere a la forma en la que se administran los recursos humanos, materiales y financieros, y al exterior, en la forma en la que se diseña e instaura una política pública.
- Consolidar el tránsito hacia un modelo de gestión de datos abiertos: una condición indispensable para la implantación exitosa de la innovación, en el actuar cotidiano, requiere de una política de datos abiertos, duradera, que ayude a apuntalar los cimientos de esta transformación.
- Alinear la visión: tener una visión clara de alcances y limitaciones para lograr un objetivo concreto, resolver un problema público específico o encontrar una solución particular a la gestión pública interna.
- Capacitar al servidor público: resulta fundamental dotar de habilidades digitales al propio personal para que explote a su máximo potencial la infraestructura tecnológica disponible, con la finalidad de que sepan cómo: exportar, integrar y mezclar datos propios con los de terceros, blindar los datos personales, utilizar las herramientas correctas para esas actividades, así como a concentrar cúmulos de bases de datos para su uso.
- Establecer metas logrables, cuyo éxito lleve a intentar otras más grandes: generar una cultura de gobierno que le da valor a los datos, los use para tomar decisiones y se regresen a la ciudadanía en forma de insumo para sus decisiones (sin procesar) y en forma de política pública (ya procesados).

INNOVACIÓN Y DATOS PERSONALES

Me gustaría detenerme unos instantes en la idea de innovación mediante un ejemplo concreto. Los primeros automóviles circulaban por la vía pública a una velocidad de entre 3 y 5 km/hora, porque en el siglo XIX, Gran Bretaña aprobó una ley, *Locomotives Highways Act*, que, entre otras cosas, requería que un hombre caminara delante de cualquier vehículo motorizado con una bandera roja por "seguridad" evitando accidentes al limitar la velocidad a la que podían circular los primeros automotores.

Más allá de lo pintoresco de la historia, lo importante es entender el papel tan relevante que han jugado los marcos regulatorios que moldean nuestra relación con la tecnología, los cuales deben promover la innovación y no interponerse a su paso, de modo que la misma pueda estar al servicio de las personas.

Esta innovación, ahora motorizada por los datos, puede ser perfectamente compatible con la privacidad, siempre y cuando se presenten los siguientes factores:

- Mecanismos de seguridad fuertes.
- Transparencia en el potencial uso de esa información.
- Control por parte del usuario.
- Portabilidad de datos.

A menudo se piensa que evitar la acumulación de datos protege de mejor manera la privacidad de las personas, sin embargo, el énfasis debiera ponerse en el uso adecuado o inadecuado que pueda hacerse de los mismos. Las prohibiciones a la recolección y la transferencia de datos impactan directamente en la innovación, cuando dichas limitaciones no están basadas en un análisis sobre su necesidad y proporcionalidad, a efecto de encontrar un equilibrio entre las mismas y la búsqueda de un ecosistema propicio para la innovación.

Y esta situación no afecta solamente a las grandes empresas de Internet, sino también a:

- Pequeñas y medianas empresas que optimizan sus costos y procesos con base en datos;
- Universidades y hospitales abocados a la investigación genética, el diagnóstico y la medicina personalizada, y
- A los usuarios y consumidores que pueden aprovechar los beneficios en costos y personalización de la economía global de la información.

La innovación basada en datos ha posibilitado el surgimiento de nuevas tecnologías con las que hoy por hoy convivimos cotidianamente:

- *Cloud Computing*;
- Internet de los objetos, e
- Inteligencia artificial y *Machine Learning*, entre otras.

Especialmente ante estas nuevas tecnologías, todos los Estados enfrentan un dilema al momento de decidir qué tipo de regulación buscan en materia de privacidad y protección de datos personales.

México cuenta con un amplio marco normativo en materia de protección de datos. Desde la *Constitución Política de los Estados Unidos Mexicanos* se prevé la protección de datos personales en los artículos 6 y 16. Asimismo, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, su Reglamento, y la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, fijan las bases para el ejercicio de este derecho. Finalmente, es importante destacar que el Tratado México-Estados Unidos-Canadá (T-MEC), el cual entró en vigor el 1 de julio del presente año, incluye diversas disposiciones en materia de libre flujo de datos al tiempo que establece protecciones a la privacidad.

En ese sentido, si bien es verdad que la protección de datos personales constituye el núcleo del comercio digital, es necesario considerar que las regulaciones que emiten los Estados con la finalidad de proteger la privacidad tienen también un impacto directo en la inversión extranjera. Así, es muy relevante entender que la privacidad no es solamente un concepto abstracto que pretende proteger a los individuos, también es un elemento muy importante que debe ser tomado en cuenta por las empresas al momento de decidir si establecen sus oficinas en un país u otro.

La protección de datos no es incompatible con la innovación, y hemos visto que la evolución alrededor del concepto *dato* conlleva a un menor énfasis en limitar la adquisición y más en el uso y seguridad.

Así, me parece que cuando se analiza una regulación en la materia, que equilibre la protección de datos con el fomento de la innovación en un entorno tecnológico, debe considerarse lo siguiente:

- Practicidad (consentimiento informado, *opt-out*, interés legítimo).
- Enfocarse en el uso que pueda darse al dato y al daño que pueda causarse, más que en categorías *a priori*.
- Enfocarse en prevenir el mal uso o uso discriminatorio de datos, más que en la naturaleza del dato en sí mismo.
- No reinventemos la rueda: muchos de los retos en privacidad para el desarrollo tecnológico son extensiones de los existentes. Los controles y regulaciones existentes se aplican a la tecnología.

- Hacer énfasis en la adecuada anonimización de los datos, a efecto de que su tratamiento no imponga riesgos innecesarios a la privacidad.
- Beneficio del uso de los datos –en muchos casos anonimizados– para poner información a disposición del público (*open data*).
- No tendría sentido crear legislación específica para cada desarrollo tecnológico, ya que está comprendida en la legislación general sobre privacidad y seguridad, así como en los esquemas de mejores prácticas de la industria.
- La regulación fragmentada frenaría la innovación y el desarrollo de esta industria.

Las *startups* generalmente no cuentan con los recursos económicos y materiales necesarios para satisfacer requerimientos legales que les impone una regulación estricta en materia de protección de datos personales de manera especial, cuando dichos requerimientos pueden ser administrativamente engorrosos y no incidir de forma clara en una efectiva protección adicional del individuo. En virtud de lo anterior, los Estados que emiten una regulación estricta en la materia, inhiben la inversión, pues la *startup* probablemente buscará establecerse en un territorio con normas menos rigurosas.

Claro ejemplo de altos estándares regulatorios que han probado no ser precisamente útiles para proteger a la persona titular de los datos, lo encontramos en la obligación de registrar las bases de datos ante las autoridades de protección: esto ha provocado que las empresas emigren a otros territorios con reglamentaciones que si bien sigan protegiendo al individuo, no establezcan requerimientos difíciles y costosos de cumplir. Otro ejemplo es la obligación de obtener la autorización de las autoridades de un determinado país para poder realizar transferencias de datos *versus* la posibilidad de realizar dicha transferencia de manera segura a través de cláusulas contractuales.

La protección de datos personales es un elemento muy importante en la oferta de servicios de las empresas y constituye una parte fundamental de su propia marca. Considero que las leyes que permiten el libre flujo de datos, incluyendo las transferencias internacionales de los mismos, con una revisión *ex post* por parte de la autoridad, constituyen un mejor modelo que, precisamente, sí contribuye a la protección de los datos de la persona, pero sin restringir el libre flujo de datos y, por lo tanto, la movilidad y crecimiento económico.

En ese sentido, es recomendable que las leyes promuevan los modelos de autorregulación con verificaciones *ex post* por parte de la autoridad. De esta manera, los datos pueden circular libremente al menos que la autoridad identifique requisitos que no se están cumpliendo. Los altos estándares de protección de datos deben reservarse únicamente para aquellas situaciones en las que media el interés público.

Entonces, ¿qué necesitamos saber al momento de diseñar un marco regulatorio que cuide la privacidad de los usuarios a la vez que promueva la innovación dentro de un ecosistema digital?

- Debe analizarse primero si en un caso concreto es necesaria nueva regulación en materia de protección de datos, o bien, si el reto consiste en la aplicación de las normativas existentes en nuevos contextos.
- Los principios de protección de datos siguen siendo vigentes. Sigue existiendo el principio de proporcionalidad aplicado siempre a una finalidad determinada (si para una finalidad, en efecto, se requieren muchos datos, eso será proporcional) *versus* la idea de minimización.
- El énfasis debe ponerse en el usuario-titular del dato y en análisis basado en riesgos, buscando dotarlo de las herramientas para tener control y acceso a mecanismos que transparenten el tratamiento de datos. Logrado esto, la privacidad no será una barrera encubierta para la innovación y el desarrollo de las grandes ideas.

LA INTELIGENCIA ARTIFICIAL Y LOS DATOS

Me gustaría detenerme un momento en el concepto y aplicación de la inteligencia artificial (IA). Se trata de una programación computacional que aprende y se adapta, cuyo potencial para mejorar nuestras vidas es profundo.

Actualmente los esfuerzos en IA se encuentran agrupados en tres grandes rubros:

a) IA para clasificar y filtrar:

i Transcribir contenidos históricos escritos a mano a texto digital.
ii Detección temprana de diabetes rinopática.
iii Aplicaciones de propiedad marcaria más rápidas y eficientes.

b) IA para proveer monitoreo y predicciones en tiempo real:

i Creación de mapeo en tiempo real de barcos pesqueros para detectar áreas con riesgo de sobrepesca.
II Predecir demanda y automatizar el resurtido para optimizar inventarios.
iii Automatizar el control de enfriado de los centros de datos para reducir consumo de energía.
IV Alertar comunidades locales de tala ilegal, con teléfonos reciclados como sensores.

c) IA para apoyar la creación de algo nuevo:

I Traducción en tiempo real de texto dentro de imágenes en la aplicación *Translate*.
II Acelerar el descubrimiento de nuevas medicinas analizando más profundamente datos biomédicos.
III Analizar nivel de habilidades lingüísticas en inglés y entregar un curso específico de aprendizaje personalizado.

Ahora bien, debe reconocerse que una tecnología tan poderosa, plantea preguntas igualmente poderosas sobre su uso. La manera en que se desarrolle y use la IA tendrá un impacto significativo en la sociedad por muchos años más. Es por eso que la industria debe guiarse por principios éticos en el uso de esta tecnología, los cuales no deben ser conceptos teóricos, sino estándares concretos que gobiernen de manera activa la investigación y desarrollo de productos e influyan en las decisiones de negocio.

De acuerdo con el Código de Ética y Conducta Profesional de la Association for Computer Machinery,[7] los principios éticos generales son los siguientes:

1 Contribuir a la sociedad y al bienestar humano, reconociendo que todas las personas son partes interesadas en la informática;

2 Evitar el daño;
3 Ser honesto y confiable;
4 Ser justo y tomar medidas para no discriminar;
5 Respetar el trabajo necesario para producir nuevas ideas, inventos, trabajos creativos y artefactos informáticos;
6 Respetar la privacidad, y
7 Respetar la confidencialidad.

EL USO DE DATOS PARA EL BIEN COMÚN EN EL CONTEXTO DE COVID-19

En efecto, el uso de datos para el bien social debería ser una práctica predeterminada para todo el ecosistema de Internet bajo su modelo de gobernanza. Las administraciones y las empresas, el mundo académico, y demás actores que estaban más avanzados en el uso de datos abiertos y su análisis para crear soluciones tecnológicas innovadoras en general, están lidiando mejor con la pandemia.

Usar los datos de manera adecuada puede ayudar a gobiernos e instituciones a ser más eficientes y tener escalabilidad para resolver los problemas más apremiantes que enfrenta la humanidad.

Los datos siempre juegan un papel fundamental en la capacidad de investigar, estudiar y combatir las emergencias de salud pública, sobre todo cuando se trata de enfrentar con rapidez una crisis mundial. El acceso a conjuntos de datos y herramientas que pueden analizarlos a escala, son cada vez más esenciales para el proceso de investigación y son particularmente necesarios en la respuesta global al Covid-19.

Cuando una empresa recaba datos personales, tiene la responsabilidad de protegerlos, pero también de utilizarlos en beneficio de sus usuarios.

[7] El código está diseñado para inspirar y guiar la conducta ética de todos los profesionales de la informática, incluyendo a los profesionales actuales y futuros, a los instructores, los estudiantes, las personas influyentes y a cualquiera que utilice la tecnología informática para generar un impacto. Además, el código sirve como una base para corregir posibles infracciones, incluye principios formulados como declaraciones de responsabilidad, basados en la idea de que el bien público siempre es la primera prioridad. Se trata de una asociación con más de cien mil miembros por todo el mundo. El equipo que aprobó la versión definitiva del código estuvo integrado por representantes de la industria, por representantes de asociaciones de profesionales y por profesionales independientes. Association for Computer Machinery. Recuperado de: https://bit.ly/3sMoTUF

Ejemplo: la gripe AH1N1 de 2009 dio origen a Google Trends. Los ingenieros empezaron a darse cuenta de que la Búsqueda de Google recibía consultas sobre "síntomas de la gripe" procedentes de ubicaciones y geografías muy específicas. Con esa información, se logró identificar a grupos de conjuntos de datos anonimizados que mostraban esas consultas anónimas en ubicaciones específicas y descubrieron que eso podría estar relacionado con brotes geográficos específicos de la pandemia, por lo que Google comenzó a alertar a las autoridades para que prestaran especial atención a esas zonas. A partir de esa experiencia, la empresa decidió construir un visualizador público poderoso de conjuntos anónimos de consultas de búsqueda en sus sistemas que pudiera dar una idea de las realidades de los usuarios y lo que estaban interesados en buscar: lo que le interesa a la gente, eventos relevantes que suceden en sus ciudades y países (¡como un brote de AH1N1!).[8]

En un sentido similar, Apple, lanzó una herramienta que genera tendencias de datos de movilidad en la aplicación Mapas de Apple, como parte de sus acciones en apoyo a las tareas en todo el mundo para paliar la propagación del Covid-19. La intención es que los datos de movilidad sean útiles para los gobiernos, especialmente para sus autoridades sanitarias y que sirvan de base para el diseño de políticas públicas. La aplicación no asocia datos de movilidad con el Apple ID de los usuarios, esto es, se trata de una recopilación de datos agregados que muestra las tendencias de movilidad en las principales ciudades y en 63 países o regiones (Apple, 2020).

Asimismo, Google desarrolló un producto llamado Informes de Movilidad Comunitaria para apoyar a las autoridades sanitarias mediante métricas que ilustran la eficacia del distanciamiento social. Estos informes utilizan datos agregados y *anonimizados* para trazar las tendencias de movimiento a lo largo del tiempo, por geografía, así como por categorías (como lugares de trabajo, tiendas, recreación, supermercados, farmacias, parques y residencias).[9]

8 Véanse otros ejemplos del uso de IA para el bien común en https://ai.google/social-good/, y recomendaciones para su regulación en https://bit.ly/3sJJc4T

9 Recuperado de https://bit.ly/3vHrJMz

Otro caso relevante es el lanzamiento de las interfaces de programación de aplicaciones (API, por sus siglas en inglés) de notificación de exposición a casos positivos de Covid-19 llamadas Exposure Notification (EN) y Exposure Notification.

Express (ENX)[10] realizadas en conjunto por Google y Apple. EN y ENX permiten a un usuario conocer de manera *anonimizada* si ha estado expuesto a personas infectadas de Covid-19. Las API están diseñadas para ser desarrolladas en aplicaciones oficiales de gobiernos o ministerios de salud, y permiten a un usuario informar de manera voluntaria y sin requerir datos personales, que ha resultado positivo a Covid-19. El mecanismo de funcionamiento es a través de llaves de seguridad aleatorias generadas por los dispositivos con la aplicación oficial (que ya instauró alguna versión de la API), mismas que se intercambian a través de proximidad con otros dispositivos con la aplicación instalada a través de tecnología *bluetooth*; para luego ser verificadas con una lista de llaves infectadas cada cierto intervalo de tiempo, lo que le permitirá al usuario del dispositivo recibir una notificación de que ha estado expuesto a otro dispositivo empleado por un usuario contagiado. Este uso de tecnología es sumamente relevante dado que, considerando la privacidad del usuario y únicamente utilizando llaves de criptografía, se permite a las personas estar alertas de si han estado expuestos a un posible contagio, recibir instrucciones de su autoridad local sobre qué hacer en ese caso, y de esta manera reducir ulteriores comportamientos que llevan a posibles contagios subsecuentes. Lo anterior, se convierte en la base para determinar el confinamiento, únicamente de personas expuestas y no de toda la población, permitiendo la reactivación económica, ya que se pueden elaborar aplicaciones ligeras para el acceso de empleados a centros de trabajo de manera segura, por mencionar algunos. Esta tecnología que se renueva y mejora constantemente (por ejemplo al día de hoy se está explorando introducir elementos de *roaming* y permitir cruces transfronterizos seguros), ya se ha instrumentado en países como Turquía, Indonesia, Japón, Filipinas, Alemania, Uruguay y Panamá y en varios estados de la Unión Americana, como Nueva York, California, Utah, Nuevo México, Hawaii, entre otros.

10 Más información en: https://bit.ly/3lHdMlg

Estos tres casos, entre otros tantos, dan cuenta de los esfuerzos de la industria tecnológica por sumarse a las organizaciones internacionales y los gobiernos para integrar un frente común que contribuya a superar de la mejor forma posible esta crisis generada por el brote de Covid-19.

Definitivamente, vemos el papel de los usos positivos y responsables de los datos, como la respuesta a Covid-19, que subraya la importancia de un marco regulatorio flexible y basado en el riesgo, que establece reglas claras para las empresas y permite a las autoridades de protección de datos ofrecer una guía procesable y ayudar a los usuarios a sentirse protegidos.

Para instaurar una política pública de salud y luego lineamientos de recuperación económica, las autoridades deben ser precisas y tener escala, utilizando la información disponible y precisa.

Además del control individual por parte del titular del dato, las empresas y organizaciones también deben asumir la responsabilidad de utilizar los datos de una manera que proporcione valor a las personas y la sociedad, y minimice los riesgos para los usuarios en función del uso de la información personal. Esto significa considerar los intereses de las personas, evaluar el impacto del uso de datos en esos intereses e implementar salvaguardas para protegerlas.

Considero que debemos pensar muy a fondo en la configuración de la nueva normativa de protección de datos para este milenio de forma equilibrada, pero creativa, entre otros, fomentar procesos/técnicas tanto en el sector público, como en el privado, que promuevan las técnicas para preservar la privacidad en uso de grandes datos, tales como *blurring*, privacidad diferencial, FLoC (Federated Learning of Cohorts), y también promover y poner foco en excepciones regulatorias de interés público, incluyendo su significado y límites.

Por último, con la firma del T-MEC sería importante crear un frente común entre estos tres países, para fomentar una política armonizada de datos abiertos compartiendo información agregada, de una manera que permita mantener un equilibrio entre la privacidad y el interés público. Contar con un Open Data Hub entre los tres países permitirá eficientar las cadenas de valor, así como hacer frente a otras regiones como Asia, que se han adelantado a llevar a cabo la explotación de datos de toda índole, no siempre respetando

derechos fundamentales. De hecho, el artículo 19.18 del T-MEC prevé disposiciones de datos abiertos gubernamentales:

Artículo 19.18: Datos Abiertos Gubernamentales

1. Las Partes reconocen que facilitar el acceso público y el uso de información gubernamental fomenta el desarrollo económico y social, la competitividad y la innovación.
2. En la medida en que una Parte decida poner a disposición del público la información del gobierno, incluidos los datos, esta procurará asegurar que la información está en un formato legible por máquina y abierto, y puede ser buscada, recuperada, utilizada, reutilizada y redistribuida.
3. Las Partes procurarán cooperar para identificar las formas en que cada Parte puede ampliar el acceso a y el uso de la información gubernamental, incluidos los datos, que la Parte haya hecho pública, con el fin de mejorar y generar oportunidades comerciales, especialmente para pymes.

CONCLUSIONES

Innovación y gobiernos

Los gobiernos deben basar sus decisiones en el análisis de datos, para eficientar su respuesta al ciudadano, eliminar ineficiencias y, por ende, ahorrar una gran cantidad de recursos y presupuesto público que pudiera ser empleado de mejor manera. En esta tarea debieran instaurar esquemas público-privados para avanzar de manera exponencial y no incremental en el logro de sus metas y objetivos. Asimismo, los gobiernos deben promover el suministro de tecnologías que permitan la innovación basada en datos y considerar la posibilidad de financiar inversiones en investigación y desarrollo en tecnologías clave como análisis de macrodatos, cómputo en la nube, Internet de las cosas, así como en tecnologías que mejoran la seguridad y la privacidad.

Usuarios y personalización de productos y servicios

En el tratamiento de datos personales, además del control individual por parte del titular del dato, las empresas y organizaciones también deben asumir la responsabilidad de utilizar los datos de

una manera transparente y que proporcione valor a las personas y a la sociedad al minimizar los riesgos para los usuarios en función del uso de la información personal. Esto significa considerar los intereses de las personas, evaluar el impacto del uso de datos en esos intereses e instrumentar salvaguardas para proteger a las personas.

Responsabilidad demostrada

Un mecanismo idóneo para minimizar los riesgos para los usuarios en función del impacto que la utilización de sus datos puede conllevar, es el principio de responsabilidad demostrada, ya que provee las herramientas específicas para este fin. Las evaluaciones de impacto a la privacidad y los esquemas de privacidad desde el diseño y por defecto, son dos de los instrumentos idóneos para blindar, de forma preventiva, los datos de los usuarios y de ese modo mitigar posibles riesgos a sus derechos ante su utilización. Otra virtud de este principio es ser un mecanismo de rendición de cuentas para los usuarios, de modo que a través del mismo se da cuenta, transparentemente, del uso de su información.

Datos abiertos e innovación

Un factor determinante para lograr una exitosa implantación de la innovación, tanto de organizaciones públicas, como privadas, pasa por una política transversal de datos abiertos, teniendo en cuenta que la información es el eje sobre el que se erigirá cualquier proceso de investigación y desarrollo. Fundamentalmente, contribuye a la generación de las condiciones necesarias para propiciar la innovación.

Usuarios y alfabetización digital

Para que haya innovación digital basada en datos, resulta fundamental involucrar a todos los actores presentes en este diálogo y uno de estos son los usuarios, de hecho, el diálogo resulta imposible sin ellos. Por esa razón, es indispensable propiciar que estos posean las habilidades digitales suficientes para explotar la tecnología disponible. Sin ellos perdería su razón de ser todo esfuerzo vinculado a la innovación. El objetivo es poner a la disposición de la sociedad los beneficios producto de la innovación basada en datos.

Transferencias internacionales de datos e innovación

Las restricciones territoriales, las decisiones de adecuación o la localización forzada de datos, deben ser concebidas como una excepción y no la regla. No debe perderse de vista que las prohibiciones para transferir datos impactan directamente sobre la innovación, por lo que los modelos de transferencias internacionales, configurados para una revisión *ex post* por parte de la autoridad, resultan más equilibrados, en tanto que contribuyen a la protección de los datos personales sin restringir su libre flujo y, con ello, la movilidad y crecimiento económico.

Autorregulación y cumplimiento para la protección de datos personales

El vehículo a través del cual se podría dar cumplimiento, para efectos de transferencias internacionales de datos, son los modelos de autorregulación reconocidos internacionalmente como las normas corporativas vinculantes, por ejemplo, el modelo de Reglas Transfronterizas de Privacidad (Cross-Border Privacy Rules, CBPR system) del Foro de Cooperación Económica Asia-Pacífico (APEC). Debido a su diseño, resultan fácilmente adaptables y atendibles, lo que además redunda en reducción de costos. Estos modelos bien instrumentados, hacen más competitivos a los países, ya que permiten la inversión en sectores clave de manera transnacional.

Modelo de habilitación para el uso de datos personales

Las causas legitimadoras del tratamiento de datos personales se han flexibilizado y el consentimiento dejó de ser la causa habilitadora por excelencia. Hoy es posible encontrar un conjunto de causas habilitantes que acompañan al consentimiento y que, incluso, han llegado a ser utilizadas con más frecuencia que el consentimiento, sin mermar la protección del titular. Un caso significativo es el reconocimiento de la posibilidad de que los responsables realicen una serie de tratamientos con base en el interés legítimo.

La ética y la toma de decisiones

Un factor que debería ser considerado esencial en el ámbito de la innovación es la ética, la cual debería constituirse en la brújula

que, ineludiblemente, oriente las decisiones de negocio en materia de investigación y desarrollo de productos. Para el procesamiento y utilización de datos por parte de todos los actores en el ecosistema tecnológico, se debería tener en cuenta lo siguiente:

1. Sopesar los beneficios del tratamiento frente a sus riesgos,
2. El uso respetuoso,
3. El uso justo y ético.

Innovación y situaciones de emergencia

En un escenario de recuperación económica poscovid, resulta indispensable que México impulse una política de innovación basada en datos, que permita:

4. El crecimiento económico acelerado y sostenido;
5. El fortalecimiento de los avances científicos en materia de salud;
6. Se evite modificar leyes que ya están muy bien orientadas y permiten un equilibrio entre innovación y protección de datos, AI, ML, entre otros.

BIBLIOGRAFÍA

Apple habilita datos de movilidad para sumarse a la lucha contra el Covid-19 (2020). Recuperado de https://apple.co/3CghpvY

Australian Government Public Data Policy Statement (2015). Recuperado de https://bit.ly/3MnCkSH

Cuántos datos se generan cada día? (2019). Recuperado de https://bit.ly/3pHPjoB

Dirección de Gobierno en línea, Guía para la apertura de datos en Colombia (2014). Recuperado de Gobierno de Taiwán, Operational Principle of Government Open Data. Recuperado de https://bit.ly/3pBJR6n

https://data.gov.tw/en/Operational%20Principle%20of%20Government%20Open%20Data%20for%20%20Executive%20Yuans%20Agencies

https://opengovreport.ocf.tw/assets/pdf/report-en.pdf

La Carta de Datos Abiertos, Global Summit (2015). Recuperado de https://bit.ly/3sJRY2N

Making data useful for public health (2020). Recuperado de https://bit.ly/3vGJcV7

Mayer-Shönberger, V. y Cukier, K. (2013). Big Data. La revolución de los datos. Rafael Calvo (trad.). Madrid: Turner Publicaciones S.L.

Muente-Kunigami, A. y Serale, F. (2018). p.45. Los datos abiertos en América Latina y el Caribe. Recuperado de https://bit.ly/3Ce7V4B

OECD (2015). Data-Driven Innovation for Growth and Well-Being. What Implications for Governments and Businesses? Directorate for Science, Technology and Innovation Policy Note. Recuperado de https://bit.ly/35V9icp

Open Culture Foundation, Taiwan 2014 > 2016 Open Government Report. Recuperado de *https://bit.ly/3pHkAYB*

The Internet Way of Networking (2020), Recuperado de https://bit.ly/3Mup4fc

Una de las características distintivas de la sociedad contemporánea consiste en su acelerado tránsito hacia el mundo digital. Finanzas, comercio, trabajo, educación, salud, justicia y relaciones interpersonales son tan sólo algunos de los ámbitos que durante la pandemia de Covid-19 se han trasladado de la presencialidad a la realidad remota a través del apoyo de las tecnologías de la información y la comunicación (TIC), particularmente del Internet. Esta realidad digital abre nuevas posibilidades para la interacción social, pero también representa retos y desafíos como el robo de identidad, el fraude cibernético, el ciberacoso, la profundización de la desigualdad y la exclusión de las personas desconectadas, entre otros.

Este libro reúne una serie de reflexiones sobre estos procesos centrales que estamos presenciando y que necesitan considerarse para la construcción de una política digital. En los diferentes capítulos las y los autores suman propuestas para diseñar leyes y normas que permitan una mayor inclusión digital en un marco de respeto y cumplimiento de los derechos humanos. Con esta obra, el Instituto Belisario Domínguez del Senado de la República confirma su compromiso de apoyar el trabajo legislativo en la búsqueda de soluciones a los grandes problemas nacionales.

RESTORE POINT
FIELD FLOW CONTROL
P-3434-3 FIX

RESTORE POINT
FIELD FLOW CONTROL
P-3434-3 FIX

9 786078 620463