Vigilancia e instituciones en MÉXICO

La agenda pendiente de la privacidad y la protección de datos personales

Vanessa Lizbeth Lara Carmona
Coordinadora

PUBLICACIONES
UAEM

Vigilancia e instituciones en México

La agenda pendiente de la privacidad
y la protección de datos personales

Universidad Autónoma del Estado de México

Dr. en Ed. Alfredo Barrera Baca
Rector

Dr. en C. I. Amb. Carlos Eduardo Barrera Díaz
Secretario de Investigación y Estudios Avanzados

Lic. en C.P. y A.P. Maricarmen Sandoval Rubio
Encargada de la Dirección de la Facultad de Ciencias Políticas

Mtra. en Admón. Susana García Hernández
Directora de Difusión y Promoción de la Investigación y los Estudios Avanzados

Vigilancia e instituciones en México

La agenda pendiente de la privacidad y la protección de datos personales

Vanessa Lizbeth Lara Carmona
Coordinadora

Toluca, 2020

Vigilancia e instituciones en México. La agenda pendiente de la privacidad y la protección de datos personales

Vanessa Lizbeth Lara Carmona
Coordinadora

Primera edición: noviembre de 2020

ISBN: 978-607-633-223-8 (impreso)

ISBN: 978-607-633-224-5 (PDF)

D. R. © Universidad Autónoma del Estado de México

Instituto Literario núm. 100 Ote.
C.P. 50000, Toluca, Estado de México
www.uaemex.mx

El presente libro cuenta con la revisión y aprobación de dos pares doble ciego externos a la Universidad Autónoma del Estado de México. El arbitraje estuvo a cargo de la Secretaría de Investigación y Estudios Avanzados, según consta en el expediente 219/2019.

Esta edición y sus características son propiedad de la Universidad Autónoma del Estado de México. Financiamiento a cargo de la coordinadora del libro.

El contenido de esta publicación es responsabilidad de los autores.

Impreso y hecho en México

Índice

AGRADECIMIENTOS

Este libro es resultado del trabajo coordinado de diversos autores de la Universidad Autónoma del Estado de México (UAEM), entre los cuales nos encontramos los pertenecientes al cuerpo académico Instituciones y Espacios de Participación en México y América Latina, de la Facultad de Ciencias Políticas y Sociales.

La obra tiene antecedentes en el proyecto de investigación Surveillance and Freedom: Global Understandings and Rights Development (Safeguard), ejercicio colaborativo de investigadores de diferentes países y las organizaciones Privacy International (PI) e International Development Research Centre (IDRC), para tener un panorama de diversos aspectos institucionales de la privacidad en los ámbitos nacionales y regionales. En el contexto del proyecto referido, se contó con el auspicio del IDRC y la gestión de PI, lo que ha hecho posible la publicación del presente texto.

PRESENTACIÓN

Las sociedades actuales han construido la posibilidad de un orden a partir de diversas premisas, entre ellas, el reconocimiento de derechos ciudadanos y humanos, el desarrollo de la ciencia y la tecnología y elementos de participación social configurados según principios democráticos. A la par, el orden social también ha fundamentado su posibilidad en una lógica de administración de información que recopila datos de su población para organizar la gestión de recursos socialmente valiosos, pero también para afrontar amenazas internas y externas procurando la seguridad de tal orden.

Así, la vigilancia y las instituciones que la llevan a cabo se encuentran hoy día en la mira del análisis y es en este contexto que el documento que se presenta busca abrir diferentes canales de discusión, con perspectivas muy distintas y en un panorama muy amplio, referido con especial énfasis al caso institucional de nuestro país, al tiempo que se tiene como referente lo que ocurre en América Latina a propósito de acciones y tecnologías de recolección y gestión de datos personales de los ciudadanos.

En México, en las últimas dos décadas, las diversas propuestas y estrategias de seguridad que involucran la recolección de datos personales y armado de bases de datos han evidenciado una constante debilidad institucional. Los principales retos y problemas están vinculados a la base normativa, la base logística y tecnológica de la recolección, posesión, resguardo y empleo de los datos e información, así como las debilidades en torno a la protección y real utilidad de datos sensibles, frente a la posibilidad de intrusión en la privacidad y empleo negativo de éstos.

Por lo tanto, este libro reúne discusiones que vinculan los proyectos de seguridad ciudadana con la agenda internacional de protección de datos personales y privacidad, enfatizando las características y repercusiones que la debilidad institucional supone. De alguna manera, un interés común entre los autores es la contextualización de las principales líneas de debate internacional en torno a la privacidad y a la protección de datos personales y con base en este contexto general, se realiza un ejercicio que pretende esquematizar los ejes principales de la discusión en nuestro país, con la finalidad de ubicar su especificidad en diversos ámbitos y dimensiones.

En esta línea de argumentación, en el capítulo primero "La privacidad como problema social", Vanessa Lizbeth Lara Carmona y José Javier Niño Martínez exponen el detonante global de la discusión sobre el derecho al respeto de la

privacidad en el manejo de los datos, frente al argumento de la seguridad nacional y la forma en que si bien el Estado requiere preservar la integridad de los ciudadanos y sus instituciones, esto no puede ni debe constituir una justificación al manejo sin límites ni controles, porque de ser así se socavarían las libertades que le dan sentido a las sociedades democráticas modernas.

Con base en este panorama amplio de interrogantes, en el capítulo segundo "Debilidad institucional y vulnerabilidad ciudadana en la protección de datos personales en América Latina", José Luis Estrada Rodríguez y Angélica Mendieta Ramírez focalizan el análisis de las leyes de protección de datos personales en América Latina y, a partir de esta revisión, se abocan a dar cuenta de diversas problemáticas que derivan de su aplicación o incumplimiento y que revelan una debilidad institucional.

Este panorama amplio da cabida para adentrarse en el capítulo tercero "Privacidad e identidad a debate ¿Una disyuntiva en México?", en donde José Javier Niño Martínez plantea una recapitulación del debate actual acerca de las relaciones entre el ejercicio de derechos democráticos y de participación social por una parte y las garantías de protección de la privacidad y los datos personales de los actores que se involucran en dicha participación, por otra. Se presentan, entonces, interrogantes acerca de los medios jurídicos que consolidan un marco de protección al respeto a la privacidad en México: ¿cuáles son los alcances y limitaciones del derecho a la privacidad en nuestro país?, ¿su ejercicio es contemplado por la normatividad y las instituciones mexicanas? y ¿cuáles son las expectativas inmediatas que tenemos en la actualidad?

De esta manera se identifica una convergencia de intereses entre capítulos a la par que se amplían los elementos de discusión documentando casos e incorporando un análisis comparativo sobre el reconocimiento constitucional que tiene en otros países la protección de datos y la privacidad para proponer acciones y políticas públicas que construyan acciones afirmativas.

Con base en el panorama normativo perfilado en los capítulos uno, dos y tres, en el capítulo cuarto "La política de protección de datos personales en México. Análisis de políticas y retos administrativos", Porfirio Mauricio Gutiérrez Cortés especifica y aporta su punto de partida de la disertación teórica en torno a las políticas públicas, lugar desde el cual se dilucida que la respuesta del Estado mexicano a la protección de datos personales no es solamente un tema normativo,

tecnológico o sectorial, en realidad forma parte del propio diseño de una arquitectura institucional que ha enfrentado las dificultades propias del esfuerzo por democratizar la vida política y social del país. Es decir, los esfuerzos por atender el tema de la protección de datos personales no son comprensibles sólo al interrogar sus vínculos con aspectos reglamentarios de las leyes nacionales e internacionales en la materia, sino al analizarlos también como mecanismos que han buscado guiar formas específicas de intervención, en un contexto político de las políticas.

Los dos últimos capítulos retoman la discusión general acerca de los retos y problemáticas normativas, tecnológicas y de resguardo, para analizar casos concretos de áreas en las que se identifican las paradojas y dificultades de la recolección, procesamiento y resguardo de datos personales. El potencial y la necesidad de adecuados medios para tales procesos se problematiza —a propósito del internet—, en el capítulo quinto "El ARCO digital en México", la premisa de los datos personales como objeto de intercambio. Los datos de los sujetos se traducen en insumo diario de los sistemas de información privados y gubernamentales con el objetivo de analizar el comportamiento de los actores, tanto en sus facetas como trabajadores, consumidores o incluso actores políticos.

En esta dinámica resultaría evidente la necesidad de brindar alguna salvaguarda de los datos e información recolectada; sin embargo, aun cuando esto exista mediante anuncios de privacidad, las instituciones públicas o privadas no contemplan aún aspectos tales como una aclaración sobre cuánto tiempo permanecerán en su poder los datos para después eliminarlos de su sistema de almacenamiento.

Con base en este planteamiento inicial, en el capítulo referido se analiza la forma en que nuestro país ha entrado en la lógica del *Convenio 108*, a propósito de los principios de tratamiento de datos a través de medios automatizados. Los llamados derechos ARCO, acrónimo de Acceso, Rectificación, Cancelación y Oposición se describen y problematizan acerca de los retos pendientes y los avances en este rubro.

Así, frente a los obstáculos de la recolección de datos y el derecho a la privacidad, en el capítulo sexto "Ausencia de datos del desplazamiento forzado por la violencia criminal: el Estado de México en la perspectiva nacional," Martha Elisa Nateras González investiga el fenómeno del desplazamiento forzado por violencia criminal en México desde el análisis de las debilidades de construcción de datos sensibles, subrayándose que el desplazamiento, como proceso, no está

visibilizado y amenaza con crecer porque se ha potencializado el dominio territorial de los cárteles de la droga y lo etéreo de éste dificulta su registro, de tal suerte que no existe una instancia institucional que concentre la información, dificultando la generación de políticas públicas para su atención.

En esta lógica, la particularidad del capítulo sexto radica en aterrizar la discusión general sobre protección de datos personales en un ámbito problemático concreto que afecta a nuestro país: el de la delincuencia y sus efectos directos en la población. Se reflexiona entonces acerca de la potencial utilidad que la adecuada construcción y protección de datos supondría para conocer y atender uno de los daños colaterales del combate a la delincuencia organizada. En este punto, es importante señalar que el desplazamiento forzado de las poblaciones afectadas por la violencia criminal es visible en el campo, pero aún no es adecuadamente registrado pese a los efectos que implica para la calidad de vida de las poblaciones y las repercusiones en la confianza de la ciudadanía en las instituciones, tanto aquellas que están encargadas de la seguridad y la impartición de justicia, como en general, las que sostienen la solidaridad colectiva.

En la presente obra, por lo tanto, hemos considerado pertinente la inclusión de este ejercicio que avanza en la discusión y se lanzan preguntas en torno a cómo se pone a prueba la nueva arquitectura legal con que contamos en materia de protección de datos, a propósito de escenarios de esta naturaleza.

Por último, se realizan algunas reflexiones finales acerca de los temas vertidos en los diversos capítulos del libro. En especial, se plantea que la cuestión de la protección de datos personales entronca de manera estructural con la forma en que las sociedades contemporáneas se articulan, así la discusión no se agota en los aspectos normativos, tecnológicos o de política pública; por el contrario, de manera transversal a éstos, se hallan interrogantes que recorren caminos tan diversos como los propios significados en términos de derechos humanos que supone la privacidad.

La intención de los autores ha sido contribuir a la amplia discusión existente desde momentos y dimensiones de discusión muy particulares, sin olvidar que en última instancia, el tema central del presente libro forma parte de discusiones más amplias, tales como los impactos de los datos personales en cuestiones como la clasificación social, la resolución de conflictos y las posibilidades de gobierno y gestión de las sociedades contemporáneas.

I

LA PRIVACIDAD COMO PROBLEMA SOCIAL

Vanessa Lizbeth Lara Carmona
José Javier Niño Martínez

Introducción

El ascenso de la sociedad vigilada como premisa central de la vida moderna conduce a indagar sobre las razones por las cuales aceptamos diversas acciones y prácticas de vigilancia, ante lo cual se puede vislumbrar una rápida intuición que ubica al peligro percibido como respuesta. Los retos de seguridad legítima en un entorno de sociedades con violencia y criminalidad ascendente constituirían el escenario en el cual se presentan los reclamos por soluciones y en respuesta la estructuración de la vigilancia como práctica social.

Aunado con lo anterior, el andamiaje de vigilancia también supone ventajas y facilidades inmediatas para la población, entre otras, la posibilidad de conectar a los sujetos con la practicidad y las facilidades de la vida moderna, tal es el caso del comercio en línea, el acceso a información instantánea y la gestión de la propia información y agenda por medio de diversas plataformas y aplicaciones en línea, lo que permite abrir ventanas comunicativas con distintos entornos.

Frente a tales facilidades, se presentan profundas paradojas, las cuales encuentran su origen en la naturaleza propia de la vigilancia; esto pone en cuestionamiento los límites del derecho a la privacidad frente a las bondades y beneficios obtenidos. Con relación al Estado, los dilemas refieren a la posibilidad de mantener y desarrollar sociedades respetuosas de la privacidad de los ciudadanos, frente a las necesidades de seguridad y gestión de riesgos y peligros que supone la misma vida social.

El detonante: la seguridad nacional

En 2013 el experto en seguridad informática Edward Joseph Snowden saltó a la fama al convertirse en informante clave para una investigación periodística de *The Guardian*, en la cual se mostraba que las agencias de seguridad nacional y de inteligencia de los Estados Unidos de América (EE UU) habían implementado programas de vigilancia masiva a sus ciudadanos y a líderes políticos de otros países, en otras palabras evidenció un complejo sistema de espionaje que abarcaba a millones de personas alrededor del mundo por medio del cual el gobierno norteamericano espiaba con el argumento de seguridad nacional. Como consecuencia, el gobierno de EE UU levantó cargos contra Snowden por robo de propiedad oficial, convirtiéndose en un delincuente que, temeroso de la persecución de las autoridades estadounidenses, optó por el exilio, primero en Hong Kong y después en Rusia, tejiendo una trama de espionaje muy al estilo cinematográfico, aunque con consecuencias reales en este caso.

Es lógico suponer que la breve historia de espías, cuyo centro de la trama es Edward Snowden, está alejada de nuestro entorno cotidiano; sin embargo, en un contexto de interconexión virtual, esto se encuentra más cerca de nuestras vidas de lo que suponemos, de hecho la discusión centrada en el respeto a la privacidad y el manejo de datos es un tema que debe formar parte de una agenda social y gubernamental esencial en las democracias, tal y como se expondrá a continuación.

La actualidad de los servicios de inteligencia desde una perspectiva de seguridad nacional y combate al crimen organizado se explica por medio del posicionamiento del terrorismo como parte de una agenda global. Posterior a los atentados en las Torres Gemelas de Nueva York en 2001, el terrorismo ha sido el tema catalizador de una perspectiva en que la información de riesgos potenciales se ha fortalecido en las administraciones de George Walker Bush y Barack Obama, así como en todas sus áreas de influencia, principalmente en América Latina. Esta tendencia se ha mantenido en el gobierno de Donald Trump, aunque con especial énfasis en la idea de la amenaza externa como sinónimo de flujo migratorio proveniente de América Latina (en los hechos este supuesto es un error, ya que la mayoría de los atentados en territorio estadounidense se ha cometido por ciudadanos de ese país). Más allá de eso, el uso de la información

personal se observa subordinada a los principios de la llamada Ley Patriótica (USA Patriot Act) emitida por el Congreso de los Estados Unidos, para ampliar las facultades de espionaje del Estado, en aras de garantizar la seguridad nacional y de los ciudadanos, el espíritu del debate acerca de la privacidad y los derechos civiles se ha visto socavado con la implementación de esta ley en nuestro vecino del norte.

La polémica señalada con anterioridad da cuenta de un debate con repercusiones más allá de las fronteras nacionales, en virtud de la capacidad de los Estados Unidos para presionar e interferir en la política interna de gran parte del hemisferio occidental, en este sentido vale la pena señalar la necesidad de que las políticas de combate al terrorismo o a distintas modalidades de crimen respondan fehacientemente al menos a cuatro controles fundamentales para entender y justificar los distintos modelos de seguridad nacional:

En primer lugar, establecer los criterios del porqué de su implementación, ya que es fundamental que las autoridades se sometan a un escrutinio en el que de manera clara se exponga el problema que habrán de resolver los distintos protocolos de seguridad nacional, así como enunciar de manera pormenorizada los beneficios a la población.

En segundo lugar, es muy importante que también se indique la temporalidad, es decir cuándo se justifica, en qué circunstancias y por cuánto tiempo, sobre todo considerando que las decisiones con carácter de emergencia por su naturaleza no pueden ser permanentes y eventualmente se debe buscar un proceso de normalización de la seguridad.

En tercer lugar, es necesario saber hacia quién se orientarán los proyectos de seguridad, de lo contrario se corre el riesgo de que los mecanismos de prevención del terrorismo o del crimen sean una reinterpretación de las formas de clasificación social previamente existentes y por lo tanto se traduzcan en vías de exclusión, pero ahora legitimadas en el discurso de la seguridad, hay que tener presente qué eventos de esta naturaleza han dejado profundas heridas en Europa y Estados Unidos durante el siglo XX.

Por último, es imperativo hacer explícito el objeto de control en la relación entre seguridad y privacidad, así se responde al ¿para qué?; esto con el fin de establecer justificaciones legítimas, consecuentes con el debate público y las necesidades de

prevención de la violencia o el crimen, pero que sobre todo permitan un escrutinio sobre las acciones del Estado, los organismos internacionales o incluso las empresas comerciales y de servicios.

Los límites de la vigilancia

El fundamento de vigilancia en las sociedades modernas ha sido el de la posibilidad de administrarlas. Tanto lo que refiere a los medios de generación, distribución y uso de recursos socialmente valiosos, como en lo que respecta a quienes son los sujetos que se encuentran en cada posición. Tener un conocimiento de la población fue fundamental para organizar la vida social de las naciones modernas. Sin embargo, el contexto global actual privilegia la necesidad de un nuevo contrato social, pues la misma complejidad de las sociedades contemporáneas permite señalar la convivencia de reclamos por el respeto a los derechos de libertad y privacidad con aquellos de seguridad tanto ciudadana como nacional.

Por lo tanto, una perspectiva renovada de un contrato social difícilmente contemplaría el fundamento del intercambio de libertad por seguridad; por el contrario, privilegiaría el acceso a la información y el manejo de datos con controles legales claros y fundados en el respeto a la privacidad, tomando en cuenta el ascenso de esta última como un derecho fundamental en la sociedad de la información. Aunado con lo anterior, hay que tener presente que el Estado posee información de sus ciudadanos. Éste es el principal riesgo porque tiene que ver con el uso que se hace de ésta, sobre todo por la posible discriminación y control sobre ciertos sectores de la población, ya sea como activos de vigilancia o como estructuras de control clientelar.

Retomando la experiencia de Snowden, sus declaraciones hicieron público algo que forma parte del imaginario propio de la modernidad: la sociedad de la información implica datos y el control de éstos es poder y capital económico; sin embargo, en alguna medida somos conscientes o suponemos que esos datos existen, por ejemplo en el incremento de las cámaras de videovigilancia o CCTV (Closed Circuit Television) para abatir los índices de criminalidad, la recopilación de datos de identidad jurídica y biométricos en documentos de identificación oficiales o en los algoritmos generados por la navegación en el internet que realizan los

ciudadanos de manera casi cotidiana. Frente a este panorama no se ha extendido de forma suficiente un marco legal que proteja la identidad de las personas, cuyos datos personales pueden recopilarse e incluso hasta comercializarse; por el contrario, es cada vez mayor la aceptación y normalización de los diversos medios de captación de datos, así como de su utilidad para la actividad comercial o de vigilancia.

Esta normalización no se presenta sólo desde la perspectiva de los usuarios, sino de los agentes que acceden a los datos personales, de tal manera que en países como México, por ejemplo, la vulnerabilidad con relación al acceso no autorizado a los datos personales es alta; en tanto que la acción de proteger, restringir y controlar tal acceso supone una enfadosa trayectoria burocrática.

Recapitulando, se pueden distinguir algunos entornos de discusión que nos permiten encontrar sentido a múltiples problemas actuales alrededor de la privacidad como elemento definitorio de la relación entre Estado, sociedad y mercado:

En primer lugar, el ascenso del discurso de la seguridad nacional como resultado de los atentados del 11 de septiembre de 2001 en la ciudad de Nueva York, Estados Unidos, los cuales significaron un cambio global en la forma en que se diseñan e implementan medidas de protección a riesgos externos a las fronteras nacionales. Con este discurso se han instrumentado acciones militares extraterritoriales por parte de Estados Unidos por medio de intervenciones armadas principalmente en medio oriente (Irak, Afganistán) y del mismo modo se han endurecido los filtros en las fronteras con el fin de controlar los flujos migratorios con el argumento de la seguridad nacional. En este sentido, vale la pena señalar las acciones de los Estados Unidos y de su personal militar en la base de Guantánamo, donde los detenidos son sometidos a procesos judiciales que regularmente violan sus derechos humanos y que de igual manera son cuestionados por instancias internacionales de derechos humanos, en gran medida, debido a que la legislación internacional se encuentra en una situación muy confusa en lo que se refiere a ese tipo de delitos. De igual manera, la administración de Donald Trump ha recurrido constantemente a la criminalización de los migrantes mexicanos y centroamericanos como un recurso discursivo con el fin de promover el cierre de fronteras, reavivando el nativismo como una ideología dominante. El efecto de este endurecimiento discursivo y práctico en las fronteras ha posicionado en un plano estratégico los medios de identificación de ciudadanos y de no ciudadanos en tránsito.

En segundo lugar, hay que tener presente la relevancia creciente de las empresas tecnológicas y el acceso a información individual, cuya apropiación se expresa en el debate sobre el manejo de los datos que se encuentran expuestos por los mismos usuarios y cuya disponibilidad corporativa da cuenta del negocio creciente del manejo de información. En este sentido, vale la pena reconocer que existen grandes limitaciones jurídicas tanto en el derecho internacional como en las normas locales que impulsan los diferentes países, sobresaliendo el esfuerzo regulatorio que ha impulsado recientemente la Unión Europea. Como consecuencia de lo anterior, el manejo de datos no sólo ha roto fronteras en su recopilación, sino sobre todo en el ámbito de la regulación en el uso de éstos, lo cual ha quedado expuesto en casos como el de la controversia de Cambridge Analytica en 2018, la cual fue expuesta por algunos diarios como *The New York Times* y *The Guardian* que hicieron de conocimiento público el uso que esta empresa dio a la información de usuarios de Facebook y que por medio de los datos de los perfiles personales buscó intervenir en distintos procesos electorales (incluido México), pero de manera sobresaliente en la elección presidencial de los Estados Unidos, lo cual sumado a la supuesta injerencia de *hackers* rusos constituyó un hito en la controversia de los comicios estadounidenses.

En tercer lugar, el acceso multitudinario a las redes sociales ha permitido la conectividad y el intercambio de información personal de manera inmediata y dinámica; sin embargo, el costo ha sido la información personal de los usuarios que se encuentra disponible en el ámbito público, pero de igual manera esto ha permitido el fortalecimiento de las plataformas comerciales. En otras palabras, el mercado en línea es un entorno fértil para la ampliación del sistema económico, tanto por la dinámica de las transacciones comerciales como de acceso a perfiles de consumo, los cuales a su vez se convierten en objetivo de interés mercantil. El mercado capitalista ha encontrado en el acceso tecnológico a medios comerciales el espacio adecuado para florecer, esto en virtud de la eficiencia en la distribución de bienes y la prestación de servicios específicos.

En cuarto lugar, datos en el mundo dejan ver con claridad el incremento de delitos relacionados con el robo de identidad o suplantación de identidad en servicios financieros, en el caso de México no es la excepción y por lo tanto resulta urgente que el marco legal se ajuste a la magnitud del problema. Según datos de la Comisión

Nacional Bancaria y de Valores (CNBV) de 2016 a 2017 se triplicaron el número de denuncias sobre este delito, superando la cifra de 16 000 reportes, por lo que a partir de 2018 los bancos en el ámbito nacional han comenzado a aplicar controles biométricos; estos datos, sin embargo, no están exentos de controversia, ya que según la Comisión Nacional para la Protección y defensa de los Usuarios de los Servicios Financieros (Condusef) las denuncias registradas por fraudes cibernéticos pasó de 172 424 en 2015 a 1 244 415 tan sólo en el primer semestre de 2019, este crecimiento sistemático y desproporcionado representó un monto aproximado de 2 834 millones de pesos el presente año, concentrándose principalmente en el rubro de comercio por internet, banca móvil y operaciones adicionales por internet.[1] Lo anterior hace indispensable promover el debate nacional e internacional respecto a los mecanismos de verificación de la identidad personal en un entorno caracterizado por el comercio en línea con el fin de combatir de manera eficiente el cibercrimen, dicha justificación que debe estar acompañada por reglas claras en la protección de datos personales y normas concretas acerca de las responsabilidades de los entes privados, el Estado y en el ámbito internacional para proteger a los individuos e incluso las colectividades sobre la forma de recabar, almacenar y usar los datos de identidad biométrica a los que se está recurriendo en la actualidad.

En quinto lugar, el fenómeno migratorio de países pobres expulsa a gran parte de su población en busca de una mejor situación económica o huyendo de condiciones de inseguridad y violencia estatal. Centroamérica, África y Asia principalmente se han convertido en entornos de expulsión de caravanas formadas por hombres, mujeres y niños que intentan llegar a Estados Unidos o Europa huyendo de la pobreza, el crimen o la guerra que azota a sus países de origen.[2] La magnitud de estos desplazamientos representa un reto determinante para los distintos estados nacionales expulsores, de tránsito y de recepción en diferentes flancos: para garantizar una reducción importante de migraciones forzadas, para asegurar facilidades a la condición de refugiado si así es el caso, para proteger los

[1] En este sentido vale la pena revisar la información que señala la Condusef: https://www.condusef.gob.mx/gbmx/?p=estadisticas

[2] Según datos de la Organización de las Naciones Unidas el número de migrantes internacionales (personas que residen en un país distinto al de su nacimiento) pasó de 244 millones en 2015 a 258 millones en 2017 en el ámbito mundial (ONU, 2018).

derechos humanos de las personas en tránsito, para promover condiciones dignas de trabajo y servicios básicos a los que adquieren la calidad de residentes. Aunado con lo anterior, se puede distinguir el endurecimiento de las políticas migratorias de los países receptores, el ascenso del reconocimiento del estatus político de ciudadano cobra una mayor importancia en un entorno de esta naturaleza.

La agenda social acerca de la privacidad también, por un lado, expone la necesidad de generar confianza entre los ciudadanos, con el fin de consolidar a la democracia política en México (Tilly, 2005); esto implica la responsabilidad del Estado en el manejo de información de sus ciudadanos, la elaboración y aplicación de leyes que permitan garantizar un resguardo pertinente de todo tipo de información personal. Al provenir de un pasado autoritario, es razonable que la ciudadanía ponga en tela de juicio la labor del gobierno en la administración de la confidencialidad de los datos.

Conclusión

Como se pudo ver anteriormente, las tecnologías de la vigilancia están presentes en el entorno cotidiano, tanto que nos pasan desapercibidas las probabilidades de recibir información o notificaciones que predicen nuestros deseos e intereses, los algoritmos están presentes en la vida cotidiana, no sólo datos como nombre, dirección, número telefónico o correo electrónico se recopilan y clasifican sistemáticamente en bases de datos, también datos biométricos como huellas dactilares, reconocimiento facial y reconocimiento de voz representan sistemas de registro de los que nadie escapa en el mundo moderno (Guzik, 2016).

Como resultado de este entorno de integración a amplias redes de articulación y distribución de información, existen distintas esferas de discusión en las que el manejo de datos personales y la privacidad del individuo sobre los éstos resulta fundamental en aras de brindar certeza jurídica y a la vez de garantizar la protección de derechos y seguridad nacional. Casos como el de Edward Snowden permiten exponer la importancia sobre este tema en un entorno global y complejo.

De igual manera, diferentes actores entran en el debate por medio de distintas plataformas de discusión:

Por un lado, el *Estado* como posible medio de recopilación de información personal y al mismo tiempo como responsable de múltiples violaciones a la privacidad de la población, debido sobre todo a la inexistencia de un marco jurídico claro.

Por otro lado, las *empresas* que disponen de la capacidad de gestionar bases de datos de información de usuarios y que pueden monetizar los datos que recopilan.

Finalmente para la *sociedad* representa un reto importante tener un conocimiento claro acerca de lo que se hace con sus datos y cuáles son las ventajas de permitir su manejo.

Para concluir, la formación de una agenda de discusión alrededor de la defensa de la privacidad hace necesario incluir a distintos actores en el debate, respetando en todo momento las libertades democráticas y ante todo la visibilidad de las consecuencias del control social, ya que de lo contrario la incertidumbre al respecto se puede traducir en concentración de información más allá del control legal, haciendo posible la existencia de sociedades esclavizadas mediante la información, en la medida en que el futuro de la convivencia social ubica el uso y gestión de datos personales como elementos clave para comprender las interrogantes que se plantean en la agenda internacional y nacional.

Referencias

Bibliografía

Guzik, Keith (2016). *Main things sticks: surveillance technologies and Mexico's War Crime*, University of California Press, Oakland.

Haggerty, Kevin D. y Richard V. Ericson (2007). *The new politics of surveillance and visibility*, Toronto University Press, Toronto.

Lyon, David (2006). "The search for Surveillance theory", en David Lyon (ed.) *Theorizing Surveillance. The panopticon and beyond,* Willan Publishing.

Tilly, Charles (2005*). Confianza y gobierno*, Amorrortu, Buenos Aires.

Mesografía

Hernández, Antonio (2018). "CNBV: durante 2017, 16 596 casos de robo de identidad" [en línea]. Disponible en https://www.eluniversal.com.mx/cartera/negocios/cnbv-durante-2017-16-mil-596-casos-de-robo-de-identidad, consultado el 8 de febrero de 2019.

II

DEBILIDAD INSTITUCIONAL Y VULNERABILIDAD CIUDADANA EN LA PROTECCIÓN DE DATOS PERSONALES EN AMÉRICA LATINA

José Luis Estrada Rodríguez
Angélica Mendieta Ramírez

Introducción

Este capítulo tiene como objetivos describir y analizar cómo se está desarrollando la economía de datos y el crecimiento de la información sobre las personas, datos que en la actualidad se encuentran en las plataformas digitales soportadas por internet, donde la normatividad resulta insuficiente para el desarrollo del resguardo a los derechos de protección de los ciudadanos en América Latina, por sus democracias frágiles y su debilidad institucional para castigar, controlar o sancionar al respecto. Un ejemplo de ello es la videovigilancia, donde si bien existe una normatividad para dar a conocer a los ciudadanos que están siendo grabados, existen inconsistencias y falta de aplicación de la ley.

The Economist, recientemente, periódico muy importante de Londres, dio a conocer que los choferes de Uber interpusieron acciones legales contra la empresa, para conocer sobre sus datos recopilados en la plataforma de servicio a usuarios; ellos deseaban saber cuál era la información que tenía la compañía sobre los viajes que realizan y cómo son calificados por los usuarios. El acceso a su evaluación, calificación y revisiones permitiría eventualmente apelar al despido improcedente que sucede cuando tienen malas calificaciones en sus servicios de chofer.

Hasta el momento no existe forma de acceder a la información que tiene la empresa, que forma parte de los datos personales que deberían ser resguardados por el Estado y las autoridades competentes. Existe también la recurrencia a la videovigilancia en el empleo, en las empresas y fábricas; como un mecanismo para

medir la productividad. Los empleados pueden ser vigilados y despedidos por su comportamiento, donde el proceso para apelar o contrarrestar a la vigilancia escapa a la legislación existente.

Si bien la ley que protege la privacidad y los datos personales tiene un avance sustancial en las legislaciones de América Latina, sobre todo en México; existe un ensanchamiento de las plataformas digitales y mecanismos de recolección de datos en formatos virtuales que proliferan y constituyen una amenaza a la privacidad de los ciudadanos; toda vez que los datos abiertos en la red abundan y no existen mecanismos explícitos para su resguardo controlado. Además, las redes sociales muestran información de manera abierta y en ocasiones se vulnera el principio de privacidad que debiera privilegiarse. En la economía actual, el valor del trabajo no proviene necesariamente de la actividad que se realice, sino de los datos que arroja, es decir, el número de personas atendidas, el número de productos terminados y el ejercicio de la libertad está en entredicho por la vigilancia; pero también, por el desarrollo de amplias formas de control a partir de los datos.

Las campañas electorales tienen un uso excesivo de datos, información y aplicaciones de *big data*, que se utiliza sin protección hacia los ciudadanos. El escándalo de Cambridge Analytica dio a conocer que se utilizaron los datos recopilados por un investigador para la campaña presidencial de Donald Trump en 2016, pero también en el referéndum Brexit, sobre la estadía de Inglaterra en la Unión Europea, así como otras campañas políticas. Hasta marzo de 2018, cuando se descubrió que esos 82 millones de perfiles habían aportado datos de sus preferencias electorales y perfiles de Facebook, fue imposible establecer sanciones y mecanismos de control. Se mostró que los ciudadanos están vulnerables a la recopilación que hace Facebook de los datos de navegación y, por ende, de la información de cada persona.

En México, un análisis del impacto de las redes sociales y del *big data* revela que existió en nuestro país un uso deshonesto sobre los beneficios de internet, para conocer la intención del voto de los ciudadanos. Se descubrió que una instancia del Partido Revolucionario Institucional (PRI) contrató servicios de vigilancia y espionaje digital en 2012 para investigar a sus contrincantes (Laurent *et al.*, 2018).

Al respecto, Cédric Laurent *et al.* mencionan: "La coordinación digital de campaña de Peña Nieto recurrió a la creación y difusión de noticias falsas, llamadas

telefónicas masivas a ciudadanos sin su consentimiento, bots orgánicos y digitales, espionaje político, servicios de medición social, encuestas falseadas y contratación de hackers, entre otras" (2018 [en línea]).

En las instituciones bancarias y de crédito también se recopila información personal. Los bancos realizan todo el tiempo esquemas de discriminación y control sobre los usuarios a partir de pautas de información que reciben sobre el número de depósitos que realizan los usuarios, el importe de sus créditos bancarios y hasta el monto de los salarios que perciben. En la encuesta sobre vulnerabilidad financiera, es decir, el riesgo manifiesto de los usuarios del banco, de haber sufrido un fraude o alteración de sus cuentas en América Latina es muy alto, la frecuencia con la que los usuarios expresan haber sido víctimas dio como resultado que en su mayoría (62.75%) sufrieron incidentes de esta naturaleza una sola vez, de acuerdo con la encuesta aplicada por la Organización de Estados Americanos (oea), en 2018.

Con frecuencia se realizan llamadas telefónicas para recibir ofertas y promociones, ¿los bancos cómo obtienen esta base de datos?, ¿cuál es la problemática que producen estos datos, los cuales están en internet?, éstas son las preguntas que se plantean para abrir la discusión sobre el tema. Si bien en un principio la recopilación de información estuvo vinculada con la mercadotecnia, ahora las campañas políticas también contratan a expertos en obtención de datos para enviar mensajes, conocer a los usuarios de las redes sociales y promover productos, ideas y candidatos. Google y Facebook recibieron, en 2017, ingresos de publicidad contratada por un monto estimado de 135 000 millones de dólares. Esto sucedió como una contraprestación por entregar los datos recopilados de los usuarios, sobre qué sitios visitan, en qué horario y cuáles son sus preferencias de consumo digital. Esta información considerada como información personal se comercializa para construir campañas de publicidad, pero también para incidir en el comportamiento y las ideas de los usuarios. La protección a la intimidad, a la imagen y a los datos están en amplio riesgo si no se cuenta con mecanismos para garantizar el resguardo de la información.

Resulta pertinente, entonces, una reflexión sobre cuáles son los alcances que tienen las leyes en América Latina y cuáles son las debilidades institucionales existentes en torno al cumplimiento del resguardo de los datos personales. Partimos de la hipótesis de que resguardar el bien jurídico que se tutela con la protección de

datos exige un amplio desarrollo de información y promoción de los derechos; para evitar que la protección de datos personales incida en el desarrollo de conductas nocivas como la corrupción o el ocultamiento de información de orden público. Si bien, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), en México ha multado a empresas con 424 millones 340 mil 941 pesos, durante el periodo de 2012 a enero de 2019; existen todavía casos en los cuales se produce un daño al orden público por las inconsistencias en el resguardo de la información, como actos de corrupción donde los servidores públicos deben tener mayor vigilancia y control que los particulares por el bien jurídico que tutelan.

El control de los datos y la información privada es muy importante, porque un tratamiento inadecuado de la información personal podría traducirse en usos que afecten la vida de las personas, exponiéndolos al riesgo de ser objetos de discriminación o hacerlos blanco de delitos graves como el secuestro o el robo de identidad. Pero también producen despidos por el control de la videovigilancia y generan diagnósticos y tratamientos médicos erróneos por la apertura en la información de datos médicos. Por este motivo, el tratamiento de esta información debe ser tratada con apego a los principios de legalidad, calidad, disponibilidad, confidencialidad, seguridad los cuales permitan que esta información sólo sea accedida por personas autorizadas (INFOCDMX, 2011 [en línea]).

José María Dorado y Jesús Fernández (2006) sostienen que con la era de la información se ha transformado el desarrollo de la sociedad, incluyendo la relación entre médicos y pacientes en el ámbito privado porque se ha trasladado a los pacientes la responsabilidad de cómo tratar su enfermedad y eso hace que los datos sobre los tratamientos estén más abiertos y públicos; es un riesgo la protección de datos tanto para los médicos, como para los pacientes. Antes era más fácil mantener una relación aislada del entorno y de acceso a terceros, pero con la telemedicina que es práctica médica a distancia, se produce un vacío en términos legales y replantea la importancia de cómo acotar y controlar la información médica en las webs sanitarias.

Un ejemplo de ello se dio en 2012, cuando el periódico *Daily Mail* publicó en su encabezado principal: "Reino Unido, adicto a las pastillas para dormir", porque habían solicitado información sobre el costo de las pastillas al área de seguridad

social, que dio a conocer un incremento en las pastillas que solicitaban los pacientes en 17%. Un tercio de la población de Reino Unido padece de insomnio. La información pareciera privada, pero mediante un recurso de acceso a la información pública se logró conocer este importante dato (Bergareche, 2012). Por ello, pareciera que la transparencia gubernamental se contrapone con el derecho de los ciudadanos a la privacidad y a tutelar la intimidad.

En la comunidad europea, se ha desarrollado una extensa normativa al respecto; pero en América Latina, sobrepasa la burocracia las posibilidades de control. En el derecho internacional no existe una norma expresa que ampare las singularidades del tratamiento automatizado y protección de los datos de salud, por lo cual es un área de oportunidad para el desarrollo de la discusión sobre este tema en un mundo hiperconectado. La propiedad de los datos en reserva de entidades públicas debe ser resguardada por el Estado y establecer mecanismos de control; en tanto que dentro del ámbito privado exige una regulación más estricta.

En ese sentido, la protección de datos personales tiene una reflexión profunda porque entraña la ampliación de los derechos fundamentales, sobre todo en el tratamiento y almacenamiento de información en redes virtuales como internet, incluyendo las redes sociales (García, 2007). La consolidación de las Tecnologías de Información y Comunicación (TIC), así como la tutela del derecho a la intimidad adquieren nuevos matices; por lo cual, este trabajo de análisis y discusión tiene dos insumos: por una parte, el análisis de las leyes de protección de datos personales en América Latina; y por otra, las problemáticas que derivan de su aplicación o incumplimiento, que constituyen las inconsistencias en torno al bien jurídico que resguardan y ante la debilidad institucional de las democracias débiles en América Latina, presenta falta de ejecución y muestra la exigencia de un rediseño institucional.

Sobre todo, después de las revelaciones que hizo Cambridge Analytica, una empresa que logró obtener los datos personales de más de 50 millones de personas, mediante dar a conocer sus hábitos y preferencias no sólo en su consumo de medios digitales; sino también de esquemas de inclinación electoral y eso podría incidir en el funcionamiento de las democracias en América Latina (Jourova, 2018 [en línea]).

Asimismo, en este capítulo se recurre a un análisis comparativo sobre el reconocimiento constitucional que tiene en otros países para proponer acciones y políticas públicas que construyan acciones afirmativas. El trabajo se divide en tres apartados: en el primero se describe el contexto histórico de la protección de datos personales, explicando la problemática que presentan; el segundo apartado analiza las leyes en la materia, por país y con una explicación detallada sobre América Latina. Finalmente, en la conclusión, proporcionamos los pormenores de la discusión al estudio documental y de casos, para el desarrollo de enclaves teóricos; así como las aportaciones para consolidar esta línea de investigación académica en su aplicación práctica y de incidencia social.

Contexto sociohistórico de la protección de datos

El derecho a la intimidad de las personas fue reconocido desde las primeras leyes en el contexto histórico; sin embargo, el derecho a la intimidad ha tenido múltiples adecuaciones, donde además de la facultad del individuo de rechazar invasiones a su ámbito privado, también exige el cumplimiento del Estado en la tutela del control y acceso de sus informaciones. Esto significa que el Estado debe ser vigilante de los datos que están en su poder, pero también regular a otras instituciones y organizaciones que eventualmente cuentan con datos de los ciudadanos.

José Luis Goñi (2007) señala que la imagen de videograbación es un dato personal que debe controlarse. La videovigilancia se ha convertido en una constante, con el incremento de la delincuencia en América Latina. Pero la normatividad es general, sólo se pide que se anuncie que hay cámaras, pero no hay mayor protección de los usuarios y de los datos que recopilan en el ámbito interno y externo. Existe una indeterminación; según el reporte del IMS Research (2014), "el mercado de la videovigilancia en América Latina mantuvo una tasa de crecimiento del 40.5% desde 2008 hasta 2013 y, según las previsiones hechas en dicho reporte, se espera que esa tasa se mantenga cuando menos hasta el 2019" (Arteaga, 2016: 195 [en línea]).

El *Reglamento General de Protección de Datos* (RGPD), aplicable en Europa, establece: "la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos"

(doeu, 2016 [en línea]); sin embargo, ante el crecimiento de las posibilidades tecnológicas se produce una carrera contra el tiempo, porque la ley avanza antes que la tecnología; sin embargo, ante el crecimiento de las posibilidades tecnológicas se produce una carrera contra el tiempo, porque la ley avanza antes que la tecnología. A continuación, se describen los antecedentes y el contexto sociohistórico de cómo se ha avanzado en el proceso del reconocimiento de los derechos de protección de datos.

Las primeras declaraciones de derechos y constituciones que se produjeron en los estados-nación consagraban los derechos y libertades: Inglaterra de 1688, Estados Unidos de 1787 y Francia de 1789 reconocen la inviolabilidad del domicilio, el secreto de las comunicaciones, cartas y documentos que se enviaban; así como la intimidad corporal. La libertad de los individuos también está centrada en la capacidad de intimidad, protección de sus datos y la posibilidad de tomar decisiones que no estén controladas por el Estado y otros actores.

La legislación sobre protección tiene sus antecedentes en Europa, donde existe un énfasis en reconocer y garantizar la protección de datos personales a sus ciudadanos, en donde toda aquella información relativa a su persona queda libre de intromisión, salvo el consentimiento del interesado. En otros países como México, Argentina, El Salvador, Colombia y Paraguay, el reconocimiento de este derecho es fundamental, pero muy incipiente. En torno a los derechos humanos que se consagran en las constituciones de estos países, podemos hablar de tres generaciones: la primera generación de derechos humanos se refiere al siglo xviii, donde se legisló sobre las libertades individuales, los derechos de la persona, como han sido llamados, donde lo que se buscó fue evitar la injerencia de los poderes públicos en la vida privada. La segunda generación de derechos recoge la posibilidad de contar con esquemas de provisión económica, social y cultural; estos derechos fueron incorporados en las legislaciones de todo el mundo, a finales del siglo xix y durante el siglo xx.

Los derechos de tercera generación están vinculados con la justicia, paz y solidaridad. La intimidad está dentro de los derechos de reconocimiento, pero también la libertad informática como un nuevo derecho del individuo a tutelar su propia identidad informática, otorgando la posibilidad de acceso a la información, bancos de datos y reconocimiento digital. Con el surgimiento de internet y las

TIC, se ha construido un mundo virtual que reconoce la dimensión social y tutela a la persona en su condición de ser social (Herrán, 2003).

Empero, existen inconsistencias en torno a la aplicación de las normas alrededor de la protección de datos, porque hay casos documentados en los cuales proteger el acceso a los documentos sobre los funcionarios públicos permite la corrupción o hasta el encubrimiento de las personas señaladas por algún acto indebido o ilícito. Como ejemplo podemos señalar el caso del juez penal de Cholula en Puebla, México, José Refugio León Flores. Un periodista mediante la búsqueda de información sobre su título que lo acreditara como abogado —un requisito inherente a su función— encontró que el juez León Flores entregó un título y una cédula falsos para probar que había estudiado la licenciatura en Derecho (Aroche y De la Torre, 2019 [en línea]).

En la historia que se relata, se solicitó a la universidad donde el juez León Flores había señalado que estudió; sin embargo, en su momento se negó dicha información argumentando que se trataba de información confidencial. Fue necesario impugnar dicha resolución ante el Instituto de Transparencia y Acceso a la Información Pública de Puebla (ITAIP); no obstante, el organismo ratificó la respuesta de la universidad; por lo que fue necesario buscar un amparo ante el juzgado federal para obtener dicha información. Por fin, el 14 de febrero se ratificó la sentencia y el tribunal colegiado en una segunda instancia otorgó el amparo y entregó la información al periodista Ernesto Aroche. No obstante, la actual presidenta del ITAIP, Laura Carcaño Ruiz, señaló sobre este tema a los medios de comunicación que el instituto decidió proteger los datos personales del juez y el derecho de la universidad pública del estado de Puebla, de mantener la reserva sobre esta información (Aroche y De la Torre, 2019 [en línea]).

En este sentido, se describe una inconsistencia de la protección de datos personales para un tema de interés público, sobre todo vinculado con un acto de corrupción, toda vez que Ley de Transparencia y Acceso a la Información Pública, en México, "establece que no se podrá reservar información relacionada con actos de corrupción o violaciones a derechos humanos. Es decir, la ley aprobada en 2015 prohíbe explícitamente la reserva de esta información por la gravedad e impacto que estos casos tienen en la vida de las personas" (Salvatierra y Oropeza, 2018).

De acuerdo con Thomas Hobbes, existe libertad por parte de los individuos en tanto que el Estado no marque una regla o norma que rompa con esa libertad. Por ello, es necesario que se acoten su actuación con leyes, pero también que permita hacer uso de su racionalidad, libertad y criterio en el ámbito interno. Posteriormente, John Locke sostiene que existe libertad de actuar por parte de los sujetos, pero debe existir una ley capaz de proteger su libertad, sin restringirla o acotarla. Los ciudadanos pueden elegir el camino que mejor decidan, siempre y cuando no se afecte los derechos de terceros o se atente contra el ámbito privado.

Así, el pensamiento liberal contempla la necesidad de proteger la esfera privada frente a las posibles intromisiones del poder público. Resguardar las bases de datos con la información sobre los ciudadanos es una tarea del Estado. Volviendo a Hobbes, él sostiene que los individuos gozan de libertad negativa o derecho negativo, que se refiere a la amplia posibilidad de que hagan lo que deseen, sin menoscabo de alguna coacción o sanción. Así, los datos personales pertenecen a estos valores jurídicos que establecen y reconocen al individuo que en la esfera personal no pueden ser invadidos. Ahí se marca una frontera entre la vida privada y la actividad pública, donde sí puede ser cuestionada una persona sobre su actividad, preferencias y bienes materiales que tiene.

Este tipo de derechos son libertades civiles porque posibilitan el desarrollo armónico de la sociedad y la construcción de un Estado de derecho que permita el libre pensamiento y autodeterminación de los ciudadanos. De ahí surgió el término *habeas data*, que es una locución latina que significa 'habed, traer tus datos', también comprende los bienes externos como la integridad física, libertad y bienes internos o inmateriales como el honor, dignidad, fama u otros, los cuales deben ser preservados por el Estado.

Los datos personales constituyen elementos o bienes personales a los cuales los ciudadanos no pueden renunciar, sin vulnerar o afectar su dignidad humana. Al respecto Carlos E. Saltor menciona:

> posteriormente en 1990, el derecho a la protección de datos personales da sus primeros pasos en América Latina a través de la incorporación de la garantía constitucional conocida como *habeas data*, en casi todas las constituciones de la región. Sin embargo, la escasa legislación en torno a la protección de

> datos promulgada en leyes tiene un sistema de control extremadamente débil y dependiente del Poder Ejecutivo, porque se carece de autonomía y recursos presupuestales propios en general, para hacer frente a una problemática vinculada con la información en internet y en dispositivos digitales (2013: 70).

El mismo autor explica que el derecho a la protección de datos personales está consagrado en la *Constitución*, pero no existen mecanismos reales con los cuales se puedan proteger efectivamente. Por ejemplo, en México los usuarios de los sistemas bancarios reciben de forma constante llamadas ofreciendo promociones, tarjetas de crédito y otros bienes; sin embargo, no sólo en este rubro, sino también en el ámbito político se realizan encuestas y se afilia a los ciudadanos sin su consentimiento, ante el vacío legal y la incapacidad sancionatoria de la ley.

Saltor, además, manifiesta: "no es posible dar protección jurídica efectiva a los datos de carácter personal sólo mediante declaraciones de derechos que en la práctica carecen de una correlativa aplicación real, así como la capacidad sancionatoria" (2013: 70). En México, por ejemplo, existen diferencias en las legislaciones en el ámbito subnacional que no coinciden. El *Convenio 108* del Consejo de Europa para los Derechos Humanos, signado el 28 de enero de 1981, establece que los datos personales constituyen toda aquella información que pueda conducir a la identificación del individuo: nombre, teléfono, dirección, datos bancarios, resultados de exámenes médicos, transacciones comerciales, correo electrónico, entre otros; donde también puedan existir datos "sensibles" que lo identifiquen como origen racial, simpatía política, convicción religiosa, salud, preferencias sexuales, entre otros.

En ese sentido, se prohíbe la transmisión de datos por cualquier mecanismo que rebase las fronteras de los Estados, porque podrían quedar interrumpidas dichas transformaciones entre América y Europa, incluyendo datos financieros, bursátiles y bancarios. En el ámbito internacional, existen diversos mecanismos para la protección de datos personales: el Pacto Internacional de Derechos Civiles y Políticos en su artículo 17, Convención Americana sobre Derechos Humanos, también conocida con el nombre de Pacto de San José de Costa Rica, así como el Convenio para la Protección de los Derechos Humanos y las Libertades Fundamentales en su artículo 8, que establece el derecho al respeto a la vida privada y familiar.

En ese sentido, Danilo Doneda expresa: "Brasil fue el primer país de América Latina en introducir la acción de *habeas data* en 1988. Esta acción otorga el derecho al individuo de poder acceder, así como poder rectificar sus datos almacenados en una base de datos" (2017: 46). Para el caso de Costa Rica, el artículo 23 de su *Constitución* sostiene que es inviolable el domicilio particular y cualquier otro recinto privado de los ciudadanos. Empero, establece que puede violarse y allanarse el domicilio particular mediante una autorización expresa por un juez. La Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, publicada el 5 de septiembre de 2011, establece que el resguardo de los datos privados se realizará sobre toda aquella información que figure en bases de datos automatizadas o manuales, tanto de organismos públicos como privados.

Al igual que en la mayoría de las legislaciones existentes en América Latina, se exige la obligación de informar a los usuarios sobre la existencia de una base de datos, de los fines que persigue la recolección de datos y cuál es el destino de los datos que se recopilan. Sucede igual que con el caso de la videovigilancia; donde es preciso informar sobre el tratamiento que se dará a dicha información, así como las consecuencias negativas y la posibilidad que tienen de ejercer alguna acción sobre los datos. La Agencia de Protección de Datos de los Habitantes (Prodhab) es un órgano desconcentrado adscrito al Ministerio de Justicia y Paz de Costa Rica.

En Uruguay, se promulgó la Ley de Protección de Datos en agosto de 2008. En Argentina, en 1994, se incorporaron las modificaciones a la *Constitución*, para garantizar los derechos de los ciudadanos, pero fue hasta 2002, que la Dirección de Protección de Datos Personales dictó normas reglamentarias en materia de registro, infracciones, medidas de seguridad y códigos de ética. En la normatividad vigente de Uruguay, se establece el ámbito objetivo que se refiere a la aplicación de la ley al ámbito privado y público, así como en el ámbito subjetivo, conformado por los datos personales que se aplican por extensión a las personas jurídicas en cuanto corresponda.

En el caso de Colombia, con la Ley 1581 y 1266 se reconoce el derecho y las obligaciones en materia de datos personales. Incluye uno de los temas más importantes que es el derecho al olvido y el nombramiento de oficiales de protección de datos. En México, la Ley de Protección de Datos Personales vigente desde 2010 establece

la privacidad en el tratamiento de datos personales, incluyendo su obtención, uso, transferencia y almacenamiento. De acuerdo con el Banco Interamericano de Desarrollo (BID, 2019), nuestro país tiene un fuerte avance en torno a los procesos, de los cuales se logró reconocer 820 procedimientos de protección de derechos ARCO, que son las acciones vinculadas con el acceso, rectificación, cancelación, oposición, limitación y portabilidad de los datos personales; donde es preciso que los ciudadanos soliciten ante el INAI estos recursos.

En tanto, el caso de Perú es importante porque mediante la Ley 29773, se busca un marco de protección más amplio y otorga derecho a los tutelares de los datos en caso de que las empresas que tratan sus datos personales no cumplan con sus obligaciones. Además, establece que todos los datos de las personas naturales que son gestionados en las empresas como clientes, colaboradores y proveedores deben tener un resguardo y protección.

En El Salvador, durante diciembre de 2010, se aprobó la Ley de Acceso a la Información Pública, normativa que dio vida al Instituto de Acceso a la Información Pública. Asimismo, desde la *Constitución de la República de El Salvador* en su artículo 2, se garantiza a todo ciudadano salvadoreño el derecho a la intimidad, entre otros; además plantea sanciones: multa de 20 a 40 salarios mínimos mensuales para el sector comercio y servicios en caso de comisión de infracciones muy graves, multa de 10 a 18 salarios mínimos mensuales para el sector comercio y servicios en caso de comisión de infracciones graves y multa de uno a ocho salarios mínimos mensuales para el sector comercio y servicios en caso de comisión de infracciones leves.

En el caso de Guatemala, la *Constitución Política de la República de Guatemala* reconoce el derecho a la intimidad, al honor y a la privacidad; que en su conjunto también garantizan la existencia y goce de otro derecho: el referido a la autodeterminación informativa. En su artículo 24 establece: "la inviolabilidad de correspondencia, documentos libros. Se garantiza el secreto de la correspondencia y las comunicaciones telefónicas, radiofónicas, cablegráficas y otros productos de la tecnología moderna" (CPRG, 1985 [en línea]). Asimismo, el artículo 31 plantea que quedan prohibidos los registros y archivos de filiación política, excepto los propios de las autoridades electorales y de los partidos políticos. La legislación más amplia en torno a los datos que recogen las agrupaciones políticas está en España;

donde por ejemplo el Partido Socialista Obrero Español (PSOE) y el Partido de los Socialistas de Cataluña (PSC) acumulan un mayor número de sanciones, seguidos de Ciudadanos y el Partido Popular (PP). En total las multas tramitadas desde 2014 a 2019 corresponden a más de 300 000 euros.

Para el caso de Honduras, el artículo 76 de su *Constitución de la República de Honduras* plantea como inviolables los derechos al honor, a la intimidad personal, familiar y a la propia imagen; asimismo, reconoce la garantía de la *habeas data*, la cual señala: "Toda persona tiene el derecho a acceder a la información sobre sí misma o sus bienes en forma expedita y no onerosa, ya esté contenida en bases de datos, registros públicos o privador y, en caso de que fuera necesario, actualizarla, rectificarla y/o suprimirla" (CRH, 1987 [en línea]).

En Panamá, la legislación aplicable está en la Ley de Transparencia y Acceso a la Información Pública, promulgada en 1972. Al igual que en los otros países, la protección hacia lo datos personales es una aplicación general que requiere un mayor detalle y adaptarse a las exigencias; con el crecimiento de aplicaciones móviles y posibilidades de repositorios de datos e imágenes.

Las leyes a favor de proteger los datos personales

Como se ha descrito anteriormente, existen antecedentes en torno al reconocimiento del derecho a la privacidad y los datos personales de los ciudadanos; pero en América Latina se construyeron recientemente debido a la influencia del derecho comparado europeo. El pasado 28 de mayo de 2018, el *Reglamento General de Protección de Datos de la Unión Europea* entró en vigor. Esto permitió que otros países como Chile, Brasil y Argentina, que no contaban con esta prevención en cuando a derechos humanos, abrieran el debate y pudieran avanzar en torno al tema (BID, 2019).

Existe también el principio de consentimiento, el cual significa que los ciudadanos pueden ser libres de decidir el momento y la forma en la cual pueden ser difundidos sus datos personales. Al respecto, en Brasil, en la reforma de 1985, se introdujo el concepto de *habeas data*, como una nueva garantía constitucional.

En tal sentido, Saltor menciona: "desde su concepción subjetiva o derecho a la autodeterminación informativa, dar amparo al ejercicio del derecho a la intimidad informática y otorga a toda persona el derecho a controlar sus datos personales por medio de una acción procesal concreta, expedita y rápida, que toma la forma de una especie de amparo" (2013: 112).

Antes de la regulación estatal sobre la protección de datos, en Brasil se tuvo el *Código de Protección y Defensa del Consumidor* que otorgaba algunos artículos con derechos de privacidad para acceder y corregir datos del consumidor, así como el tratamiento de datos vía internet. La legislación de julio de 2018 aprobó la Ley General de Protección de Datos Personales de Brasil que impone incluso multas a los empresarios por hasta 2% de sus ingresos brutos en caso de incumplir las disposiciones normativas.

En Chile, la protección de datos se estableció desde 1999, con el propósito de garantizar que los ciudadanos cuenten con protección sobre sus datos, impidiendo que terceros puedan consultar esta información; esto ha generado multas al incumplimiento. En Ecuador, el numeral 19 del artículo 66 de la *Constitución* vigente desde 2008 estipula el derecho a la protección de los datos de carácter personal; sin embargo, al igual que en los otros países anteriormente reseñados, existen lagunas legales y del ámbito institucional que impiden el eficaz cumplimiento de la norma. En la mayoría de los países de América Latina, las empresas de bancos cuentan con datos sobres sus clientes, tienen servicios de *telemarketing* y no está regulado el uso de los datos para ofrecer promociones, encuestas o venta de productos por teléfono. Las empresas pueden contar con una base de datos obtenida legal o ilegalmente sin mayores consecuencias en el ámbito penal.

La venta de bases de datos, por ejemplo, en México se presenta mediante las redes sociales y se ofrece de manera ilegal; produciendo incluso problemas en torno a la seguridad, porque en ocasiones se genera la extorsión telefónica como producto de los datos en manos del crimen organizado. Por lo cual se fractura el estado de derecho y la construcción armoniosa del país.

Los casos presentados ilustran este capítulo, el cual tiene como objetivo garantizar la incidencia social en la reflexión y análisis del tema, plantea, como mecanismo preventivo, el establecimiento de sanciones y multas a quienes incumplen los ordenamientos legales. Por ejemplo, en Colombia, durante 2019, se aplicó sanción

a las empresas Banco Falabella y Rappi, los cuales recibieron la petición de eliminar su número telefónico de su base de datos y dejar de enviar mensajes, esto fue desatendido por el banco. De manera similar, Rappi no protegió los derechos de las personas en el tratamiento de su información, toda vez que se pidió eliminar los registro y dejaran de enviar mensajes para fines comerciales o de *marketing*. En España durante 2017, se multó a una empresa de internet con 5 000 euros, porque utilizaba sin el consentimiento información mediante *cookies*. Es preciso que las páginas proporcionen advertencia a los usuarios sobre la recopilación de información que realizan, para formar clientes y ciudadanos informados. Al respecto, Saltor escribe:

> La acción de *habeas data* se define como el derecho que asiste a toda persona —identificada o identificable— a solicitar judicialmente la exhibición de los registros —públicos o privados— en los cuales están incluidos sus datos personales o los de su grupo familiar, para tomar conocimiento de su exactitud; a requerir la rectificación, la supresión de datos inexactos u obsoleto o que impliquen discriminación. Constituye, en suma, un cauce procesal para salvaguardar la libertad de la persona ante la acumulación y procesamiento informático de sus datos personales (2013: 114).

Sin embargo, el recurso de *habeas data* exige que los ciudadanos sean quienes soliciten o demanden que sus datos sean depuestos o dados de baja de la plataforma o lista de usuarios. Por lo cual, las instituciones garantes del Estado participan de manera marginal o poco activa en la aplicación de la ley.

Fenómenos como la corrupción, el cual se esconde bajo la tutela del derecho a la privacidad y el derecho a la protección familiar, exigen una cabal solución; así como el uso de la base de datos de los ciudadanos para incidir en sus preferencias electorales o promover productos bancarios; lo anterior requiere un análisis pormenorizado de las acciones que se tomarán. En el caso de América Latina, como se señaló anteriormente, las legislaciones para proteger los derechos de tercera generación están en construcción y este capítulo abona a comprender los restos sobre los cuales es preciso trabajar para incidir en el reconocimiento de los derechos y promover la democracia como un mecanismo de protección ante la vulnerabilidad del Estado, los particulares y otros ciudadanos.

Conclusión

Los datos masivos que se encuentran en internet y otras plataformas digitales alertan sobre la importancia de garantizar su protección, porque existe un riesgo en tanto privacidad y protección de datos personales que el Estado debe vigilar, pero no sólo su obtención y tratamiento, sino las posibles consecuencias que deriven del uso de estos datos. Como se describe en el trabajo, existe una amplia debilidad institucional en América Latina, por la normatividad incipiente sobre el tema y porque su uso está vinculado con la investigación de los ciudadanos, sobre sus preferencias electorales y simpatías políticas, vulnerando con ello la frágil democracia de los países.

Las autoridades encargadas de garantizar la protección de datos personales tienen un enorme reto en los países democráticos, porque la intromisión en la privacidad vulnera las libertades consagradas en la *Constitución Política de los Estados Unidos Mexicanos*. Se requiere, por tanto, instituciones sólidas; con autonomía e independencia legal; así como presupuesto para actuar libremente. Por lo anterior, Saltor expone: "es aconsejable la organización de un registro de datos y un sistema de inspecciones eficaz, que cuente con los recursos humanos y técnicos" (2013: 71). Asimismo, con la ampliación de los derechos de tercera generación se pretende en todo momento proteger la dignidad y desarrollo de los ciudadanos, por medio de campañas de difusión y promoción de la cultura para establecer un autocuidado y exigencia del reconocimiento de los derechos a la privacidad y protección de datos.

Durante 2018, se recibieron, por una parte, 1 692 denuncias por mal uso de los datos personales, informó el presidente del INAI (Ramos, 2019); por otra parte, existe una amplia vulnerabilidad de los sistemas financieros, porque de acuerdo con la OEA (2018), 49% de las entidades bancarias aún no están implementando herramientas, controles o procesos; en cambio, están usando tecnologías digitales emergentes, tales como *big data, machine learning* o inteligencia artificial; lo cual supone riesgos para los usuarios y carencia de mecanismos de apoyo y control por parte del gobierno. El robo de identidad es una de las amplias posibilidades que existen en el mal uso de los datos e información de los ciudadanos.

El uso de *big data* está creciendo, la vulnerabilidad de los usuarios de internet está, por tanto, presente en cada una de las aplicaciones que descargan; pero también en las páginas que visitan. Gayo Recio (2017) sostiene que debe incrementarse la protección de los usuarios a los metadatos y la recolección digital que hace internet, pasar de la *privacidad por consentimiento* a la *privacidad por medio de la responsabilidad*. Por ejemplo, las preferencias comerciales dejan una huella digital y pueden conocer nuestro consumo las grandes empresas y tiendas departamentales, por lo que el control hacia los ciudadanos no sólo se encuentra en el gobierno; sino también en la iniciativa privada. El uso de datos recolectados en internet es una constante en las campañas electorales, como por ejemplo en la primera campaña de 2008 de Obama, para la presidencia de Estados Unidos se utilizaron muchos recursos de *big data* para incidir en el electorado.

Barbara Trish (2018) describe el auge en la economía política de los datos, tomando como ejemplo el caso de Obama, ex presidente de Estados Unidos; quien utilizó la información recolectada en las plataformas digitales para promover el voto, pero también para incidir en la agenda pública. La reelección de Obama en 2012 se desarrolló, incluso, con el uso de datos sobre los votantes, sus simpatías y preferencias electorales.

El uso de datos en la red para el sistema bancario tiene áreas de oportunidad, porque

> los usuarios privilegian los medios virtuales sobre los presenciales, lo cual concuerda con el alto grado de digitalización de los servicios y el impulso a la utilización de éstos, ya que el 53% de los encuestados revisa transacciones y saldos usando teléfonos inteligentes más que los que consultan en el banco (29%) o por línea telefónica (23%) e igualmente prefieren transferir fondos a través de Banca Móvil (43%) que trasladándose al banco (37%) (oea, 2018: 12).

Juan Carlos Upegui (2018) sostiene que la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental (lftaipg) tiene elementos controversiales e inconsistentes respecto al fin último de la ley que es promover la transparencia en torno a los gobernantes y sujetos obligados de la función pública, pero a su vez la ley los protege por dos casos: las relaciones de parentesco

y la situación patrimonial. La protección de datos personales, en este sentido, debilita la legislación en torno a la transparencia y rendición de cuentas, porque existen casos documentados de corrupción donde los funcionarios públicos han sido beneficiados por la ley en comento, porque establece lo siguiente: "Toda información en posesión del Estado es pública, salvo los casos de reserva y de confidencialidad" (*DOF*, 2002 [en línea]).

Con este esquema, se antepone el valor de la confidencialidad sobre la publicidad de la información personal y además propone una concepción maximalista en virtud de que plantea que toda información sobre personas físicas, identificables o no identificables tienen resguardo, restricción y exclusión a su consulta por parte de los ciudadanos.

En la discusión sobre la protección de los datos en América Latina, podemos señalar que existen leyes y reglamentos que resguardan el derecho de los ciudadanos para ocultar o evitar que se difundan sus datos o información personal; sin embargo, existe una ausencia de cultura de protección de datos en toda América Latina, y los ciudadanos desconocen cuáles son sus derechos y cómo exigir su cumplimiento. En ese sentido, los retos de la protección de datos personales están en la incidencia social, en el reconocimiento de las ausencias legales y la búsqueda de esquemas para fomentar la denuncia, la participación y la aplicación de la ley. De lo contrario, continuarán las prácticas nocivas en el uso de los datos de los ciudadanos ante la indefensión opuesta a la democracia como sistema de contrapeso y protección a los derechos humanos.

Referencias

Bibliografía

Arroyo Kalis, Juan Ángel (2017). "*Habeas data*: elementos conceptuales para su implementación en México", en Eduardo Ferrer Mac-Gregor y Rogelio Flores Pantoja. *La Constitución y sus garantías. A 100 años de la constitución de Querétaro de 1917*, unam, Ciudad de México.

Doneda, Danilo (2007). *Da privacidade à proteção de dados pessoais*, Renovar, Río de Janeiro.

Goñi Sein, José Luis (2007). *La videovigilancia empresarial y la protección de datos personales*, Cizur Menor (Navarra), Aranzadi.

Hemerografía

Bergareche, Borja (2012). "Umbrales de transparencia en la era wikileaks," *Política Exterior*, vol. 26, núm. 148, julio-agosto, pp. 162-171.

García González, Aristeo (2007). "La protección de datos personales: derecho fundamental del siglo xxi. Un estudio comparado", *Boletín Mexicano de Derecho Comparado*, núm. 120, pp. 743-778, unam, Ciudad de México.

Gobierno de México (2002). "Ley de Transparencia y Acceso a la Información Pública Gubernamental", *Diario Oficial de la Federación*, 11 de junio de 2002.

Herrán Ortiz, Ana Isabel (2003). "El derecho a la protección de datos en la sociedad de información", *Cuadernos Deusto de Derechos Humanos*, núm. 26, Bilbao, Universidad de Deusto.

Recio Gayo, Miguel (2017). "*Big data*: hacia la protección de datos personales basada en una transparencia y responsabilidades aumentadas", *Revista de Derecho Comunicaciones y Nuevas Tecnologías*, núm. 17, enero-junio.

Upegui Mejía, Juan Carlos (2018). "Posible relación entre corrupción y protección de datos personales en México", *Revista de la Facultad de Derecho de México*, t. lxviii, núm. 271, mayo-agosto de 2018.

Mesografía

Arteaga Botello, Nelson (2016). "Regulación de la videovigilancia en México. Gestión de la ciudadanía y acceso a la ciudad", *Espiral*, vol. xxiii, núm. 66, mayo-agosto, [en línea]. Disponible en http://www.scielo.org.mx/pdf/espiral/v23n66/1665-0565-espiral-23-66-00193.pdf, consultado el 1 de junio de 2019.

Aroche Aguilar, Ernesto y Karen de la Torre (2019). "El juez que no debió serlo", [en línea]. Disponible en https://ladobe.com.mx/2019/06/el-juez-que-no-debio-serlo/, consultado el 1 de junio de 2019.

Bid, Banco Interamericano de Desarrollo (2019). "Competitividad porturia en América Latina y el Caribe: un análisis de la regulación, gobernanza y competencia en el sector portuario de la región" [en línea]. Disponible en https://publications.iadb.org/es/competitividad-portuaria-en-america-latina-y-el-caribe-un-analisis-de-la-regulacion-gobernanza-y, consultado el 23 de mayo de 2019.

Bojalil, Paulina y Carlos Vela Treviño (2019). "Despuntan las reformas en materia de protección de datos en América Latina", [en línea]. Disponible en https://blogs.iadb.org/conocimiento-abierto/es/proteccion-de-datos-gdpr-america-latina/, consultado el 1 de junio de 2019.

Diario Oficial de la Unión Europea (2016). *Reglamento General de Protección de Datos*, 2016/679 del Parlamento Europeo y del Consejo, 27 de abril de 2016 [en línea]. Disponible en https://www.boe.es/doue/2016/119/L00001-00088.pdf, consultado el 10 de noviembre de 2019.

Dorado, José María y Jesús Fernández Herrera (2006). "La protección de datos en la práctica privada", *Actas Dermo-Sifiliográficas*, vol. 97, núm. 1, pp. 18-30. Disponible en https://www.sciencedirect.com/science/article/abs/pii/S0001731006733439, consultado el 1 de junio de 2019.

ftd, Federal Trade Commision (2012). "Protecting consumer privacy in an era of rapid change", [en línea]. Disponible en https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf, consultado el 14 de noviembre de 2017.

Gobierno de Guatemala (2019). *Constitución Política de la República de Guatemala* (1985), [en línea]. Disponible en https://www.minfin.gob.gt/images/downloads/dcp_marcolegal/bases_legales/Constitucion_politica_de_la_republica_de_guatemala.pdf, consultado el 9 de marzo de 2019.

infocdmx, Instituto de Acceso a la Información Pública y Protección de Datos Personales de la Ciudad de México (2011). *Retos de la protección de datos personales en el sector público*. [en línea]. Disponible en http://www.infodf.org.mx/, consultado el 13 de febrero de 2019.

Jourova, Vera (2018). "Proteger los datos es proteger la democracia", *El País*, 28 de marzo de 2018, [en línea]. Disponible en https://elpais.com/elpais/2018/03/27/opinion/1522154135_052349.html, consultado el 12 de mayo de 2019.

Laurent, Cédric *et al.* (2018). "Datos personales e influencia política. Investigación sobre las estrategias digitales del PRI en cuatro de sus campañas electorales recientes en México", [en línea]. Disponible en https://sontusdatos.org/wp-content/uploads/2018/07/180629-a12-datos_personales_e_influencia_politica-vf.pdf, consultado el 18 de junio de 2019.

Morga, Katherine (2012). "Data privacy and the foreign corrupt practices act: a study of enforcement and its effect on corporate compliance in the age of global regulation" [en línea]. Disponible en https://scholarship.law.edu/commlaw/vol20/iss2/8/, consultado el 18 de junio de 2019.

oea, Organización de Estados Americanos (2018). "Estudio comparativo: protección de datos en las Américas", [en línea]. Disponible en http://www.oas.org/es/sla/ddi/docs/CP-CAJP-3063-12.pdf, consultado el 18 de junio de 2019.

_____ (2016). "Estado de la ciberseguridad en el sector bancario en América Latina y el Caribe", [en línea]. Disponible en https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf, consultado el 19 de mayo de 2019.

Ramos, Rolando (2019). "Inai recibió 1 692 denuncias por uso de datos personales en 2018", *El Economista*, 28 de febrero de 2019, [en línea]. Disponible en https://www.eleconomista.com.mx/politica/INAI-recibio-1692-denuncias-por-uso-de-datos-personales-en-2018-20190228-0115.html, consultado el 8 de mayo de 2019.

Saltor, Carlos E. (2013). *La protección de datos personales: estudio comparativo Europa-América con especial análisis de la situación argentina*, memoria para optar al grado de doctor en Derecho por la Universidad Complutense de Madrid, España, [en línea]. Disponible en https://eprints.ucm.es/22832/1/T34731.pdf, consultado el 8 de mayo de 2019.

Salvatierra, Sarahí y Janet Oropeza (2018). "Corrupción y transparencia: inconsistencias del Inai", [en línea]. Disponible en https://www.animalpolitico.com/res-publica/corrupcion-y-transparencia-las-inconsistencias-del-inai/, consultado el 1 de octubre de 2018.

Trish, Barbara (2018). "Big data under Obama and Trump: the data-fueled u.s. presidency", *Politics and Gobernance*, vol. 6, núm. 4, pp. 29-38, [en línea]. Disponible en https://www.cogitatiopress.com/politicsandgovernance/article/view/1565, consultado el 23 de mayo de 2019.

III

PRIVACIDAD E IDENTIDAD A DEBATE. ¿UNA DISYUNTIVA EN MÉXICO?

José Javier Niño Martínez

Introducción: el ascenso de una sociedad de datos

La consolidación del marco de derechos democráticos es fundamental para alimentar las posibilidades de participación ciudadana en un marco de legitimidad del Estado moderno; de esta manera, las libertades sociales se definen como elemento fundamental para comprender las posibilidades del ejercicio ciudadano, pero sobre todo incrementan distintas líneas de acción en las que los individuos inciden en su entorno político y social.

La revisión del funcionamiento de las democracias, por un lado, suele enfatizar la importancia de las elecciones periódicas, competidas y confiables como criterio fundamental en su diagnóstico; sin embargo, hay que reconocer que no basta con que haya posibilidades de emitir sufragios como una finalidad absoluta, ya que para que esto pueda suceder es indispensable que los ciudadanos dispongan de libertades específicas (votar y ser votado, asociación y de imprenta) con el fin de que el proceso de elegir represente una expresión ajena a distintos mecanismos coercitivos que condicionen el voto.

Por otro lado, hay que señalar que el debate acerca de los medios jurídicos que consoliden un marco de protección respeto a la privacidad en México es un tanto difuso, al menos en la carta magna; sin embargo, el artículo 16 de la *Constitución Política de los Estados Unidos Mexicanos* (en adelante CPEUM) establece: "Nadie debe ser molestado en su persona, familia, domicilio, papeles o posesiones", así como mantener el control de la publicidad de su información personal (persona, familia, pensamientos o sentimientos). Le corresponde al Estado velar el respeto de este derecho y establecer los medios para que no se vulnere de modo alguno el principio de respeto a la vida privada de las personas. Hay que señalar que el citado

artículo también establece las condiciones de excepcionalidad de la protección de la privacidad, ya sea en caso de temas de seguridad nacional, así como asuntos de seguridad ciudadana, salud pública o para proteger los derechos de terceros. Estos preceptos fueron introducidos en la carta magna en 2009. Vale la pena enfatizar que el derecho a la privacidad en nuestro país no sólo compete a la potestad de no ser molestado en la vida privada, sino también a la esfera de la autodeterminación del uso de la información, es decir, la capacidad de cada individuo de autorizar o negar el uso de sus datos a empresas privadas o instancias de gobierno, por lo que "el objetivo de la protección de los datos personales puede ser resguardar la intimidad de la persona, su tranquilidad y la no perturbación de su espacio de reserva, que es el espacio de libertad. La persona decide con quién compartir esta información" (Ferreira, 2016: 33).

En el marco de profundos cambios de la organización social, cuyo origen podemos rastrear en el avance tecnológico y la construcción de profundos debates acerca de los derechos humanos, es necesario plantearse las siguientes preguntas: ¿cuáles son los alcances y limitaciones del derecho a la privacidad en México?, ¿su ejercicio es contemplado por la normatividad y las instituciones mexicanas?, ¿cuáles son las expectativas inmediatas que tenemos en la actualidad?

Si bien es difícil plantearse un panorama concluyente sobre estas cuestiones, sobre todo debido a que la agenda en la que se inscribe este asunto en la actualidad no ha sido analizada con decisión por los actores relevantes sobre el tema, es pertinente cimentar la discusión en la arena académica, con el fin de construir un panorama claro para disponer de los elementos adecuados para eventualmente tomar decisiones en beneficio de la sociedad mexicana.

La sociedad actual se caracteriza por el ascenso de la importancia de los datos como elementos formativos de los vínculos sociales. Más que nunca se entiende la relación entre sujetos por medio de los códigos y la información que generamos por medio de registros de todo tipo, ya sea mercantiles, información oficial, antecedentes criminales, entre otros. La frontera público-privada se envuelve en un marco difícil de establecer, más aún si la información adquiere la capacidad de fluir a receptores sin el control de las fuentes de datos, en este caso los individuos.

Existen varias condiciones que sustentan este cambio, entre las que podemos enunciar a las siguientes:

- Desarrollo de tecnologías de almacenamiento de datos (capacidad y sistematización de la información). Esto ha sido posible gracias a la miniaturización de los dispositivos de almacenamiento y posteriormente al desarrollo de mecanismos de portabilidad de los datos. Como consecuencia de estos avances, se facilitó el tratamiento y sistematización de datos pasando de inmanejables archivos impresos que ocupaban amplios espacios físicos para su almacenamiento a archivos digitales capaces de ser almacenados en unidades portátiles e incluso disponibles en medios virtuales como la nube.
- Capacidad de difusión de la información. Desarrollo de medios de transmisión de información casi inmediata, que sustituyeron al correo o a la paquetería tradicional por correo electrónico, videollamadas o redes sociales. La información que podría tardar días o semanas en darse a conocer encuentra ahora diferentes medios de difusión con una mayor agilidad.
- Desarrollo de capacidades de control. La sistematización y posibilidad de intercambiar datos hace posible que el control sea más factible, registros policiacos o información sensible para ingresar a otro país cobran relevancia en un entorno en el que las migraciones son más comunes.

Ante este entorno, la narrativa vigente puede ser analizada por medio de dos matrices fundamentales:

- La intervención del mercado en la definición del estilo de vida y las acciones de los individuos (la sociedad del consumo).
- La acción del Estado para minimizar riesgos de la integridad de las personas y sus bienes (la sociedad de la seguridad).

En ambos casos, el desarrollo de procesos de innovación tecnológica, por un lado, ha sido un proceso revolucionario que, por lo tanto, ha tenido un efecto transformador de las instituciones de la sociedad, lo cual es posible observar en el diseño de un mercado más flexible y adaptable a las necesidades de los consumidores; las políticas de seguridad globalizan la prevención de amenazas a la seguridad nacional e individual por medio de dispositivos de vigilancia.

Por otro lado, la sociedad de datos encuentra su distintivo en las nuevas formas de construcción de la identidad como principio organizativo, entendiendo por identidad "el proceso mediante el cual un actor social se reconoce a sí mismo y construye el significado en virtud sobre todo de un atributo o atributos culturales determinados, con la exclusión de una referencia más amplia a otras estructuras sociales" (Castells, 2006: 48); en este sentido, la identidad es consecuencia de la modernización de los vínculos individuales con estructuras sociales y económicas en los términos de consumo y seguridad que se aludieron previamente, en todo caso, el entorno es definido por la incertidumbre y el riesgo, en los términos que plantea Ulrich Beck (1998).

El ascenso de los desarrollos tecnológicos permite una mayor capacidad de registro tanto a las empresas como a los gobiernos, se establece el tránsito de los archivos impresos a la información encriptada en chips o en algunos casos disponible en línea. En este sentido, mientras que Erving Goffman (2006) pone énfasis en la estigmatización como un mecanismo de clasificación social; por su parte David Lyon (2006) se concentra en la vigilancia como instrumento de consolidación del panóptico al que aludía Michel Foucault, pero considerando que el proceso de observación de la vigilancia no se concentra en la observación de los cuerpos de los sujetos, sino que la capacidad de observación se define por el acceso a la información con que se identifica la personalidad de los sujetos, entendida como parte del reconocimiento biométrico único para cada quien. El panóptico, en este sentido, es una expresión de poder con carácter disciplinar, ya que puede ser el vehículo de sanciones con una política de control extensiva por medio de la información de la sociedad en general.

El control con base en la observación se extiende en contextos virtuales, acrecentando su eficiencia gracias al registro y sistematización de información de los individuos, rompiendo con la barrera de la observación directa y fomentando la importancia de bases de datos. Poder es sinónimo de datos y, de cierta manera, es la nueva expresión del riesgo social, entonces ¿sabemos quién tiene nuestra información?, ¿sabemos qué información privada se encuentra en bases de datos del gobierno o de empresas privadas como los bancos o redes sociales?

Las esferas de la libertad

Retomando a Giovanni Sartori (2015), la libertad es el mecanismo de protección del ciudadano ante la opresión del poder; en este aspecto, podemos sugerir que una de las fuentes de la libertad es la privacidad, entendida como el respeto del orden político y de particulares respecto a información privada de los individuos u organizaciones; en este sentido, el marco jurídico mexicano, por una parte, es congruente con el enfoque de la mayoría de las democracias occidentales, ya que toma como punto de partida "el derecho a no ser molestado", aunque por otra hay que señalar que la *CPEUM* hace alusión a la protección de datos personales y al acceso a la información y de igual manera establece el marco general de las instituciones avocadas al tema; sin embargo, esta enmienda se ha extendido en dos esferas:

- La relación Estado-ciudadano, el reconocimiento de la identidad entendida como un derecho ciudadano, por un lado, implica la recopilación de información individual para prevenir delitos como la suplantación de identidad y al mismo tiempo puede constituir una herramienta efectiva para garantizar la distribución de apoyos gubernamentales. Por otro lado, el disponer de información de este tipo le permite al Estado disponer de medios útiles durante contingencias como desastres naturales, epidemias u otro tipo de políticas de bienestar.
- La relación empresa-ciudadano consiste en la información que las distintas empresas u organismos financieros particulares acreditan y que eventualmente comparten con otras empresas, esta información puede ser utilizada con fines publicitarios o incluso de cobranza.

En ambos casos, el respeto del derecho a la privacidad se puede entender como la atribución que tiene el ciudadano para definir los usos con que se utiliza su información personal, los medios por los cuales se difunde y sobre todo los fines para los que se usa, lo cual resalta el hecho de que se apela a la autodeterminación respecto de los datos de las personas; en otras palabras, no se autoriza el uso de dicha información sin el conocimiento previo y autorización correspondiente de la fuente de la información. En teoría, el marco legal básicamente debe establecer las reglas de esta autodeterminación, las cuales deben ser válidas tanto para el aparato estatal como para los agentes de mercado.

En el caso de México, se cuenta con un marco general brindado por la *CPEUM* que garantiza ciertas protecciones individuales principalmente en la esfera Estado-ciudadano. El artículo 16 constitucional es claro respecto a la protección de los datos personales de los mexicanos, así como de la inviolabilidad de las comunicaciones privadas, con las excepciones señaladas por la propia ley que fueron enunciadas previamente. Aunado con esto, el marco legal mexicano contempla la existencia de leyes específicas como la Ley Federal de Protección de Datos Personales en Posesión de Particulares (vigente desde el 6 de julio de 2010) y Ley General de Transparencia y Acceso a la Información Pública (vigente a partir del 5 de mayo de 2015), que se articulan con la acción del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) como el ámbito por medio del que se ubica la respuesta del Estado al respeto al derecho a la privacidad.

Un par de problemas

El primero:

En octubre de 2018, el Instituto Nacional Electoral (INE) denunció ante la Fiscalía Especializada para Atención de Delitos Electorales (Fepade) la venta del padrón electoral en internet, el cual específicamente se encontraba disponible en la plataforma YouTube. Este acto constituye un delito electoral que afecta de manera importante la credibilidad de la institución electoral en lo que se refiere al manejo de información privada de los ciudadanos mexicanos. De igual manera, esta noticia es grave en virtud de las siguientes condiciones:

La magnitud de la información: debido a que en México se carece de una cédula de identidad ciudadana, la credencial de elector se ha convertido *de facto* en el medio de identificación con el que cuentan los ciudadanos; por ello, el número de personas inscritas en el padrón electoral es cercano a 90 millones de personas (89 millones 332 mil 31) (INE, 2018), cifra superior a cada uno de los países de Europa, excepto Rusia; mayor que cada país de América, excepto Estados Unidos y Brasil. Como se puede observar, la mayoría de los mexicanos mayores de 18 años han solicitado su inscripción el padrón electoral y la disponibilidad indebida de esa información puede tener un amplio efecto en la población mexicana.

El tipo de información: como resultado de los altos estándares de seguridad que se hacen necesarios en el registro de los ciudadanos, el INE recaba no sólo información personal (nombre, dirección, código postal, sexo, clave de elector, municipio, localidad), sino que también se obtienen datos biométricos (fotografía y huellas dactilares) para garantizar la no duplicidad del registro. Dichos datos representan información muy sensible.

En suma, este caso mostró la vulnerabilidad de la información de los ciudadanos en manos de las instituciones públicas en México (en este caso la electoral), aunque ya habían existido antecedentes de este tipo en 2003, cuando se hizo del conocimiento público que la empresa Choice Point había adquirido la base de datos del padrón electoral; de igual manera, en 2009 y 2014, se puso a la venta el listado en sitios de comercio en línea y al parecer las medidas de las autoridades electorales no fueron suficientes para evitar que se repitiera el caso en 2016 y 2017.

Ante esta situación, ¿cuál es el riesgo que enfrentan los ciudadanos cuando las instancias que recaban y resguardan información de identidad no son capaces de protegerla de manera eficiente?, ¿cómo establecer las distintas pautas de responsabilidad y prevención para que estos casos no se repitan?

Hay que recordar que debido a que en México el gobierno no ha podido implementar con éxito el registro de los ciudadanos por medio de una cédula de identidad, la credencial para votar representa el documento más utilizado para realizar trámites gubernamentales y financieros (se requiere para inscribir a los hijos a la escuela, pagar algunos servicios públicos, abrir una cuenta en el banco o retirar dinero de la ventanilla bancaria), para obtener dicha credencial el ciudadano debe acudir al INE e inscribirse en el padrón electoral, para lo cual debe otorgar información personal y biométrica. Cabe señalar que el INE es un organismo autónomo del Estado mexicano y, por lo tanto, el gobierno no es depositario directo de la información registrada; en ese sentido, el INE ha manifestado en reiteradas ocasiones su rechazo a la emisión de una cédula de identidad ciudadana, debido a que al existir otro documento de identificación diferente a la credencial de elector, se teme que se reduzca el incentivo para registrarse en el padrón, afectando la participación ciudadana en los procesos electorales.

Otra polémica paralela fue la sentencia emitida por el Tribunal Electoral del Poder Judicial de la Federación (Trife) respecto a la autorización expresa del

ciudadano para que aparezca su dirección en la credencial o que se presente el dato de manera encriptada. Esta resolución tomó en cuenta que el documento cumple con dos funciones, ya sea como medio de identificación a falta de una cédula de identidad ciudadana, lo cual facilita su uso para la realización de trámites o como instrumento necesario para poder participar en los comicios. Sin embargo, la dirección es un dato personal sensible, cuya difusión es susceptible de ser negada por las personas; aunado con esto, ya se dispone de tecnología pertinente para interpretar la codificación, ya sea por bancos o instancias gubernamentales. En consecuencia, la resolución indicó que corresponde al ciudadano la elección sobre la visibilidad de esta información en la credencial. Cabe señalar que la gran mayoría de las personas ha preferido que se encuentre visible este dato (Ferreira, 2016). También hay que recordar que en otras resoluciones el Trife también ha impuesto multas significativas a los partidos políticos, ya que siendo su derecho el tener acceso al padrón electoral, han incumplido con el resguardo de la información y es por ese motivo que en otras ocasiones, ésta ha terminado en el mercado negro.

El segundo:

El delito de robo de identidad se tipifica "cuando una persona obtiene, transfiere, posee o utiliza de manera no autorizada datos personales de alguien más, con la intención de asumir de manera apócrifa su identidad y realizar compras, obtener créditos, documentos o cualquier otro beneficio financiero en detrimento de sus finanzas" (Amigón, 2015 [en línea]). Tomando esto en consideración, según datos de la Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros (Condusef), el crecimiento del delito de robo o suplantación de identidad[1] ha ido en ascenso en años recientes, principalmente por la adquisición de créditos a nombre de otra persona o por medio de la realización de compras en línea adjudicando el saldo a la cuenta de un tercero. El crecimiento de este delito, por un lado, se observa sistemáticamente desde 2015, año en que las reclamaciones imputables a un posible robo de identidad se incrementaron 40% con respecto

[1] Los datos personales constituyen la identidad: nombre, teléfono, domicilio, fotografías, huellas dactilares, números de licencia y de seguridad social, incluyendo información financiera o médica, así como cualquier otro dato que permita identificar a una persona.

al mismo periodo de 2014, al pasar de 20 168 a 28 258. Por otro lado, sobre "el monto reclamado por los usuarios, en el primer semestre del año ascendió a 118 millones de pesos, 19% más a lo reclamado en el mismo periodo de 2014 y de este monto el saldo abonado fue de 69 millones de pesos, es decir, 58%. Los bancos que concentran el mayor número de reclamaciones por esta causa son Santander, Banamex y HSBC", (*Forbes*, 2015 [en línea]), los cuales registran 76% del total de reportes.

En el referente internacional, también se observa un significativo crecimiento del delito en México, ya que "nuestro país ocupa el octavo lugar a nivel mundial en este delito; en un 67% de los casos, el robo de identidad se da por la pérdida de documentos, 63% por el robo de carteras y portafolios, y 53% por información tomada directamente de una tarjeta bancaria" (Amigón, 2015 [en línea]).

Ante la gravedad del problema, las autoridades mexicanas han implementado una serie de estrategias con el fin de atender a las múltiples denuncias, poniendo en primer lugar la necesidad de brindar certeza jurídica a los usuarios de servicios financieros por medio de la garantía del derecho a la identidad.

La *CPEUM* establece que es obligación del Estado acreditar la identidad de los ciudadanos mexicanos; por lo tanto, es un derecho disponer de los medios que permitan hacer uso de éste. Así, la disponibilidad de medios de identificación impedirá que exista una apropiación indebida de la personalidad financiera de terceros y que se realicen fraudes o delitos financieros responsabilizando a personas inocentes. Otra justificación es que un medio de identidad eficiente permitirá el acceso a servicios del Estado (salud y programas sociales) en mejores condiciones para los ciudadanos que así lo necesiten.

En este sentido, se pueden establecer las siguientes preguntas: ¿qué medios legales permiten al ciudadano monitorear el uso que el Estado da a los datos que recaba para acreditar su identidad?, ¿cuál es la ruta que deben seguir las instituciones para preservar las garantías individuales al hacer uso de la información de la población?

Los dos casos mencionados se ven envueltos en la disyuntiva entre el derecho a la identidad y el derecho a la privacidad, ya que cada uno constituye un bien jurídico establecido constitucionalmente, pero que por un lado permite acreditar la personalidad jurídica y financiera de los individuos; por otro, busca limitar la

injerencia externa en información disponible de los ciudadanos; sobre todo hay que resaltar la capacidad de autodeterminación de las personas para autorizar el uso de sus datos ya sea con fines comerciales o de seguridad.

El derecho a la identidad garantiza la personalidad jurídica de alguien y al mismo tiempo permite definir sus derechos y obligaciones en un marco legal nacional e internacional; de igual manera, dispone de derechos brindados por el Estado como la educación y la salud. Al mismo tiempo, deja que el individuo disponga de acceso a información de su interés exclusivo a información sensible (cuentas de bancos, datos médicos, entre otros). Es un derecho que el Estado le garantiza a sus ciudadanos, con el fin de que puedan hacer uso de servicios públicos, disponer de los medios legales para tener una personalidad jurídica y tener acceso a medios financieros; esto da cuenta de la existencia de una persona por medio del reconocimiento jurídico que le permite tener nombre y apellidos, nacionalidad, ser inscrito en un registro público y al mismo tiempo la posibilidad de formar parte de una colectividad que tiene como punto de partida la familia.[2] Un ejemplo es el reconocimiento jurídico de los hijos, el cual brinda protección no sólo al menor, sino también a la madre en caso de separación de los padres o acceso a programas sociales.

Por un lado, podemos afirmar que la privacidad trasciende la naturaleza de las normas legales, pues se puede considerar al mismo tiempo como un elemento de control de la acción del Estado y del mercado, en la medida en que la autodeterminación del sujeto implica una barrera de la acción arbitraria del gobierno y del capitalismo. La violación a la privacidad por parte del Estado implica el resquebrajamiento de los principios liberales de las democracias contemporáneas, y por parte del mercado refleja el riesgo de la inexistencia de controles para que el mercado se ciña a las leyes.

Por otro lado, el tipo de régimen define lo que hace el Estado con la información de los ciudadanos, no se trata de que éste no disponga de información ciudadana, de hecho existen experiencias en las que la información es muy útil (en caso de desastres naturales, para dar seguimiento en una pandemia y promover

[2] En estos términos se ha expresado la Convención sobre los Derechos del Niño y de la Niña, en sus artículos 7 y 8.

la vacunación-servicios de salud, combate al crimen como extorsiones o robo de identidad). Se debe disponer de un instrumental que permita a los ciudadanos tener incertidumbre respecto a lo que las autoridades hacen con su información, la garantía de ésta no será utilizada con fines no autorizados por el ciudadano.

Registro y privacidad en México: entre el control y el derecho

El proceso histórico acerca de la existencia de un sistema de registro ciudadano controlado por el Estado nos expone dos visiones alrededor de un mismo problema:

- La información puede ser utilizada con fines de vigilancia y control social usando las herramientas del Estado y de la información por medio de la cual tiene acceso.
- Un manejo adecuado de información puede garantizar de manera más eficiente y digna el derecho a la identidad de cada ciudadano.

En todo caso, es polémico el tratamiento que históricamente el gobierno mexicano ha dado a la información de los ciudadanos, para lo cual se expondrán dos experiencias relativamente recientes, que en la práctica han sido fracasos rotundos como se verá a continuación:

El Registro Nacional de Usuarios de Telefonía Móvil (Renaut) fue un proyecto del gobierno mexicano que consistía en elaborar un registro de usuarios de teléfonos móviles de abril de 2009 a abril de 2010; con este fin, el proceso de registro asociaba la línea telefónica con la Clave Única de Registro de Población (CURP). Todo esto con la finalidad de combatir extorsiones y fraudes telefónicos, que ya para entonces se habían convertido en delitos con una alta incidencia. En el momento en que se comenzó a implementar el proceso de registro existían aproximadamente 98 millones de líneas telefónicas disponibles. A pesar de la campaña intensiva por promover el registro de los usuarios, el proyecto fracasó principalmente porque se encontró evidencia de un gran número de registros duplicados y también un número muy alto de registros con nombres falsos; en gran medida, debido a la fragilidad del control del procedimiento y sobre todo a la poca disposición de las principales compañías telefónicas. En 2011, se abrogó la iniciativa y se procedió a destruir las copias de toda la información.

El Registro Nacional Vehicular (Renave) buscaba ser una base de datos de todos los vehículos automotores del país, a cargo de la Secretaría de Seguridad Pública, con el objetivo de consultar la situación jurídica de cualquier automóvil, acceso y registro de manera gratuita para el usuario. El sistema de consulta no permitía tener acceso a los datos personales en el registro (sujeto obligado) excepto el propietario; posterior al registro del vehículo, se integraba una calcomanía infalsificable en el parabrisas de éste, lo cual daba cuenta de la finalización del trámite. Hay que señalar que existieron experiencias previas en registros de este tipo en 1977 con el Registro Nacional de Vehículos y el Registro Público Vehicular que entró en vigencia en 2008. El fracaso del Renave se debió a que el entonces responsable del programa, Ricardo Cavallo, fue detenido por cometer crímenes de lesa humanidad cometidos durante la dictadura argentina (1976-1983). Como consecuencia de esta situación, el programa fue abandonado y retomado más adelante con estándares diferentes.

Aunado con lo anterior, hay que mencionar que en nuestro país existen diferentes mecanismos de identificación como los siguientes:

- Cartilla del servicio militar. Emitida por la Secretaría de la Defensa Nacional (Sedena), no es muy extensiva debido a que a pesar de su obligatoriedad para los varones, no lo es para las mujeres; por tanto, no tiene validez para la realización de trámites.
- Registro Federal de Contribuyentes (RFC), registro a cargo de la Secretaría de Hacienda. Su principal limitación es que se circunscribe a los ciudadanos que pagan impuestos.
- Credencial de elector. Emitida por el INE, es el instrumento de identificación más común y confiable, normalmente se utiliza para todos los trámites que el ciudadano requiere hacer.
- Clave Única de Registro de Población (CURP). Se encuentra bajo la responsabilidad del Registro Nacional de Población, que a su vez forma parte de la Secretaría de Gobernación.

Tomando en cuenta lo anterior, no es una novedad que exista un registro de información de los ciudadanos mexicanos en manos del gobierno o de otras instancias como el INE, hecho que se fundamenta en el artículo 4º constitucional, que señala que toda persona tiene derecho a la identidad y a ser registrado de

manera inmediata a su nacimiento. Respaldándose en este fundamento legal, en 2009, el gobierno federal, encabezado por Felipe Calderón Hinojosa, presentó un proyecto de recopilación de información por medio de la emisión de una cédula de identidad ciudadana, con la cual se obtendrían y sistematizarían datos personales y biométricos de la población mayor de 18 años. Esto se dio con el Acuerdo Nacional por la Seguridad que se promovió durante su administración.

El Registro Nacional de Población encuentra fundamento en la Ley General de Población (vigente desde 2014) y el reglamento respectivo, en cuyo artículo 85 se establece expresamente que corresponde a la Secretaría de Gobernación registrar y acreditar la identidad de todos los residentes en el país, así como de los mexicanos en el extranjero (artículos 86, 87 y 88), aunque hay que reconocer que en el artículo 91 de la citada ley se define que la incorporación del registro personal se realiza por medio de la CURP.

La misma normatividad vigente es clara en el capítulo 7º (artículos 97-112), en donde se establece la responsabilidad de la Secretaría de Gobernación en la emisión de la cédula de identidad ciudadana, así como la obligatoriedad de los ciudadanos para obtenerla. También se enuncian los procedimientos del trámite y su importancia como medio de identificación, además se establece la no obligatoriedad a portarla en todo momento.

La propuesta de expedición de cédula de 2009 sobrepasaba los criterios señalados en la normatividad, recabando información sobre huellas dactilares, iris de los ojos e imagen del rostro; de igual manera, incluía el uso de banda magnética y señalaba el tipo de sangre del titular, ya que los únicos datos biométricos que indica la ley es la huella dactilar. El argumento metajurídico para la emisión de este documento de identidad consistió en brindar seguridad a los ciudadanos, pero también para agilizar sus trámites y acceso a servicios y programas sociales.

La propuesta del gobierno de Felipe Calderón enfrentó una significativa resistencia por parte de los partidos políticos de izquierda con el argumento de que se dotaba de facultades a la Secretaría de Gobernación que eventualmente le permitirían construir un "Estado policiaco" con atribuciones y capacidades de vigilancia sobre los ciudadanos. Sin embargo, esta no es la única razón por la que resultaba cuestionable la propuesta, ya que además había que considerar los riesgos que implica el manejo de la información concerniente a una persona

física identificada o identificable si no se dispone de los medios adecuados para su resguardo como se verá más adelante, esto debido a la posible existencia de datos que afecten a la esfera más íntima de su titular o que conlleven discriminación de cualquier tipo o riesgos a su seguridad.

El problema anterior fue medianamente atendido por la legislación de protección de datos personales, la cual se concentró en el derecho a decidir qué información se hace pública y cuál permanece en la esfera privada. Sin embargo, quedó en el limbo el diagnóstico de los peligros de fomentar a vigilancia estatal, pues al no tener un control adecuado de las instituciones políticas, se utilizó sólo la información recabada.

Si bien la propuesta de Felipe Calderón no prosperó, tampoco representó el punto final del proyecto de registro, ya que el tema se retomó durante el inicio de la presidencia de Enrique Peña Nieto. A finales de 2012, se firmó en el Castillo de Chapultepec el Pacto por México, que no era otra cosa que un acuerdo político entre las principales fuerzas políticas del país en ese momento (PRI, PAN, PRD), con el fin de impulsar proyectos de desarrollo tanto en el ámbito económico como en la política social y de seguridad. Atendiendo a este interés en común, entre los compromisos se encontraba uno que establecía lo siguiente: se analizaría la creación de la cédula de identidad ciudadana, aclarando que el documento no tendría un uso político o electoral. A pesar de la disposición de los partidos políticos firmantes, el gobierno en funciones no pudo impulsar la cédula, quedando nuevamente interrumpido el proyecto.

Ante tantos obstáculos en la implementación de esta norma legal es posible preguntarse si existen causas suficientes para desconfiar del uso que las instituciones políticas mexicanas puedan dar a la información. En este sentido, una de las objeciones más fuertes encuentra sustento en el hecho de considerar que el Estado mexicano espía como una práctica más o menos cotidiana y para muestra un botón:

En 2017 se dio a conocer la adquisición y uso del software espía Pegasus (*The New York Times*), por medio de la Secretaría de la Defensa Nacional (Sedena), Procuraduría General de la Republica (PGR) y el Centro de Información y Seguridad Nacional (Cisen), con el fin de obtener información de los dispositivos móviles de periodistas, activistas sociales y defensores de derechos humanos.

La Red en Defensa de los Derechos Digitales (R3D), en colaboración con el Citizen Lab de la Universidad de Toronto, acreditó el uso del software en más de 100 intentos,

cuya venta se reserva a los gobiernos de distintos países (no se vende a particulares), con el fin de combatir prácticas terroristas; sin embargo, el hecho documentado en México nos indica que existe un patrón de vigilancia sistemática por parte del gobierno y que el objetivo de dicha práctica no son criminales ni terroristas, sino activistas sociales y periodistas. La utilización de estos instrumentos de espionaje no se orientó en evaluar y reaccionar hacia alguna amenaza de seguridad nacional; en cambio, se realizó con la intención de utilizar información con fines no claros, ya que no se sabe si la información obtenida podía usarse con fines represivos (Gómez, 2017).

Con este antecedente, se dejó evidencia de que el gobierno mexicano tiene la capacidad y la voluntad de recabar información privada de los ciudadanos, ya que el software tiene la capacidad de infiltrarse en los dispositivos móviles mediante notificaciones falsas (*Short Message Service*: SMS, Servicio de Mensajes Cortos) y tener acceso a llamadas, mensajes y archivos, así como controlar cámara y micrófono del dispositivo telefónico.

La respuesta inicial del gobierno mexicano consistió en negar que las autoridades federales fueran responsables de este uso discrecional; de esta manera, se invitó a los perjudicados a interponer la denuncia correspondiente ante la PGR, pues posiblemente una de las instancias gubernamentales que adquirió el software, por lo tanto, fue responsable de realizar el acto de espionaje, así la PGR se convertiría en juez y parte de la investigación.

Este caso visualizó el control y abuso de poder que se generan debido a la ausencia de mecanismos de control del espionaje público, ya que, por un lado, si bien hay una ley que busca proteger la información y datos personales; por otro lado, también existe una zona opaca de las funciones de seguridad que eventualmente puede traducirse en intimidación a actores estratégicos en temas sensibles para el gobierno en turno, lo cual representa una violación flagrante a las libertades democráticas.

De igual manera, se pudo observar que vivimos en una época en la que existe una transformación de las instituciones tradicionales de control en los términos de la vigilancia, ya no orientadas hacia la reclusión, ya que basta con disponer de información estratégica para disponer de medios de amenaza a la disidencia o a sectores críticos, coartando libertades por medio de datos cautivos, ésa es la nueva forma de control social, incluso en las democracias (Bogard, 2007).

Conclusión

La coerción en el mundo moderno ha adquirido diferentes matices respecto a tiempos pasados, pasando del encarcelamiento a las condiciones inmateriales o virtuales de control, recurriendo al registro como mecanismo de consolidación de una nueva sociedad disciplinaria, a diferencia de lo que plantea Foucault, la vigilancia no se dirige a los cuerpos, sino a los datos.

Como se explicó previamente, el marco legal mexicano, por un lado, establece con claridad el derecho a la identidad como una prerrogativa de los mexicanos, sobre todo en un argumento poderoso si tomamos en cuenta que un perfil de delitos en ascenso es aquel que vulnera la personalidad de los individuos en el sistema financiero. Sin embargo, no hay que olvidar que, por otro lado, existen riesgos en el uso de un sistema de registro ciudadano, como la tentación de limitar las libertades civiles por medio del control de la información ciudadana, muy común en países sin controles democráticos ni los medios de establecer límites al ejercicio arbitrario del poder político, así como detección de patrones de vida de ciudadanos incómodos al poseedor de dicha información.

También hay que señalar que existen riesgos de implementación del uso de la cédula de identidad ciudadana, entre los que podemos incluir el manejo discrecional de la información y afectaciones a los incentivos de otros registros, en particular el padrón electoral.

En este sentido, las democracias contemporáneas tienen el reto de articular leyes que permitan a los ciudadanos poseer una identidad jurídica y que al mismo tiempo sean capaces de autorregular la disponibilidad o no de dicha información. Aunado con ello, es indispensable garantizar por todos los medios posibles que la información sea protegida para que no sea usada con fines punitivos o de vigilancia sin que medie un asunto de seguridad nacional o combate a crímenes de alto perfil.

En el caso mexicano, las experiencias sobre el tema no han sido muy alentadoras, ya que no se ha podido acreditar un manejo adecuado de datos ciudadanos mediante la cédula de identidad, al menos en lo que se refiere a los fines de prevención del delito o formación de un banco de información de apoyos sociales; en cambio, dicha información se ha obtenido por medios ilegales algunas veces y lo más grave es que se ha espiado a ciudadanos que mantienen una postura crítica del gobierno.

Referencias

Bibliografía

Beck, Ulrich (1998). *La sociedad del riesgo: hacia una nueva modernidad*, Paidós, Barcelona.

Bogard, William (2007). "Welcome to the society of control: the simulation of surveillance revisited", en Kevin D. Haggerty y Richard V. Ericson (coords.) *The new politics of surveillance and visibility*, Toronto University Press, Toronto.

Castells, Manuel (2006). *La era de la información. Economía, sociedad y cultura*, Siglo XXI Editores, México.

Ferreira Rubio, Delia Matilde (2016). *La credencial para votar y la protección de los datos personales*, nota introductoria de Daniel Juan García Hernández y José Luis Ceballos Daza, Tribunal Electoral de la Federación, México.

Goffman, Erving (2006). *Estigma*, Amorrortu, Buenos Aires.

Haggerty, Kevin D. y Richard V. Ericson (2007). *The new politics of surveillance and visibility*, Toronto University Press, Toronto.

Lyon, David (2006). "The search for Surveillance theory", en David Lyon (ed.) *Theorizing Surveillance. The panopticon and beyond*, Willan Publishing, Routledge.

Sartori, Giovanni (2015). *La democracia en 30 lecciones*, Debolsillo, México.

Mesografía

Amigón, Edgar (2015). "Robo de identidad, un delito en aumento", *Proteja su Dinero*, [en línea], núm. 186, septiembre de 2015. Disponible en file:///Users/ipg/Downloads/psd_186.pdf, consultado el 20 de enero de 2019.

Forbes (México) (2015). "8 medidas eficaces contra el robo de identidad", [en línea]. Disponible en https://www.forbes.com.mx/8-medidas-eficaces-contra-el-robo-de-identidad/, consultado el 20 de enero de 2019.

Gómez Romero, Luis (2017). "For many mexicans, this government spying scandal feels eerily familiar", [en línea]. Disponible en https://theconversation.com/for-many-mexicans-this-government-spying-scandal-feels-eerily-familiar-79981, consultado el 22 de marzo de 2019.

r3d (2017). "#Gobierno espía. Vigilancia sistemática a periodistas y defensores de derechos humanos en México", [en línea]. Disponible en https://r3d.mx/2017/06/19/gobierno-espia/, consultado el 20 de enero de 2019.

IV

LA POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES EN MÉXICO. ANÁLISIS DE POLÍTICAS Y RETOS ADMINISTRATIVOS

Porfirio Mauricio Gutiérrez Cortés

Introducción

La protección de datos personales se ha ido posicionando en las agendas de investigación y de reforma institucional a lo largo de los últimos años, tanto en lo concerniente a la posesión de particulares como de instituciones del Estado. Se ha hecho hincapié en la gran complejidad que involucra, pues articula la interacción de elementos legales, tecnológicos, económicos, sociales, comerciales; así como de alcances en relación con seguridad pública, social y nacional. Quizá una de sus características distintivas es que nos obliga a observar acciones que tienen manifestaciones y problemáticas particulares en lo que podemos entender como un mundo digital. Es decir, una nueva arena de interrelación social de la que, de acuerdo con datos del informe 2019 de We Are Social y Hootsuite, formamos parte 57% de la población mundial; es decir, somos usuarios de internet (Galeano, 2019).

A diferencia de la información que se recaba de manera física, sujeta a las limitantes de personal y tiempo, el volumen de datos digitales que las organizaciones gestionan, de acuerdo con el tercer estudio Dell Global Data Protection Index 2019, ha pasado de 1.45 perabytes en 2016 a 9.70 en 2018. Esto revela un incremento de 569% de 2016 a 2018, de la cual, 68% procede de nuestros dispositivos móviles (Galeano, 2019).

Queda claro que esta información es un activo central para la operación y la toma de decisiones con la que cuenta, o espera contar, toda organización. Por ello, representa también altos niveles de riesgos, tanto para los propietarios de los datos, como para las sociedades e incluso para la conducción de las instituciones políticas y la gobernabilidad de los estados. Y es que paralelo a su recopilación y uso, en la capacidad de sistematizar estos datos, radica también la posibilidad real

de convertirla en información útil para propósitos distintos a los que les dieron origen. La información es entonces un activo en sí mismo y, por tanto, una parte neurálgica legal de negocios y otros que operan al margen o fuera de la ley.

De acuerdo con cifras compartidas por Facebook, esta red social valora el perfil de cada usuario y establece una tarifa en dólares de acuerdo con la información que proporciona. Así, por ejemplo, el precio promedio por el perfil de un ciudadano en el ámbito mundial está valuado en 6.18 dólares, el de un ciudadano europeo en 8.76, y el de un usuario canadiense o estadounidense casi 27 dólares (Levet, 2018 [en línea]).

En contraparte, según Mendoza (2016), en el informe publicado recientemente por LogDog revela que prácticamente cualquier tipo de cuenta en línea es ofertada en el mercado negro. Cuentas de PayPal, Amazon, Uber, eBay, Netflix, Twitter y de plataformas de correo electrónico se ofrecen por distintos precios. Por ejemplo, el precio de una cuenta de Gmail oscila entre 0.7 y 1.2 dólares, de Uber y Netflix entre uno y dos dólares y de Twitter entre dos y tres dólares. Es así que información legalmente obtenida y procesada puede ser sujeta de prácticas como el *phishing*, o de la presencia de brechas de seguridad, ya sea de integridad, disponibilidad y comúnmente de confidencialidad como las que protagonizaron Facebook y Cambridge Analytica. Ambas empresas, protagonistas de un incidente que será referente obligado sobre el tema en el que se dio a conocer que Facebook había cedido datos personales de 90 millones de usuarios a la consultora política para utilizarse durante la campaña electoral presidencial en los Estados Unidos de 2018, de la que será vencedor el actual presidente Donald Trump (Harán, 2018 [en línea]).

El problema escapa en su dimensión y alcance a la esfera de atención de cualquier país, es pues un tema internacional de seguridad, gobernanza y con importantes implicaciones de derecho internacional y en la economía global. Por ello, observamos la participación de diversas organizaciones internacionales como la Organización para la Cooperación y el Desarrollo Económico (OCDE), la Organización de las Naciones Unidas (ONU), la Unión Europea (UE) y la Red Iberoamericana de Protección de Datos (RIDD) para generar mecanismos legales y reglamentarios mediante los que buscan armonizar el fundamento, reglamentación y funcionamiento de los organismos garantes y aparatos institucionales de

sus países miembros. Por ejemplo, uno de los elementos distintivos de este entramado institucional se fundamenta en la recomendación de establecer órganos y mecanismos de control, con características específicas, orientados a garantizar la protección de datos personales. En este sentido, entendemos los Estándares de Protección de Datos para los Estados Iberoamericanos (2017) y la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad (2009).

En México, iniciamos el diseño de una arquitectura institucional en el tema hace poco más de 15 años. Su resultado ha merecido reconocimiento internacional, esto queda de manifiesto en la formal inclusión del Estado mexicano en el *Convenio 108* del Consejo de Europa. Ello significa que, por un lado, lo eleva a la más alta categoría normativa en materia de protección de datos personales y privacidad, de acuerdo con la comisionada del INAI Patricia Kurczyn Villalobos (Arellano García, 2018). Por otro lado, al interior del país, persiste una marcada desconfianza por parte de la ciudadanía respecto de sus capacidades reales para hacer efectiva dicha normatividad. Se ha reconocido por las autoridades del propio instituto garante que nuestro país es un paraíso de bases de datos clandestinas (Montes, 2018 [en línea]). ¿Cómo entender estos hechos que parecen contrapuestos?

Desde esta investigación, lo que podemos señalar es que para responder es necesario observar en la relación entre el proceso de desarrollo de esta arquitectura institucional, la claridad de mecanismos que supone la operación de las normas para enfrentar el problema y el diseño de intervenciones que la vuelvan efectiva. Tres momentos o procesos que no forzosamente guardan coherencia natural entre sí. Es decir, no se diseñan al unísono ni necesariamente sobre una misma dimensión de problema. Sobre todo, en espacios en los que supone la vinculación de actores de gran nivel de complejidad y decisión y la dependencia con escenarios políticos, de los que depende, a su vez, la estructura de facultades legales y la capacidad de generación de acuerdos con una gran diversidad de actores sociales.

Es decir, la tarea no depende exclusivamente de analizar al organismo garante responsable, sino también girar la atención hacia las condicionantes institucionales y las derivadas del tipo de políticas desplegadas para orientar los recursos y las capacidades definidas para ello. Así, en este documento se explora la posibilidad de hablar de una política pública de protección de datos personales en México como una forma de observar la construcción de la respuesta sistemática

del Estado mexicano a los retos que supone la protección de datos personales, orientada hacia garantizar la privacidad de los datos digitales que proporcionan los ciudadanos en el ámbito de las relaciones de intercambio privado de bienes y servicios, y de su interacción con las autoridades públicas.

Desde esta óptica, la protección efectiva de datos personales no se entiende vinculada exclusivamente a los aspectos reglamentarios de las leyes nacionales e internacionales en la materia, sino también a partir de reconocer las formas en que se diseñan mecanismos que buscan conducir formas específicas de intervención para solucionar el o los problemas en que se manifiesta su debilidad, es decir, desde el contexto político de las políticas; para los propósitos de este trabajo, se emplean elementos teóricos, propios del enfoque de políticas públicas, además de concretos, como la ventana de oportunidad desde el enfoque de Kingdon (1995), así como la tipología de políticas de Lowi (1995). Desde ello, se propone una lectura articulada de tres tipos de políticas: institucional, reglamentaria y de construcción de políticas públicas.

Así, se postula que la respuesta del Estado mexicano a la protección de datos personales no puede verse sólo como un tema normativo-tecnológico o sectorial, sino que es resultado del diseño de una arquitectura institucional que ha sido resultado y parte de una arena de transformación de la vida pública de mayor alcance. Es decir, ha enfrentado las dificultades propias del esfuerzo por democratizar la vida política y social del país, abriéndose paso entre las características, limitantes, restricciones y agendas propias de nuestro sistema político.

Así pues, la reorientación de mecanismos y normas, resultado de la reforma de 2016, representa, en este escenario, una gran oportunidad para observar la puesta en marcha de mecanismos distintos y concebidos en la primera ley. En éstos, a partir de un contexto institucional, de vinculación con la sociedad, de desarrollo tecnológico, se busca diseñar intervenciones dirigidas a modificar comportamientos asociados al cumplimiento del marco reglamentario. Se explora, como veremos más adelante, una alternativa para trascender los conflictos que habían sido propios de lo que se entiende como debilidad institucional.

Partamos de un principio de observación. Al tratar de analizar el rumbo que van marcando las propuestas que buscan transformar el estado actual de las cosas de un país, una sociedad, un estado, hablamos de manera general de lo que puede

traducirse en tres elementos, que se entienden como superpuestos. Es decir, a las manifestaciones que le dan contenido a lo que teóricamente se denomina *polity*, *politics* y *policy*, que en su traducción al español en todos los casos se refiere al vocablo política.

La diferencia es sutil, pero sustantiva. El primero, *polity*, refiere lo que se conoce como régimen político o sistema político desde autores como David Easton (1969), Gabriel Almond (1999), Maurice Duverger (1962), entre muchos otros. El segundo, *politics*, hace alusión a la actividad política en su sentido más tradicional, relacionado con el quehacer de las instituciones y sus representantes, los partidos políticos, los debates y conflictos en torno al ejercicio, reproducción y búsqueda por el poder político (Bobbio, 1989).

El tercer término, *policy*, hace posible hablar de una política como una serie de acciones mediante las cuales se define una respuesta estandarizada a un problema. Esto es el centro de la contribución del enfoque de políticas públicas. Así, en palabras de William Dunn, "una política pública es cualquier insatisfacción relativa a una necesidad, una demanda o una oportunidad de intervención pública" (2004: 98). Y, siendo aún más específicos, Mauricio Merino apunta que este curso no sólo atiende a un sentido incremental, sino que mediante él se tiene por objetivo cambiar el *statu quo* de una circunstancia.

Esta dimensión permite hacer preguntas del tipo: ¿por qué se toman ciertas decisiones, se consideran ciertos problemas, se les da importancia a formas específicas de entenderlos y otros simplemente no se consideran, jamás llegan a capturar la atención de los gobernantes? o bien ¿cómo se establecen, deciden, seleccionan los diferentes tipos de recursos que deberán ser empleados y administrados para que las decisiones tomadas puedan concretarse en acciones? y, por ende, ¿se usan de manera eficaz y eficiente? y ¿por qué pese a contar con decisión, recursos y administración no se logra siempre el resultado prometido, aspirado, proyectado?

Al respecto, la existencia de un problema público es un elemento decisivo del estudio de las políticas públicas. Éste será un elemento clave del enfoque, pues manifiesta una necesaria distinción de los detonantes de la respuesta tradicional de las burocracias públicas, es decir, desde el marco programático que sigue de la creación de planes y de marcos de atribuciones. El análisis de políticas busca

revelar algunos elementos clave como este que permitan observar la construcción de un problema público y su manifestación en una serie de alternativas de solución.

Algunos de los elementos que integran esta respuesta pueden entenderse desde lo administrativo, político y social; o bien en la interacción de las esferas de acción burocráticas, institucionales y de participación. Su articulación es parte de lo que se entiende como la condición de coherencia (Cejudo y Michel, 2016) que busca integrar toda política pública para su éxito. Pero ¿cómo identificar sus características?, es decir, cómo observar el proceso que vincula las intenciones que originaron la decisión de actuar con su desempeño. Brevemente se apuntan dos claves al respecto.

En la literatura que se ha vuelto clásica en el análisis de las políticas, encontramos una obra que es parte de una intensa reflexión sobre la necesidad de contar con modelos teóricos que permitan reconocer diferencias entre tipos de acciones de políticas. Una de ellas es *The politics of regulation*, de James Q. Wilson (1980), quien desarrolla una compleja reflexión sobre el comportamiento regulatorio de los estados, enmarcado en principio por las relaciones entre los postulados de las teorías económicas sobre la regulación de George Stigler (1971) y la teoría política debatida por autores como Theodor Lowi (1969) y Marver Bernstein (1955), entre muchos otros. Derivado de ello, autores como Joan Subitars han decantado las características y condiciones que Wilson reconoce en los distintos tipos de regulación y sus actores, proyectándolo hacia un entorno de comprensión ampliado sobre la influencia de las políticas y la política.

Esto nos deja articular una pregunta ¿qué es lo que define el tipo de respuesta mediante políticas a un problema? Si reparamos un momento en el texto de Lowi (1995), la respuesta no es como esperaríamos, la política; es decir, la posición ideológica o los intereses del tomador de decisiones, la que define la orientación de las políticas. Es el tipo de conflicto político que detona la definición de políticas lo que termina siendo un criterio esencial. De acuerdo con este enfoque, la definición de una política está aparejada a la identificación de los costos que representará en cuanto a las acciones que se despenderán de ella. En síntesis, el tipo de conflictos que detonará y los que es posible enfrentar por quien la emprende.

Esto nos da cuatro tipos de combinaciones posibles y formas de acción de políticas, por consiguiente, resultado de la relación de costos y beneficios:

Redistributivas. Costos concentrados-beneficios concentrados.
Distributivas. Costos difusos-beneficios concentrados.
Regulativas. Costos concentrados-beneficios difusos.
Institucionales/constitucionales. Costos difusos-beneficios difusos.

Cabe mencionar que esta tipología permite reemplazar o ampliar el marco de comprensión de la acción del gobierno más allá de su sectorización. Desde una perspectiva más funcional, la configuración de lo que este autor denomina arenas de políticas responde también a un cambio en el perfil del estado. Esta serie de cambios que se manifiestan en la necesidad de incorporar mecanismos de interacción con otros actores y dinámicas sociales y políticas y, sin duda, otros para atender distintos tipos de conflictividad derivado de ello. A decir:

1. El principio que rige las políticas redistributivas es la generación de mecanismos orientados a intervenir lo que se consideren las bases que originan la desigualdad social, tales como las políticas fiscales y las propias políticas sociales. La idea es resarcir la brecha de desigualdad, no de individuos, sino de grupos específicos e identificados. Los beneficios en principio son concentrados en estos sectores. Al igual que los costos para generar los beneficios, como en el caso de la recaudación de impuesto.

2. Las políticas distributivas se caracterizan, a decir de Ives Meny y Jean Claude Thoening (1992), por generar beneficios y privilegios, ya bien por la acción directa del Estado, como por la excepcionalidad en el cumplimiento de una regla, dispuesto desde una lógica unilateral desde el Estado. Siendo una arena de políticas relativamente baja de conflicto, pues se resuelve por lo regular con transacciones vinculadas al ejercicio del gasto público. Por lo cual podríamos considerarlas de costos difusos, pues no recaen de manera singular en algún sector en específico. Por el contrario, los beneficios sí se distinguen concentrados, frente a lo que Lowi señala, que suelen estar referidas a la creación de bases clientelares.

3. Las políticas regulativas o reglamentarias se basan en la facultad del gobierno para generar normas, es decir, leyes, reglamentos, ordenanzas, con las cuales se busca ordenar procesos específicos de interacción social. Es una arena de conflicto latente. Nuevamente, de acuerdo con Meny y Thoening (1992-1999), pues mediante un decreto legal, las libertades individuales están limitadas y los intereses de los ciudadanos transformados. Los beneficiados y afectados son resultado de

la regulación de un determinado campo de acción (Aguilar, 1996). Si bien los costos de la reglamentación tienen que estar focalizados, así como el descontento que provoca, no es así con los beneficios, pues, no obstante, su importancia en el discurso político, en términos de su identificación, el bienestar general, suele ser ambiguo. Por ello, los costos que supone la implementación de estas acciones suelen ser altos para el decisor, pues la confrontación es inmediata, evidente y suele acompañarse del despliegue de mecanismos y recursos por parte de los actores afectados que buscan impedir su reconocimiento.

4. Finalmente, las políticas institucionales o constitucionales son las más abiertas de todas. No representan un costo concreto, por lo que su oposición no suele ser frontal ni directa, pero sus beneficios tampoco se manifiestan claramente, por lo que su defensa ante escenarios de riesgo u obstaculización, tampoco despiertan grandes movilizaciones. No por ello son menos relevantes, aunque suelen asociarse con discusiones menos abiertas a la participación ciudadana, sino reservarse por su naturaleza a grupos muy bien organizados que han logrado acceso a la discusión de la agenda pública y política.

Lo que se puede destacar de esto es una idea simple: la forma de articular una respuesta a un problema público no se materializa en un sólo tipo de definición de acción, así como tampoco existe una única manera de orientar el gran número de recursos y medios disponibles por parte de las autoridades para articular alternativas de respuesta.

Los problemas, así como las soluciones posibles, tanto como sus capacidades de instrumentación y efectividad, son en esencia fenómenos político-administrativos. Por tanto, en interacción con medios y fines, así como con intereses y desacuerdos, el entorno de análisis no es una relación aislada entre acción-respuesta-resultado, sino una en la que convergen una serie de elementos, que teorizados, adquieren formas observables, que se conducen en procesos diferenciados vinculados con un contexto político.

Una política institucional para facultar al Estado en materia de datos personales

Una política no está compuesta de manera exclusiva de elementos técnicos o legales, sino que será igual de importante la relación política con el contexto. Lo importante

de esto es que tanto la definición del problema, como la de una política pública, va a estar relacionada, o incluso delimitada y acotada por los valores con los que se le asocie y dimensione, y con ello se encadena a un tipo de respuesta y de recursos.

Así, al observar el entorno que encuentra la entrada a la agenda pública y gubernamental en México de la protección de datos personales, se distingue su anclaje a tres importantes discusiones históricas de agenda pública y política, distintivas del último tercio del siglo XX en nuestro país, lo cual va a representar lo que Kingdon (1995) llama una ventana de oportunidad de acuerdo con su modelo de vertientes múltiples. Es decir, una coincidencia entre tres elementos: un proceso político, un problema y alternativas.

Según este modelo, los tres elementos pueden entenderse como familias de procesos o afluentes que articularán la decisión de políticas. Esto busca explicar cómo la manera en que un tema ingresa a la agenda le dará solución como problema público mediante una ventana de política pública. Su convergencia es lo que explica el posicionamiento que se traduce en que las autoridades lo incluyan en su agenda, generen un tipo de alternativas y adopten un tipo de decisión sobre la formulación de políticas a su alcance, y en relación con el conflicto que representan. A continuación, se emplean estos elementos teóricos para analizar el fenómeno de estudio que da motivo al presente libro.

El primer gran proceso político en el que se sitúa es la transición democrática que vive nuestro país desde la reforma política de 1977. Éste será el principal centro de debate, conflicto y de reestructuración institucional del Estado por más de cuatro décadas. El pilar de esta reforma, y de su agenda, fue la redefinición de las reglas de la competencia electoral con el fin de dar cabida a la imperante pluralidad en la que se afirmaría la sociedad mexicana desde entonces, así como la demanda de construir un nuevo sistema de contrapesos al ejercicio del poder público.

De ello, se desprendió un necesario proceso de reforma del Estado, es decir, de sus instituciones políticas para adaptarlas a los cambios democráticos que demandaba, tanto la sociedad, como la redefinición del estado mismo en la globalidad. Tres temas centrales de ello fueron, como siguen siendo, la promoción, respeto, protección y garantía de los derechos humanos; la importancia de transparentar la acción pública de todas las autoridades públicas, principalmente las del Poder Ejecutivo, como una forma de establecer mecanismos para limitar el accionar de

las autoridades públicas y la creación de nuevas modalidades de facultar al Estado, no al gobierno, para responder a los valores, demandas y problemas propios de la construcción de una sociedad que sigue tratando de afirmarse en valores democráticos. Resultaba indispensable modificar las reglas del juego. Descartando la posibilidad de soluciones reglamentarias o de políticas. Estas contenían en sí mismas un problema de origen: el predominio y meta constitucionales del ejercicio del poder por parte del Poder Ejecutivo Federal.

Este problema encuentra, entre un complejo margen de oportunidades, una alternativa de atención en la fragmentación de las facultades del Poder Ejecutivo, aislando de su control y responsabilidad temas prioritarios en la propia agenda democrática, a partir de la figura de los organismos constitucionales autónomos. Éstos van a ser, por ejemplo el Banco de México, la Comisión Nacional de Derechos Humanos, el Instituto Nacional Electoral, el Tribunal Electoral del Poder Judicial de la Federación, el Consejo Nacional para Prevenir la Discriminación y el Instituto Federal de Acceso a la Información Pública.

El tema nos mueve hacia el principio de división de poderes y a la distribución del poder público. La evolución de este último concepto ha decantado en la caracterización y regulación de la actuación una figura que no se encuentra sujeta a los depositorios tradicionales del poder público, a decir los poderes Legislativo, Judicial y Ejecutivo, de manera que se les han encargado funciones estatales específicas, con el fin de obtener una mayor especialización, agilización, control y transparencia para atender eficazmente las demandas sociales (SCJN, 2011).

Su condición constitucional va a ser estratégica para el fortalecimiento democrático del país. El problema es que supeditó un largo proceso legislativo, indispensable por su propia condición jurídica, para que el Congreso de la Unión dotara a cada uno de las facultades necesarias para enfrentar retos tan complejos como el que supone la triple articulación en un mismo organismo garante en temas de transparencia, acceso a la información y protección de datos personales. En un contexto, como hemos dicho, de nueva competencia electoral, que generó importantes cambios en la composición política, tanto del Congreso de la Unión, como de los congresos estatales, piezas clave para la ratificación de las facultades y de legislación específica para cada entidad federativa, de acuerdo con los principios del pacto federal.

Visto de esta manera, la ventana de oportunidad con la que se identifica la entrada del tema de protección de datos personales a la agenda va a ir definiendo, desde una lectura del contexto, tanto el problema como la solución. Se logra, mediante una lucha política, que el acceso a la información sea reconocido como un derecho no referido exclusivamente al ámbito electoral, sino como parte toral de un ejercicio del poder más transparente y que rinda cuentas.

La transformación de su caracterización normativa hizo que no sólo se refiriera el derecho a la información desde su posición y manifestación, sino del acceso a ella. Con esto, se definió la responsabilidad pública del Estado de rendir cuentas acerca de sus procesos internos de funcionamiento y, por lo tanto, sobre los datos, usos, control, vigilancia de y sobre éstos. Como es de todos sabido, este derecho se ha enfrentado una y otra vez a los problemas propios del tipo de arquitectura institucional del Estado mexicano y a la intromisión de intereses que encuentran en la opacidad un aliado.

Si volvemos la vista sobre la tipología de Lowi, lo que encontramos es una definición del tipo de política mediante la que se dimensionarán problemas y alternativas de solución. Se puede reconocer la definición de una política del tipo institucional o constitucional, cuyo conflicto se ha manifestado de manera más clara en el plano legislativo, por parte de actores políticos de gran peso decisional, que junto con *stakeholders* van a movilizar recursos de cabildeo y argumentación desde una arena de políticas más bien cerrada.

Ello habla de una condición de beneficios difusos, como se puede evidenciar desde los estudios que apuntan el bajo conocimiento de los ciudadanos de la existencia e importancia de sus derechos ARCO, así como de la importancia de identificar y proteger sus datos personales. Esto representa uno de los mayores obstáculos en cuanto a la efectividad de políticas reglamentarias creadas para su protección. Este mismo obstáculo, visto desde la construcción de una política institucional, contribuye al letargo con que las autoridades tradicionales enfrentan los procesos y tiempos de decisión y la manipulación de la reglamentación en la materia. Así, al no contar con la presión directa, se difumina el costo significativo en términos político-electorales, de sus acciones. En resumen, sin costos directos, y con beneficios difusos, la política de protección de datos personales sigue los

tiempos máximos que permite la ley y está sujeta a los intereses que pueden manifestar sus beneficios de manera clara e inmediata.

En términos de políticas públicas, podríamos aventurar a decir que, en el caso de la protección de datos personales, el problema ha sido definido en gran medida por una solución asociada directamente a un proceso político de mayor envergadura, del que ha resultado un actor central que es el organismo garante.

Desde esta segunda lectura, vista desde el desarrollo político, señala el proceso de conformar un entramado normativo que le permita a este organismo garante tutelar, en el contexto descrito, el derecho a la protección de datos. Este proceso llevará prácticamente 14 años de deliberación, aprendizaje y decisión política entre los que se lograrán avances paulatinos en la materia hasta contar con los dos principales instrumentos que le permitieran hoy al Estado una adecuada estrategia de intervención. A decir: la Ley Federal de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en 2010 y la Ley General de Protección de Datos Personales publicada el 26 de enero de 2017.

Una manifestación de los problemas a los que se enfrenta una política institucional como la que aquí se señala se ejemplifica con el proceso de armonización que ha seguido la Ley General de Protección de Datos Personales, por parte de las legislaturas locales de las entidades federativas. Veamos.

El plazo definido por el INAI para armonizar a esta nueva Ley General marcó la fecha de vencimiento el día 27 de julio de 2017. Se tuvo una respuesta inmediata de nueve estados, sumando 22 los que lo hicieron dentro del plazo legal. Cinco entidades cumplieron con el proceso fuera del tiempo legal, mientras que en cuatro se desacataron los tiempos.

En cuanto a las observaciones particulares, el INAI señaló que, pese a haber elaborado una ley modelo para guiar el proceso de armonización y evitar las diferencias resultados de otros procesos similares, se emprendieron acciones legales en contra de los ordenamientos promulgados por las legislaturas estatales. Esos recursos resultaron en la impugnación de 17 legislaciones de las publicadas en la materia y, por tanto, a su revisión por parte de la Suprema Corte de Justicia de la Nación. Las violaciones recurrentes que dieron lugar a este mecanismo fueron: en el establecimiento de plazos diferentes a los marcados por la Ley General en agravio de los titulares de la información, en el establecimiento de requisitos aña-

didos a los determinados por la ley para el ejercicio de los derechos; en materia de la emisión de avisos de privacidad, siendo que la ley establece que deben darse de manera inmediata y los congresos otorgaron plazos para el inicio de su vigencia de varios meses.

Si bien los mecanismos de revisión correspondientes señalaron con puntualidad las violaciones e inconsistencias, las cuales se atendieron conforme a proceso, puede reconocerse la manifestación de un comportamiento organizacional que entiende la ley como un parámetro de referencia que puede ser ajustado, incluso sin mala intensión, a procesos graduales y diferenciados de aplicación a conveniencia. Es decir, una tendencia a reconocer espacios de discrecionalidad en el cumplimiento de la ley, no en la búsqueda de contar con las mejores condiciones institucionales específicas para responder a su entorno, sino a criterios fuera de la ley para favorecer condiciones políticas asociadas a intereses particulares.

Una política regulatoria para la protección de datos personales en posesión de particulares

Podríamos decir que la política institucional, entonces, se transforma. Al tomar como punto de partida su publicación y entrada en vigor, se detonan nuevas formas de interacción con el entorno, que nos devuelven a la premisa política-políticas. En relación con la tipología de Lowi, podríamos decir que responden a las características de una política de tipo regulativa. Es decir, una facultad exclusiva de las autoridades públicas que radica no en establecer actos de autoridad burocrático-legal, sino en coartar libertades y generar acciones encaminadas al ejercicio de derechos.

Su entramado regulatorio aspira a generar mecanismos específicos que quieren transformar comportamientos organizacionales e individuales específicos, en este caso en las empresas de mercado. Al respecto es importante señalar que no se trata de una facultad ejecutiva, que contenga los recursos del gobierno, sino de un organismo facultado para ejercer una forma específica de relación con la protección de un derecho. Su capacidad es regulatoria, no condicionante, y sólo vinculatoria a procesos administrativos y jurídicos en el marco de sus facultades.

Las leyes se convierten en instrumentos generadores de acciones, que van a representar una serie de intervenciones, derivadas de la especificidad de los mecanismos que supone su contenido. Así, la identificación del conflicto es parte intrínseca del detonante de la acción. Sin costos claros, o con incentivos mal dimensionados, el conflicto se diluye, y con él la posibilidad de transformar el comportamiento de la manera deseada.

La importancia en esta interpretación de diferenciar dos momentos distintos de políticas, institucional y regulatoria, se encamina a hacer un poco más explícitas algunas de sus problemáticas asociadas. Reafirmamos que una ley no es una política, por lo que cuando aquí se ha hecho referencia a la política de protección de datos personales, no es a la publicación en sí mismas de ambas leyes en la materia ni a una acción en específico de una autoridad pública, sino al conjunto de decisiones y acciones que conforman intervenciones deliberadas de las instituciones del Estado, mediante las cuales se aspira a que se resuelva un problema público, así se atacan las causas identificadas que lo generan.

Referirlas como parte de las decisiones y acciones deliberadas para buscar solucionar un problema implica diferenciar los procesos que animan el desarrollo de cada una; es decir, hay que observar sus interrelaciones, la coherencia entre ellas, pero distinguiendo sus conflictos específicos. Eso nos conduce al menos a dos elementos para abonar a este análisis: el primero quizá sea un valor asociado a la ley en un sentido general, y es que se considera que si la ley ha sido aprobada, es porque manifiesta el acuerdo entre los actores involucrados acerca de su operación. El segundo sitúa este argumento en el contexto de la lógica racional de entornos burocráticos. De manera tal que la ley se transforma en acciones que atraviesan estructuras, reglas, tradiciones, en los que realmente aspira a incidir.

No distinguir estas diferencias es lo que puede dar lugar a interpretaciones parciales sobre la debilidad institucional del Estado para, en este caso, hacer valer el ejercicio de un derecho, lo cual hace suponer que, si existe el instrumento legal, da por supuesto que se cuentan o que se puede forzar a que todos los actores cuenten con los recursos para generar las acciones necesarias para cumplir su responsabilidad, y para esto es suficiente con los mecanismos que parcialmente contiene una ley o su reglamento, lo cual no es así. No sólo en lo que respecta a este tema en particular, sino por condición asociada a la operación política y administrativa

de las instituciones públicas, de conducción de las organizaciones burocratizadas (públicas y privadas), y a la doble condición político-técnica de toda política pública, como hemos venido señalando a lo largo del presente documento.

Para tratar de hacerlo un poco más explícito, a continuación, se recuperan algunos de los múltiples problemas que manifiesta el cumplimiento de las disposiciones reglamentarias de la Ley Federal de Protección de Datos Personales en Posesión de Particulares.

Se han señalado anteriormente algunos datos que refieren las manifestaciones diversas de este tema, como el hecho de que la obtención de la información representa un negocio muy rentable, y que ahora también lo es la protección de los datos personales. Sólo por poner un ejemplo, las organizaciones necesitan sistemas integrales de encriptado, cuya contratación se encuentra al alza, según el estudio 2019 del Ponemon Institute revelado por Becerril (2019). De este mismo estudio, podemos tomar dos datos interesantes, y es que 45% de los encuestados expresan que sus organizaciones cuentan con un plan integral de encriptado que se aplica de manera consistente en la empresa, mientras que otro 42% lo tiene para un plan o área específica.

En contraparte, el panorama en México luce distinto, incluso desalentador. Y no tiene que ver directamente con la capacidad institucional del organismo garante. De acuerdo con un estudio realizado en 2016, a 300 empresas en 24 estados de la República Mexicana por la empresa PWC México (2017), compañía dedicada a los servicios de auditoría, consultoría de negocios, impuestos y servicios legales, 88% de las empresas tienen la percepción de cumplir con las disposiciones de ley en materia de protección de datos. Sin embargo, 48% en realidad no lo hace. Esto a partir de que la percepción se basa en contar y publicar por algún medio un aviso de privacidad. En consecuencia, en 2016, de acuerdo con el INAI, se generaron multas por 85 millones de pesos por incumplimiento de la Ley Federal de Protección de Datos en Posesión de Particulares.

El cumplimiento de la ley requiere la participación tanto del organismo garante como del sujeto obligado, y en este caso, incluso juega un papel determinante el desarrollo de alternativas de mercado. Es decir, además del papel del instituto, por un lado, implica lograr que las empresas reguladas cuenten con las capacidades técnicas, y de recursos humanos y financieros para instrumentar los mecanismos,

tecnologías y procedimientos que le permitan cumplir con su responsabilidad ante la ley. Y por otro lado, deben existir condiciones apropiadas para el desarrollo de negocios asociados a la materia. Por ejemplo, el análisis de riesgo para las empresas y la concientización de los usuarios, como proponen algunas empresas de ciberseguridad como GeneXus (*Forbes,* 2016).

Frente a ello, este mismo estudio realizado por PWC señala que 48% de las empresas no tiene equipo alguno de monitoreo de la información interna. Es decir, incluso en la era de la información, implica que no se cuentan con los medios para sistematizar y controlar la información que recaban u almacenan; por tanto, ni hablar de su uso, acceso, situación, porque una vez que se ha cumplido con el procedimiento en el que se requiere de manera específica saber dónde fue a parar la información. Sumando a ello, de esta muestra, sólo 26% señaló contar con una oficina dedicada a la gestión de datos para proteger la privacidad de sus clientes.

Las consecuencias de esta falta de control tienen implicaciones más amplias en cuanto a la vulnerabilidad de las personas, como a la afectación de sus derechos en extensión de los ARCO. De acuerdo con Expansión, en 2017 aumentaron 89% los ataques cibernéticos en México, lo cual ha generado pérdidas estimadas entre 3 000 a 5 000 millones de dólares anuales, de acuerdo con reportes de 2017 de la Unidad de Innovación y Estrategia Tecnológica de la Presidencia de la República.

Desde esa misma línea, en 2015, el Banco de México informaba que nuestro país se situaba en el octavo lugar en el mundo por monto de fraudes electrónicos relacionados con el robo de identidad. Ese mismo año, la empresa Kaspersky, ya señalaba a México como uno de los países más atacados en internet en el mundo. De acuerdo con la Comisión Especial de las Tecnologías de la Información y Comunicación de la Cámara de Diputados, la industria del ciberdelito en México se disparó al alrededor de 60% de 2010 a 2016, dañando así a 22.4 millones de mexicanos.

Frente a ello, se exploraron distintas alternativas al final del sexenio anterior.[1] Por ejemplo, se impulsaron reformas al *Código Penal* para tipificar esos delitos. Esto en la búsqueda por hacer que México finalizara el proceso de adhesión al

[1] 2012-2018. Ley General de Protección de Datos Personales.

Convenio de Budapest sobre ciberdelincuencia, con lo cual se posibilitaría la búsqueda de asesorías y capacitación para policías, ministerios públicos y jueces para la investigación y castigo para esos delitos.

De igual forma, en octubre de 2017, la Secretaría de Hacienda y Crédito Público (SHCP), con aval de bancos, aseguradoras, uniones de crédito y cajas populares, dio a conocer cinco rubros con los que se busca reforzar la ciberseguridad financiera en México, entre los que destaca la colaboración para fortalecer los controles de seguridad de los distintitos componentes de la infraestructura y plataformas operativas que soportan los servicios financieros del país, y fomentar la educación y cultura de la ciberseguridad ante los usuarios financieros y el personal de las propias instituciones.

No obstante, pese a los esfuerzos en materia de regulación y estrategias, el entorno de acción y operación interna de las organizaciones empresariales es lo que se pone en el centro del problema. De nuevo con cifras poco optimistas, según de PWC, 54% de las empresas encuestadas señalan no contar con procedimientos para responder ante un robo de información; 38% de las empresas tarda al menos un año en detectar un robo de información y 29% no cuenta con acciones concretas ni procedimientos que les señalen qué hacer en caso de que ello suceda.

Es decir, las empresas del país no cuentan con el conocimiento adecuado, el desarrollo tecnológico, instrumentos de capacitación, protocolos de respuesta, equipo, personal, áreas especializadas, capacidades de reacción, e incluso de vinculación con las autoridades competentes. Y lo que es más, abiertamente señalan no tener intensiones de invertir en ello, y el organismo garante no ha logrado descifrar el mecanismo que genere los incentivos adecuados para modificar este comportamiento, lo cual es motivo, entre otros, del énfasis en los programas de concientización sobre la importancia de los derechos ARCO y medidas de protección.

Mientras las multas se siguen incrementando igual que los amparos ante éstas. Siendo más "rentable" pagar aquellas en que se derive una investigación por causa procedente de solicitud ante el INAI, en un entorno en el que persiste una baja cultura de la denuncia y de la protección de datos personales. De nuevo, ante la ausencia de beneficiarios claros, el incentivo también se diluye frente a los costos que representa, los cuales no son difusos como en la política institucional, sino bien claros y específicos en cuanto al espacio y procedimientos que se buscan regular.

Así no es sólo el incumplimiento de una ley, sino la prevalencia de comportamientos; en este caso, cuya consecuencia se manifiesta en la violación de dicha ley, lo cual nos dice que no ha podido incidir en esta transformación. Por tanto, hay comportamientos asociados, tanto al dueño de los datos personales, como a los actores con los cuales interactúa; ante ello, la ley conceptualiza como autoridades públicas o sujetos obligados responsables.

La redefinición de la política

En las grandes democracias, la protección de datos personales es una característica fundamental de su correcto funcionamiento. Sin embargo, hoy en día, a pesar de que la garantía de esta protección es un derecho fundamental de los ciudadanos, la revolución tecnológica y la capacidad del internet hace que este derecho y la capacidad de las instituciones se pongan a prueba. La discusión sobre la protección de datos personales hoy va más allá del reconocimiento y conocimiento de los derechos ARCO, y de la obligación que impone la legislación de los avisos de privacidad o aceptar los términos y condiciones.

Aunque al mismo tiempo, no dejan de ser parte del problema y de la agenda burocrática. Se orienta también a analizar los mecanismos y la creación de condiciones necesarias para tener una adecuada gestión de bases de datos, fortalecer capacidades logísticas y tecnológicas para una adecuada recolección, posesión, resguardo y empleo de datos e información; así como hacer responsables directos aquellos encargados de recopilar y resguardar estos datos.

Tener información sobre estos aspectos representa una gran inversión de recursos para conocer cuáles son las medidas, no sólo jurídicas, sino de incentivos como administrativas que requiere; es parte de la definición de políticas públicas más efectivas, lo cual es punto toral de la redefinición de la política nacional que se deriva de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, 26 de enero de 2017.

Dos son los elementos más significativos: el primero reconoce que la labor de protección de datos personales, transparencia y acceso a la información pública no son responsabilidad exclusiva de un solo órgano, sino de todas las instancias que, siendo parte de la administración pública, con independencia de su nivel

de gobierno, tienen injerencia en el tema, definiendo así un nuevo esquema de gobernanza del Estado mexicano, del que formará parte sustantiva el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. El segundo ubica nuevos instrumentos de política pública como parte de este nuevo diseño institucional, con distintos alcances de coordinación y colaboración gubernamental para garantizar su diseño, ejecución y evaluación. Del que destaca la creación del Programa Nacional de Protección de Datos Personales (2018-2022), instrumento de alcance nacional que adopta una orientación de política pública, basada en la identificación de problemas y diseño de objetivos y acciones que contemplan estructura y mecanismos de evaluación. Desde el cual se definirán y coordinarán las bases de la política pública de protección de datos personales en el país (CNSNTAIPPDP, 2018).

Esta ley transforma al Instituto Federal de Acceso a la Información y Protección de Datos (IFAI) a Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y contiene elementos de gran trascendencia. De acuerdo con su contenido, cambian las facultades y el alcance de acción del Instituto, porque se fortalece en el ámbito nacional con gran esfuerzo de armonización y criterios internacionales.

Al mismo tiempo, no sólo busca regular el área específica correspondiente, sino distribuye y regula competencias entre los organismos garantes de la federación y las entidades federativas en la materia y faculta al Sistema Nacional de Transparencia en materia de datos personales; también define, no sólo responsabilidades, sino los lineamientos de acciones específicas, observables y evaluables. Por lo tanto, el alcance de regulación abarca cualquier autoridad, entidad, órgano y organismo de los poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, de la federación, las entidades federativas y los municipios. Siendo que además podrá regular los medios de impugnación y procedimientos para la interposición de acciones de inconstitucionalidad y controversias constitucionales por parte de los organismos garantes locales y de la federación.

Por su parte, entre la compleja reglamentación, se definen con puntualidad criterios esenciales, como en su artículo 4° que señala la aplicabilidad de la ley "a cualquier tratamiento de datos personales que obren en sopores físicos o

electrónicos". En el artículo 5° de la misma ley, se hace una puntual definición de lo que se considera como fuentes de acceso público:

> I. Las páginas de Internet o medios remotos o locales de comunicación electrónica, óptica y de otra tecnología, siempre que el sitio donde se encuentren los datos personales esté concebido para facilitar información al público y esté abierto a la consulta general;
>
> II. Los directorios telefónicos en términos de la normativa específica;
>
> III. Los diarios, gacetas o boletines oficiales, de acuerdo con su normativa;
>
> IV. Los medios de comunicación social, y
>
> V. Los registros públicos conforme a las disposiciones que les resulten aplicables. (Congreso General de los Estados Unidos Mexicanos, 2017 [en línea])

En ánimo por "destrabar" los esfuerzos institucionales de los problemas de coordinación entre el Instituto y los organismos garantes de las entidades federativas, se sientan las bases de regulación, integración, organización y función del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales. Al mismo tiempo, se va a vincular de nueva cuenta la política con un proceso político macro, que será el combate a la corrupción, señalando su articulación con el Sistema Nacional Anticorrupción, de acuerdo con las leyes publicadas el 18 de julio de 2016.

El Sistema estará integrado, de acuerdo con los artículos 1º y 30 de la Ley General de Transparencia y Acceso a la Información, por el Instituto, los organismos garantes de las entidades federativas, la Auditoría Superior de la Federación, el Archivo General de la Nación y el Instituto Nacional de Estadística y Geografía. Dichos organismos integrarán un consejo nacional, el cual deberá reunirse al menos cada seis meses, y que tiene la posibilidad de invitar a representantes de la sociedad civil para el tratamiento de sus temas.

En lo referente a sus funciones establecidas, destaca el artículo 14, en donde se dispone lo siguiente: acordar y establecer los mecanismos de coordinación que permitan la formulación y ejecución de instrumentos y políticas públicas integrales, sistemáticas, continuas y evaluables, tendentes a cumplir con los

objetivos y fines del Sistema Nacional, de la presente ley y demás disposiciones que resulten aplicables en la materia (inciso IV); diseñar e implementar políticas en materia de protección de datos personales (inciso IX); promover la comunicación y coordinación con autoridades nacionales, federales de los Estados, municipales, autoridades y organismos internacionales (inciso XV), entre otros.

Cabe destacar que el propósito que revela el fomento de buenas prácticas es la apuesta a construir y promover información sobre las acciones que se realizan en el país, con el fin de generar conocimiento que permita compartir y contrastar experiencias con otros y tener un impacto en el diseño de políticas públicas para orientar, corregir y evaluar el desempeño institucional.

De acuerdo con el artículo 31, se dispone el deber de "establecer y mantener las medidas de seguridad de carácter administrativo, físico y técnico para la protección de los datos personales, que permitan protegerlos contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, así como garantizar su confidencialidad, integridad y disponibilidad" (Segob, 2017 [en línea]). Considerando la importancia de definir medidas mínimas de cumplimiento de actividades para el cumplimiento de la ley, es importante resaltar que su artículo 33 señala actividades interrelacionadas de manera específica para establecer y mantener medidas de seguridad, tales como: "crear políticas internas para la gestión y tratamiento de los datos personales, que tomen en cuenta el contexto en el que ocurren los tratamientos y el ciclo de vida de los datos personales, es decir, su obtención, uso y posterior supresión (inciso I); "elaborar un inventario de datos personales y de los sistemas de tratamiento; realizar un análisis de brecha" (inciso III) (Segob, 2017 [en línea]).

Cabe destacar, por último, el papel del Programa Nacional de Datos Personales, Pronadatos 2018-2022. Éste realiza un intenso diagnóstico en rubros como educación y cultura de protección de datos personales entre la sociedad mexicana, ejercicio de derechos ARCO y portabilidad, capacitación a los responsables de protección de datos personales, implementación y seguimiento de un sistema de gestión de seguridad; estándares nacionales e internacionales; buenas y mejores prácticas, acciones preventivas, monitoreo y perspectiva normativa de política pública.

De este diagnóstico se definieron los criterios para vincular el programa a tres problemas públicos:

a) Resolver la utilización de los derechos ARCO orientada a un beneficio concreto para el titular de los datos.

b) Solucionar el tratamiento y seguridad de los datos considerando situaciones urgentes.

c) Implementar simplificadamente la ley y establecer prioridades en la administración pública.

Para lo cual se definen ocho ejes y tres líneas estratégicas transversales, las cuales contienen problemáticas, estrategias y objetivos asociados. Siendo los ejes los que definieron el diagnóstico y las líneas estratégicas transversales: sensibilización, promoción, difusión y socialización; fortalecimiento institucional; y un área que había sido considerada, pero no atendida: el fortalecimiento presupuestal.

Es decir, la garantía del derecho cuenta con nuevos instrumentos, estrategias, enfoques, orientación, mecanismos institucionales y programáticos de coordinación por medio de los que se busca optimizar y mejorar los esfuerzos de construcción institucional producto del largo camino que comenzó en un sentido político en 1977 y de construcción de políticas en 2002.

Conclusión

¿En qué radica la debilidad institucional por parte del Estado mexicano en materia de la protección de datos personales que parecemos percibir cuando la prensa nos informa de una nueva vulneración de nuestros derechos? Acercarnos a reconocerlo es comenzar por puntualizar partes de este problema.

Para finalizar, se señalan cinco ideas:

1. La respuesta del Estado mexicano a la protección de datos personales no puede verse solamente como un tema normativo, tecnológico o sectorial, sino que es resultado del diseño de una arquitectura institucional que ha sido resultado y parte de una arena de transformación de la vida pública de mayor alcance. Es decir, ha enfrentado las dificultades propias del esfuerzo por democratizar la vida política y social del país, abriéndose paso entre las características, limitantes, restricciones y agendas propias de nuestro sistema político. El análisis desde el enfoque

de políticas públicas abre importantes posibilidades para diferenciar ámbitos de acción institucionales, operacionales y normativas que permiten dimensionar la posibilidad de acción de las acciones institucionales, como los retos que enfrentan.

2. Cuando hablamos de recursos, no sólo nos referimos a los económico-presupuestarios, sino también humanos, legales, políticos como consenso y legitimidad, procesos cognitivos, tecnológicos, de información, coercitivos, retóricos, patrimoniales, relacionales, coercitivos, entre otros. Éstos deben ser diferenciados de las capacidades para emplear los recursos en el cumplimiento de las facultades manifiestas en un instrumento de política como uno de regulación, pudiendo ser éstas de conocimiento, de definición de objetivos, de interrelación, de monitoreo y evaluación (CNSNTAIPPDP, 2018). La aplicación de la ley debe contar con mecanismos para su desarrollo coherente.

3. Las dos leyes principales en la materia buscan incidir en los espacios; éstos son organizacionales y manifiestan reticencias propias del cambio organizacional, tales como la existencia de rutinas de operación, que acompañan a la escasez de recursos y ausencia de capacidades. Analizar los factores de incumplimiento de la ley supone también la revisión de los incentivos que contempla su diseño para incidir en la transformación de los comportamientos asociados; así como la valoración de los recursos y capacidades del órgano garante para generar intervenciones adecuadas.

4. La trascendencia de los cambios introduce la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO), su reglamento y el primer Pronadatos; además, se manifiesta la necesidad de construir un sistema de gobernanza para enfrentar la responsabilidad que demanda el tema, planteado ya como guía de la instrumentación de la LGPDPPSO y queda como punto de atención referido a la regulación del sector privado. El diseño de acciones no puede seguir exclusivamente una lógica programática, sino trasladarse a su vinculación con problemas públicos, que se traduzcan en estrategias, no sólo medibles, sino evaluables. Contamos con un instrumento que diagnostica debilidades institucionales y se traza una estrategia clara y evaluable de fortalecimiento, la cual tendrá repercusiones en el cumplimiento de ambas leyes que será necesario evidenciar.

5. La apuesta por un enfoque de gobernanza, políticas públicas, decisiones basadas en evidencia, mecanismos de evaluación que hoy se considera para el sector público impone no sólo el reto de evaluar su efectividad, sino pone de manifiesto

la necesidad de evaluar desde una óptica distinta lo concerniente a la regulación del derecho a la protección de datos personales en posesión de particulares.

Referencias

Bibliografía

Almond, Gabriel (1999). *Una disciplina fragmentada. Escuelas y corrientes en las ciencias políticas*, FCE/Colegio Nacional de Ciencias Políticas y Administración Pública, Ciudad de México.

Aguilar Villanueva, Luis (1996). *La hechura de las políticas públicas*, Miguel Ángel Porrúa, México.

Bernstein, Marver (1955). *Regulating business*, Princeton University Press, New Jersey.

Bobbio, Norberto (1989). *Estado, gobierno y sociedad*, fce, México.

Dunn, William (2004). *Public policy analysis. An introduction*. New Jersey, Pearson Prentice Hall.

Easton, David (1969). *Esquema para el análisis político*, Amorrortu, Argentina.

Duverger, Maurice (1962). *Instituciones políticas y derecho constitucional*, Ariel, Barcelona.

Kingdon, John W. (1995). *Agendas, Alternatives and public policies*, Harpercollins College, New York.

Lasswell, Harold (1951). *The policy sciences*. Stanford University Press, California.

Lowi, Theodore (1995). "American business, public policy, case studies, and political theory", en Daniel C. McCool, *Public policy theories, models, and concepts: an anthology*, Prentice Hall, New Jersey.

Meny, Yves y Jean Claude Thoenig (1992). *Las políticas públicas*, Ariel, Barcelona.

Peschard Mariscal, Jacqueline (2013). "El derecho fundamental a la protección de datos personales en México", en José Luis Piñar Mañas y Lina Ornelas Núñez (coords.). *La protección de datos personales en México*, Tirant Le Blanch, México.

Stigler, George (1980). *The politics of regulation*, Basic Books, New York.

Subirats, Joan (1994). *Análisis de políticas públicas y eficacia de la administración*. Ministerio para las Administraciones Públicas, Madrid.

Mesografía

Arellano García, César (2018). "Exigen cuidar los datos de participantes en la consulta", *La Jornada*, sección política, martes 30 de octubre de 2018, [en línea]. Disponible en https://www.jornada.com.mx/2018/10/30/politica/003n3pol, consultado el 28 de marzo de 2019.

Barlett, Jay (2019). "nCipher: estudio de tendencias de cifrado global 2019", [en línea]. Disponible en https://security.world/es/ncipher-2019-global-encryption-trends-study, consultado el 28 de marzo de 2019.

Becerril, Antonio (2019). "Ataques maliciosos, el arma favorita para robar datos: Cost of a Data Breach Report 2019", *El Economista*, 23 de julio de 2019 [en línea]. Disponible en https://www.eleconomista.com.mx/tecnologia/Ataques-maliciosos-el-arma-favorita-para-robar-datos-Cost-of-a-Data-Breach-Report-2019-20190723-0088.html, consultado el 26 de mayo de 2020.

Cano Guadiana, Areli (2017). "Nueva Ley General de Protección de Datos Personales: punto de partida", *El Financiero*, [en línea]. Disponible: https://www.elfinanciero.com.mx/opinion/areli-cano-guadiana/la-nueva-ley-general-de-proteccion-de-los-datos-personales-un-punto-de-partida, consultado el 17 de enero de 2017.

Cejudo, Guillermo y Cynthia Michel (2016). "Coherencia y políticas públicas. Metas, instrumentos y poblaciones objetivo", en *Gestión y Política Pública*, vol. xxv, núm. 1, pp. 3-31, [en línea]. Disponible en http://www.scielo.org.mx/pdf/gpp/v25n1/v25n1a1.pdf, consultado el 17 de enero de 2017.

Cgeum, Congreso General de los Estados Unidos Mexicanos (2018). "Ley de la Comisión Nacional de los Derechos Humanos", [en línea]. Disponible http://www.cndh.org.mx/sites/all/doc/normatividad/Ley_CNDH.pdf, consultado el 17 de enero de 2017.

Congreso General de los Estados Unidos Mexicanos (2015). "Ley General de Transparencia y Acceso a la Información Pública", [en línea]. Disponible: http://www.diputados.gob.mx/LeyesBiblio/ref/lftaip/LFTAIP_orig_09may16.pdf, consultado el 17 de enero de 2017.

_____ (2017). "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados", [en línea]. Disponible en http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017, consultado el 17 de enero de 2017.

_____ (2018). "Ley Federal de Protección de Datos en Posesión de los Particulares", [en línea]. Disponible en https://www.gob.mx/cms/uploads/attachment/file/123648/Ley_Federal_de_Protecci_n_de_Datos_Personales_en_Posesi_n_de_los.pdf, consultado el 17 de enero de 2017.

_____ (2018). "Ley General de Archivos" [en línea]. Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGA_150618.pdf, consultado el 17 de enero de 2017.

_____ (2012). "Ley Federal de Archivos", [en línea]. Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LFA_150618.pdf, consultado el 17 de enero de 2017.

Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (2018). *Programa Nacional de Protección de Datos Personales,* [en línea]. Disponible en http://www.dof.gob.mx/nota_detalle.php?codigo=5511542&fecha=26/01/2018, consultado el 17 de enero de 2017.

Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (2018). Acuerdo por el que se aprueba el Programa Nacional de Protección de Datos Personales, [en línea]. Disponible en https://www.dof.gob.mx/nota_detalle.php?codigo=5511542&fecha=26/01/2018, consultado el 17 de enero de 2020.

Cuarto Tribunal Colegiado en Materia Administrativa del Primer Circuito (2012). "Principios de universalidad, interdependencia, indivisibilidad y progresividad de los derechos humano", en Seminario Judicial de la Federación, [en línea]. Disponible en https://sjf.scjn.gob.mx/sjfsist/paginas/DetalleGeneralV2.aspx?ID=2003350&Clase=DetalleTesisBL&Semanario=0, consultado el 17 de enero de 2017.

Forbes, México (2016). "Protección de datos personales, nueva oportunidad de negocio", [en línea]. Disponible en http://www.habeasdatafinanciero.com/2018/, consultado el 13 de mayo de 2019.

Galeano, Susana (2019). "El número de usuarios de Internet en el mundo crece 9.1% y alcanza los 4.388 millones (2019)", *Markeing4commerce,* [en línea]. Disponible en https://marketing4ecommerce.net/usuarios-internet-mundo/, consultado el 31 de enero de 2020.

Harán, Juan Manuel (2018). "Las brechas de seguridad y casos de exposición de datos más importantes de 2018" [en línea]. Disponible https://www.welivesecurity.com/la-es/2018/12/26/brechas-seguridad-exposicion-datos-mas-importantes-2018/, consultado el 26 de diciembre de 2019.

Levet, Viviana (2018). "Protección de datos personales, nueva oportunidad de negocio", *Forbes* (México), [en línea]. Disponible en https://www.forbes.com.mx/proteccion-de-datos-personales-nueva-oportunidad-de-negocio/, consultado el 25 de abril de 2018.

Mendoza, Miguel Ángel (2015). ¿Por qué es importante proteger tus datos personales?", [en línea]. Disponible en https://www.welivesecurity.com/la-es/2015/10/16/importancia-datos-personales-proteccion/, consultado el 16 de octubre de 2019.

_____ (2016). "¿Cuánto por esa cuenta? El valor de la información en el mercado negro", [en línea]. Disponible en https://www.welivesecurity.com/la-es/2016/11/25/informacion-mercado-negro/, consultado el 25 de noviembre de 2019.

Montes, Rafael (2018). "México es 'paraíso' de bases de datos clandestinas: inai", *Milenio* [en línea]. Disponible en https://www.milenio.com/politica/mexico-paraiso-bases-datos-clandestinas-inai, consultado el 23 de mayo de 2019.

Morales Sánchez, Julieta y Esperanza Guzmán Hernández (2011). "Organismos constitucionales autónomos en materia de derechos humanos", en Manuel González Oropeza y David Cienfuegos Salado (coords.) *Estudios de derecho constitucional local,* México, Poder Judicial del Estado de Coahuila, Congreso del Estado de Coahuila LVIII Legislatura y Editorial Laguna, [en línea]. Disponible en https://archivos.juridicas.unam.mx/www/bjv/libros/7/3032/14.pdf, consultado el 14 de enero de 2019. Personales en Posesión de Sujetos Obligados", [en línea]. Disponible en https://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/2017, consultado el 14 de febrero de 2018.

Presidencia de la República (2011). *Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares,* [en línea]. Disponible en http://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf, consultado el 14 de enero de 2019.

pwc. México (2019). "Ciberseguridad y privacidad ¿Y tú cómo estás respondiendo a los riesgos cibernéticos?", [en línea]. Disponible en https://www.pwc.com/mx/es/servicios-consultoria/ciberseguridad-y-privacidad.html, consultado el 14 de junio de 2019.

Red Iberoamericana de Protección de Datos (2017). *Estándares de protección de datos para los estados Iberoamericanos,* [en línea]. Disponible en https://www.infoem.org.mx/doc/publicaciones/EPDPEI_2017.pdf, consultado el 14 de mayo de 2019.

Redacción emc (2019). "Dell EMC: el volumen de datos que gestionan las empresas en mundo crece casi un 600% en dos años", [en línea]. Disponible en https://www.muycomputerpro.com/2019/03/26/dell-emc-el-volumen-de-datos-que-gestionan-las-empresas-en-mundo-crece-casi-un-600-en-dos-anos, consultado el 26 de marzo de 2019.

Segob, Secretaría de Gobernación (2017). "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados". Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf, consultado el 13 de mayo de 2019.

_____ (2019). "Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados" [en línea]. Disponible en http://www.dof.gob.mx/nota_detalle.php?codigo=5469949&fecha=26/01/201, consultado el 28 de mayo de 2019.

Servicio Profesional en Derechos Humanos (2012). *Las reformas constitucionales en materia de derechos humanos. México: Comisión Nacional de Derechos Humanos,* [en línea]. Disponible en https://cdhdf.org.mx/serv_prof/pdf/lasreformasconstitucionalesenmateriade.pdf, consultado el 14 de mayo de 2019.

Staff (2018). "Adhesión de México al *Convenio 108* del Consejo de Europa garantiza la tutela eficaz del derecho a la privacidad", *LJA.MX*, [en línea]. Disponible en http://www.lja.mx/2018/11/adhesion-de-mexico-al-convenio-108-del-consejo-de-europa-garantiza-la-tutela-eficaz-del-derecho-a-la-privacidad/, consultado 8 de noviembre de 2018.

scjn, Suprema Corte de Justicia de la Nación (2005). "Controversia constitucional 32/2005. Órganos constitucionales autónomos. Sus características", [en línea]. Disponible en http://sjf.scjn.gob.mx/sjfsist/documentos/tesis/1001/1001339.pdf, consultado el 13 de junio de 2019.

Tomeo, Fernando (2019). "Legislar sobre el mundo digital", *La Nación*. [en línea]. Disponible en https://www.lanacion.com.ar/opinion/columnistas/legislar-sobre-el-mundo-digital-nid2228376, consultado el 14 de marzo de 2019.

V

EL ARCO DIGITAL EN MÉXICO

Alejandro Cuadros Medina

Introducción

El creciente interés por la obtención de datos personales puede considerarse en la misma proporción con relación al desarrollo de tecnologías digitales; en la actualidad, vemos este flujo de información como una actividad simple y cotidiana dentro de las dinámicas de nuestra vida. Internet ha sido una herramienta clave en esta progresión de información, la cual ha ganado una relevancia social y económica muy significativa; a los datos personales se les ha intitulado como "el nuevo petróleo de internet y la nueva moneda del mundo digital" (Kuneva, 2009: 2); esta estimación financiera es producto de la creciente oleada de información que genera el ecosistema digital del ciberespacio.

Los datos personales se han transformado en un objeto mercantil, como lo menciona Nelson Remolina "esta información se ha convertido en un bien permanentemente comercializado en el mercado nacional e internacional y en un insumo diario de los sistemas de información privados y gubernamentales" (2010: 492 [en línea]); las empresas transnacionales hacen uso de bases de datos que en muchos de los casos son de uso libre y los transforman en un bien comercializable. La finalidad de una empresa es expandir sus productos; para ello, se ha llegado al análisis del comportamiento del consumidor, el resultado es hacerle llegar lo que necesita y lo que no necesita, pero le interesa. Ésta es la respuesta personalizada que se le brinda con una atención basada en los gustos y comportamientos propios de cada ciudadano; por su parte, las instituciones gubernamentales llegan a utilizar las bases de datos para buscar influir en la toma de decisiones que la ciudadanía emita hacia sus gobernantes, realizando así una nueva dinámica en el proceso de elección, a lo que se puede considerar como un nuevo orden de una *democracia digital*.

Un complemento a la recolección de los datos personales es el ofrecer o brindar a quien los proporciona la salvaguarda de éstos con una protesta de carácter ético, mostrada en su aviso de privacidad; pero sin que la institución pública o privada que los recopila haga una aclaración por cuánto tiempo permanecerán en su poder para después eliminarlos de su sistema de almacenamiento. Este punto debe considerarse como un tema de suma importancia en las diversas propuestas y estrategias de seguridad que se han declarado por comunidades internacionales, regionales o locales, pues la logística digital de los datos permite modificar, editar e incluso compartir de manera sencilla una gran cantidad de información propia de cada uno de los ciudadanos del orbe, sin el consentimiento previo o directo de la persona que es la indicada, con esta acción deshonesta por parte de las instituciones se puede considerar una afrenta a la dignidad humana.

Convenio 108

En las últimas décadas del siglo pasado, algunas personas manifestaron su preocupación por la protección de sus datos, que son compartidos en el ámbito público como privado. Fueron los estados europeos a quienes se les ha llegado a considerar como los pioneros en materia de legislación para brindar protección de datos personales; se organizaron y después de varias reuniones de trabajo colaborativo obtuvieron un resultado significativo, publicar un material escrito que contendría los derechos y obligaciones sobre el uso y transferencia de datos personales, documento conocido como *Convenio 108*, el cual en nuestros días podemos considerarlo como el pilar visionario en el desarrollo tecnológico que se avecinaba para la última década del siglo XX, el uso masivo de internet.

Es el 28 de enero de 1981, fecha en que se firma el documento por parte del Comité de Ministros del Consejo de Europa. Dicho *Convenio* se signó para la protección de las personas con respecto al tratamiento automatizado en sus datos de carácter personal; hasta nuestros días, es el instrumento más importante en el ámbito mundial en materia de protección de datos personales; documento que los participantes dejaron abierto para que el mismo Consejo de Europa invitara a otros países de cualquier continente a formar parte de él, por ende, aunque no sean miembros del Consejo, pero que sí se cumplan lo solicitado por éste. A partir

del contenido, el *Convenio 108* ha permitido en diferentes países ser el sustento y el soporte para crear, o en su caso modificar, leyes que permitan proteger al ciudadano en materia de datos personales.

El fin y objeto del *Convenio 108* es explicito en su artículo 1: "El fin del presente *Convenio* es garantizar, en el territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o su residencia, el respeto de sus derechos y libertades fundamentales, concretamente su derecho a la vida privada, con respecto al tratamiento automatizado de los datos de carácter personal correspondientes a dicha persona ('protección de datos')" (Consejo de Europa, 1981: 2 [en línea]).

La privacidad sobre los datos personales de cada ciudadano, sin considerar su nacionalidad, color o creencia religiosa, es un derecho que se debe garantizar por parte de las instituciones, sean éstas públicas o privadas. La sensibilidad al trato de los datos personales ha crecido en la medida que ha evolucionado la automatización de las bases de datos que colectan la información, es así como la atención de los expertos ha sido atraída por diversos espacios donde se exponen múltiples conferencias y foros de debates en todos los niveles intelectuales para tratar el tema de relevancia social y económica de la información que posee cada ser humano como parte de su individualidad ciudadana.

Retomando el tema del *Convenio 108*; se considera importante hacer mención que a partir de esta declaración se decretó que el 28 de enero de cada año se considere como el Día Internacional de la Protección de Datos Personales, conmemoración que no sólo enmarca la celebración como llano acontecimiento; por el contrario, varios estados aprovechan este aniversario para efectuar diversas actividades relacionadas o encaminadas a la reflexión y al debate sobre el tema; también buscan promover la importancia de la obtención, el manejo y la transferencia de los datos personales por parte de quien los obtiene; con ello, se han dado a conocer propuestas fundamentales que enriquecen y aportan elementos que ayudan a fortalecer la evolución de esta materia; por mencionar un ejemplo de ello ha sido la aprobación de la Directiva 2003/98/CE del Parlamento Europeo y del Consejo, la cual refiere a la reutilización de la información del sector público, de acuerdo con la Comisión Europea citada en Antonio Troncoso, se define *reutilización* como "el uso de documentos que obran en poder de las Administraciones y organismos del sector público por personas físicas o jurídicas

con fines comerciales o no comerciales, siempre que dicho uso no constituya una actividad administrativa pública" (Troncoso, 2010). Esta reutilización de datos ha derivado en la promulgación de una ley en España; como este ejemplo, se pueden enlistar muchos que han trascendido a favor de la protección de los datos personales.

El *Convenio 108* es el documento de mayor relevancia en el tema de protección de datos personales que se tiene en los últimos 40 años, su influencia ha sido tan notable que algunos países han hecho de éste un eje fundamental para generar el cimiento de sus leyes en relación con el tema; nuestro país no ha sido la excepción, como lo comenta Fátima Cambronero:

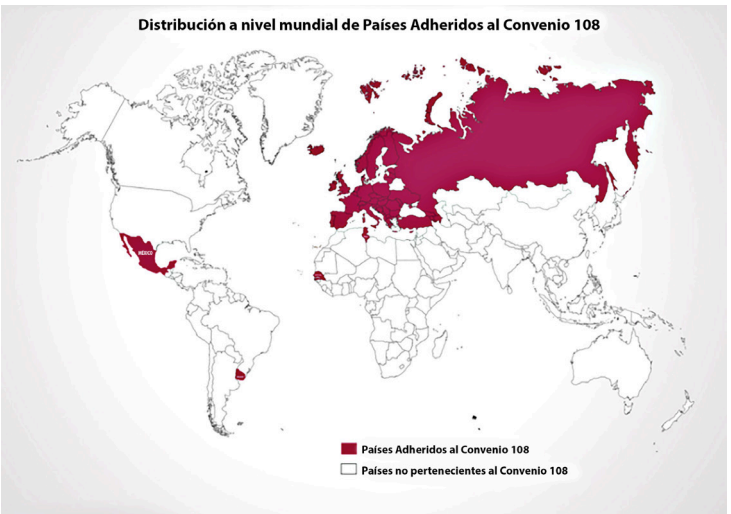
> Este *Convenio* incluye principios para el tratamiento de los datos personales a través de medios automatizados, que luego van a ser recogidos e incluidos en casi todas las legislaciones en materia de datos personales, como la mexicana; principios tales como calidad de los datos, legalidad, lealtad, finalidad, proporcionalidad, periodo de conservación necesario para el cumplimiento de las finalidades para los cuales fueron recogidos, prohibición de tratar de manera automatizada los datos personales sensibles, de seguridad en el tratamiento de los datos personales, derechos de acceso y rectificación del titular de los datos personales (2018: 1 [en línea]).

En los años posteriores a la publicación y aplicación del *Convenio 108*, se logró un rápido avance en el procesamiento de información personal, contribuyó a cimentar las primeras regulaciones de bases de datos en las grandes empresas y en distintos gobiernos, en un inicio estaba conformado por los Estados Partes que fueron España, Francia, Alemania, Noruega y Suecia, países en los cuales se dejó abierta —como ya se mencionó anteriormente— la posibilidad de que otros Estados no europeos se adhirieran al *Convenio 108* y con ello se lograba un alcance de carácter universal.

El primer país del continente americano en adherirse fue Uruguay; en el caso de México, es el segundo país de América que se ha sumado al *Convenio 108*, debieron de pasar algunos años para que se aceptara pertenecer al grupo, aunque la invitación como observador le llegó en 1999; fue hasta 2018 cuando oficialmente y por decreto presidencial se acepta reconocer el *Protocolo adicional al Convenio 108*; con ello, se desempeña un papel primordial en el ejercicio de derechos fundamentales, tales como la libertad de expresión, la protección contra las intromisiones en la vida privada y contra el uso incorrecto de los datos personales.

En poco más de tres décadas desde su creación, el *Convenio 108* se ha ido modificando acorde con los cambios tecnológicos que se han desarrollado así como también ha ido creciendo con los países que se han adherido a éste; pero a pesar de los esfuerzos por parte de sus miembros para contribuir a llevar a bien el uso de las datos personales que proporcionan los ciudadanos a figuras institucionales sean públicas o privadas, se ha logrado adherir a pocos países no pertenecientes al continente europeo, como lo podemos ver en el siguiente mapa, donde los estados pertenecientes al *Convenio 108* están representados en color oscuro, en tanto que los no adheridos están en color blanco; el contraste cuantitativo es muy significante.

Mapa 1



Elaboración propia

En una era globalizada por la tecnología en donde se recibe y envía información con suma facilidad por medios digitales, se debe avanzar en un mayor resguardo para evitar su mal uso. La utilización de internet tiene una ventaja para el *Convenio 108*: aplicar su dimensión transfronteriza para la protección de datos a terceros países. Pero para llegar a ello por medio del *Protocolo adicional*, primero hizo su aparición internet en el mundo entero.

World Wide Web

Al cumplirse la primea década de vida del *Convenio 108*, la informática presentó al mundo entero el protocolo de distribución de documentos de hipertexto, la denominada World Wide Web desarrollada por el físico inglés Tim Berners-Lee en 1991; esta red informática en sus planes iniciales estaba destinada para lograr una comunicación local en el centro laboral de la Organización Europea para la Investigación Nuclear, conocida por sus siglas como CERN: Conseil Européen pour la Recherche Nucléair, pero Berners-Lee pronto se dio cuenta que podía funcionar para todo el mundo; con este nuevo sistema de comunicación se generó una inmediatez en los datos personales, los cuales se vieron afectados en su custodia, al grado de considerarse vulnerables por la facilidad de transferencia de éstos mediante el novedoso soporte de gestión de la información.

Para los años que iniciaban la década de 1990, la World Wide Web identificada más por la ciudadanía como WWW; preparaba su camino; con ello toda persona alcanzaba el acceso, con sus respectivas limitantes en relación con costos económicos por obtener el servicio y la conectividad, entendida ésta como la capacidad de conectarse a la red o a otros dispositivos computacionales.

Es así como se daba inicio a una transferencia internacional de datos personales, acción que es parte de una nueva integración económica y social mundial, por la cual ha apelado internet; el traslado o envío de datos entre una institución o empresa de un país a otro, se le ha llamado "movimiento internacional de datos o flujo transfronterizo de datos" (Garriga Domínguez en Remolina, 2010: 495).

El flujo transfronterizo de la información a partir del uso de la World Wide Web al parecer influyó en el Consejo de Europa para que en 2001 se firmara el *Protocolo adicional al Convenio 108*, el cual en su preámbulo considera que el incremento en el intercambio de datos personales por medio de las fronteras requiere de una efectiva protección al derecho a la privacidad (Consejo de Europa, 2001).

La transferencia de datos personales a un tercero que se encuentre fuera del Consejo de Europa lo establece el artículo 2, párrafo 1, del *Protocolo adicional al Convenio 108*, el cual expresa lo siguiente: "cada parte preverá que la transferencia de datos personales a un destinatario sometido a la competencia de un Estado u organización que no es Parte del *Convenio* se lleve a cabo únicamente si dicho Estado u organización asegura un adecuado nivel de protección" (Consejo de Europa, 2001: 2).

En este contexto que se presenta sobre todo en países europeos como pioneros en el tema de la protección de datos personales, podemos observar su comportamiento y actuar constante para promover derechos que puedan brindar protección a la integridad de cada persona. Trasladando estas acciones hacía nuestro país, nos permite visualizar un panorama en donde los procesos han sido un tanto tardíos o en otros casos se encuentran en vías de desarrollo.

Más de 15 años tuvieron que trascurrir para que en México se le diera reconocimiento al *Protocolo adicional* (de acuerdo con la publicación en el *Diario Oficial de la Federación*), pues éste se aprobó por la Cámara de Senadores del Honorable Congreso de la Unión, con fecha del 26 de abril de 2018, suscrito por el Ejecutivo Federal en turno y en donde se reconoce el instrumento de adhesión en conformidad para el control y flujo transfronterizos de datos personales. El decreto firmado por el presidente de la República se publicó el 28 de septiembre y en el transitorio se estableció que entrara en vigor a partir del 1 de octubre de 2018.

Antes de estas fechas ya se había aprobado la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* con fecha del 5 de julio de 2010. Dicha ley como lo dispone en su artículo 1 "es de orden público y de observancia general en toda la República, reglamentaria de los artículos 6º, Base A y 16, segundo párrafo, de la *Constitución Política de los Estados Unidos Mexicanos*, en materia de protección de datos personales en posesión de sujetos obligados" (Cámara de Diputados del H. Congreso de la Unión, 2017 [en línea]).

De acuerdo con información del portal digital de la Cámara de Diputados del H. Congreso de la Unión, se pueden consultar las diferentes reformas realizadas a la *Constitución Política de los Estados Unidos Mexicanos* a lo largo de la historia; el primer antecedente en relación con la protección de datos se encuentra en la reforma realizada en 2007 sobre el artículo 6º constitucional, en el que se adicionó un segundo párrafo a este numeral, donde se asientan las bases respecto al derecho a la información, se incluye la protección de datos personales por parte de las entidades públicas y se reconocen los derechos de acceso y rectificación; para 2013, se realiza otra reforma al mismo artículo en donde se adiciona información que va a crear el apartado A que hace referencia al derecho de acceso a la información (transparencia) y a que toda información sólo podrá ser almacenada

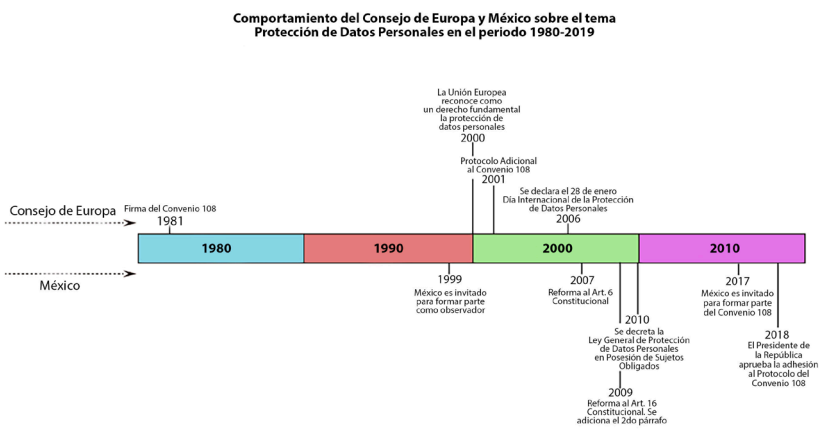
temporalmente por razones de interés público y seguridad nacional, en los términos que fijen las leyes.

En lo referente al artículo 16, en 2009, se le adicionó el segundo párrafo en el que se puede leer que toda persona tiene derecho a la protección de sus datos personales, al acceso, rectificación y cancelación de éstos, así como a manifestar su oposición, en los términos que fije la ley (LGPDPPSO, 2010).

La reforma y adición de párrafos a ambos artículos fue necesaria, si consideramos que antes de ello no existía un sustento jurídico que permitiera la creación de una nueva ley; sobre todo con la reforma al artículo 16, en donde se establece que toda persona puede ejercer sus derechos denominados ARCO, acrónimo de Acceso, Rectificación, Cancelación y Oposición; con los que se da reconocimiento expresamente al panorama normativo que el país requería para cumplir con sus compromisos internacionales, en donde se considera expedir una nueva ley en la materia para crear un respaldo en la información.

La firma del *Convenio 108* en 1981 por parte del Consejo de Europa y el decreto de aprobación al *Protocolo adicional del Convenio 108* fueron firmados por las autoridades federales mexicanas en 2019. En este periodo, se permite hacer una representación gráfica para mostrar los diferentes comportamientos que se han suscitado en ambas esferas.

Gráfica 1



Elaboración propia

Esta línea de tiempo, por un lado, permite visualizar que 37 años debieron de transcurrir para que México se adhiriera a los principios enunciados en el *Convenio 108*; por otro lado, suman ya nueve años de haberse promulgado la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, de la cual mínima difusión y aplicación se ha tenido hacía la ciudadanía. Con esta aprobación a la adhesión no se pretende hacer un reemplazo a la ley, por el contrario, se deben implementar en sus artículos acciones y medidas complementarias que permitan nivelarse con el *Protocolo adicional al Convenio 108*, que expresa lo siguiente:

> Los Estados Partes en el *Convenio* deberán establecer una o varias autoridades independientes con el objetivo de asegurar el respeto de los principios enunciados en el *Convenio*. Estas autoridades de control tienen el poder de investigar e intervenir, de interponer una acción judicial o de poner en conocimiento de las autoridades judiciales las violaciones de la legislación sobre la protección de datos (Consejo de Europa, 2001: 108).

Derechos ARCO

Las autoridades correspondientes deben amalgamar sus acciones con los derechos ARCO, que en últimas fechas ha sido un término que poco a poco se ha extendido entre la ciudadanía, en algunas ocasiones se mal interpreta y se ha llegado relacionar con el cumulo de información que oferta internet, pero ¿qué son los derechos ARCO?, una pregunta que debe responderse para conocer como ejercerlos en la práctica con carácter adecuado y correcto. Estos derechos sólo pueden ser aplicados de manera personal, es decir, sólo logra ejecutarlos el titular de los datos, por su representante legal o por un representante acreditado, es información de valor que se debe proteger de malos usos en todos los entornos, incluyendo el digital o ciberespacio; esta información está relacionada con la persona misma, incluye nombre, número telefónico, huellas dactilares, domicilio, lugar de empleo, así como cualquier otro dato que pueda ser útil para identificar a una persona.

¿Cómo se puede proteger la información que comparte una persona por cualquier medio, sea análogo o digital? Desde la óptica jurídica, el titular de los datos está posibilitado para realizar una solicitud de derechos ARCO con la finalidad de tener el control y administración de su información o al menos conocer el estatus

de cómo se tiene almacenada. De acuerdo con información publicada en el portal web del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, el titular puede presentar ante esta institución una solicitud de protección de sus datos, con la finalidad de evitar que se haga mal uso de ellos.

De acuerdo con la información que publica el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (Infoem), en su portal de internet presenta un resumen de los derechos ARCO.

> Derecho de acceso: aquel mediante el cual el titular tiene derecho a solicitar y ser informado sobre sus datos personales, el origen de los mismos, el tratamiento del cual sean objeto, las sesiones realizadas o que se pretendan realizar, así como a tener acceso al aviso de privacidad al que está sujeto el tratamiento.
>
> Derecho de rectificación: aquel mediante el cual el titular tendrá derecho a solicitar la rectificación de sus datos personales cuando éstos sean inexactos, incompletos, inadecuados o excesivos, siempre que sea posible y no exija esfuerzos desproporcionados, a criterio del Sujeto Obligado en posesión.
>
> Derecho de cancelación: si el titular tiene conocimiento de que el tratamiento que se está dando a sus datos personales contraviene lo dispuesto por la Ley de Protección de Datos del Estado de México o de que sus datos personales han dejado de ser necesarios para el cumplimiento de la finalidad(es) de la base de datos previstas en las disposiciones aplicables o en el aviso de privacidad, puede solicitar la cancelación de sus datos.
>
> Derecho de oposición: aquel derecho que tiene el titular a oponerse por razones legítimas, al tratamiento de sus datos personales para una o varias finalidades, en el supuesto en que los datos se hubiesen recabado sin su consentimiento, cuando existan motivos fundados para ello y la ley no disponga lo contrario (Infoem, 2019 [en línea]).

Hoy en día, queda fuera de toda duda que se requiere el uso de datos personales para cualquier actividad que realice el ciudadano como ente individual, es así como los datos personales son una pieza importante para ejecutar cualquier transacción económica, para concretar algún trámite social, para alguna gestión política; en sí, para toda actividad fundamental en donde el factor humano sea pieza clave para

realizar determinada acción o labor. Lo que ha facilitado estas operaciones es la tecnología innovadora de la información como es internet, el cual permite que cualquier tipo de organización privada o pública sea pequeña o grande, gestione, explote y almacene cierta cantidad de información relacionada con los datos de las personas. Para llegar a estos quehaceres y facilidades que ofrece internet, tuvieron que pasar poco más de dos décadas desde que inicio la web.

A partir de que internet es liberado con destino al uso y consumo de carácter social en 1990, al año siguiente aparece la primera página web; pero antes de continuar con el tema, es pertinente mencionar que la web es diferente a internet, como lo expresa Marino Latorre: "internet es la red de redes, donde reside toda la información, siendo un entorno de aprendizaje abierto, más allá de las instituciones educativas formales. La web es un subconjunto de internet que contiene información a la que se puede acceder usando un navegador" (Latorre, 2018: 1).

Tal pareciera que la web es un organismo vivo, desde su nacimiento hasta nuestros días ha sufrido diversos cambios; esta evolución se ha ido clasificando por etapas con sus propias características. La web 1.0 fue unidireccional sin posibilidad de interactuar; la web 2.0 fue dinámica, fomentó la colaboración y el intercambio ágil de información, aparecen las redes sociales; a la web 3.0 se le conoce como la *web semántica* porque propone su propio lenguaje, es inter operativa y alcanza autonomía con respecto al navegador; por último, la web 4.0 permite una computación cognitiva, una interacción con el usuario y adelantarse a situaciones cotidianas, por medio de potentes almacenes digitales se procesan los datos para lograr una comunicación máquina a máquina (Latorre, 2014). Actualmente nos encontramos en la transición entre la web 3.0 y la web 4.0.

Este avance tecnológico ha llevado a la humanidad a convivir dentro de lo que es la fase primaria de la web 4.0, en donde no sólo estarán interconectadas las personas, sino también los objetos, y con ello nos tocará vivir la plenitud de la etapa del Internet de las Cosas (IoT por sus siglas en inglés de Internet of Things). Sobre el tema podemos encontrarnos con múltiples definiciones, pero se toma como referencia lo que el grupo de trabajo CASAGRAS[1] publicó en 2014, considerada como una de las más certeras y que al paso de los años se ha ido fortaleciendo:

[1] Coordination And Support Action for Global Rfid-related Activities and Standardisation.

> Internet de las Cosas es una infraestructura global interconectada enlazando objetos físicos y virtuales a través de la explotación de la captura de datos y las capacidades de comunicación. Ofrecerá identificación específica de objetos y capacidades sensoriales y su conectividad como base para el desarrollo de servicios cooperativos y aplicaciones independientes. Se caracterizarán por un alto grado de captura de datos autónoma, transferencias de eventos, conectividad de red e interoperabilidad (CASAGRAS, 2014 [en línea]).

El Internet de las Cosas se trata de objetos cotidianos que son focalizados de manera individual, conectados entre sí e identificados por equipos que manejan una gran cantidad de información y capacidad de actuación independiente, de tal manera como si fueran seres humanos. En este panorama, el IoT fomentará integraciones y descubrirá aplicaciones en el mundo empresarial, educativo, médico, en sí en toda actividad realizable; en este conocimiento necesario hará que las marcas cambien sus procesos, aparecerán nuevas formas de trabajo y se destruirán otras; la manera de consumir, relacionarnos y trabajar será modificada. Hablamos de un futuro no demasiado lejano (Romero, 2017).

En este contexto tecnológico nos moveremos, el IoT no es sólo una tecnología, un producto o algo inmaterial; debemos ser claros en que es un concepto que hace referencia a objetos comunes interconectados a internet. Actualmente el uso de *smartphones*, tabletas y computadoras portátiles se han convertido en herramientas de trabajo de uso común, con la plenitud del IoT, indudablemente la dependencia a internet aumentará y para poder hacer un buen uso funcional de los dispositivos que se tengan disponibles en su momento se requerirá de un acceso a una mayor cantidad de información y, por ende, de datos personales.

Veremos grandes desafíos al entrar el IoT en nuestras vidas, ventajas y desventajas, indudablemente una de ellas será el manejo de los datos personales; tema que hoy en día preocupa a distintos gobiernos, organismos, empresas y a la sociedad en general, esa amenaza a la seguridad y a la privacidad del usuario. De acuerdo con Romero (2017), sin duda, el manejo de gran cantidad de datos es una de las ventajas de IoT. Pero la desventaja es el uso que hagamos de ellos. No sólo los datos que proporcionemos serán válidos, también lo serán los que se puedan derivar de la recopilación, análisis y cruces entre dispositivos.

El comportamiento en el manejo de este gran cúmulo de información de los usuarios será el tema que se debatirá entre los Estados que en estos días luchan por los derechos y la protección de los datos personales, con estos nuevos desafíos, el *Convenio 108* continuamente se está revisando para adaptarse a las nuevas realidades. El Consejo de Europa trabaja en su modernización, pero no hay que dejar de preguntarnos ¿los gobiernos tendrán ventaja en tiempo ante el Internet de las Cosas? Posiblemente el IoT avance más rápido que las reformas necesarias a las leyes de protección de datos personales, o quizá sea lo contrario. Con las prospectivas que se tienen sobre internet y en un sentido positivo esperemos que las leyes vayan adelantadas y estén en espera del gran cambio que se avecina en internet.

Por su parte la sociedad red debe tener mayor información sobre el tema de la protección de datos personales, pues la gran oferta de "aplicaciones para dispositivos móviles, que hoy en día permiten al usuario estar conectado a internet, recaban datos personales en cantidades considerables, lo cual hace posible un monitoreo digital continuo, sin que los usuarios estén conscientes a menudo de que esto sucede" (García, 2016 [en línea]).

La protección de datos personales debe ser una necesidad apremiante tanto en los ámbitos mundial y nacional, puesto que los usuarios son susceptibles de vulneraciones a la protección de su información, que en la mayoría de los casos —como ya se comentó— no hay conocimiento o consciencia de la cantidad de datos que aportan diariamente en internet. En este universo de información, la exploración sobre algún dato en particular quedará en manos de la minería de datos, campo disciplinario en donde convergen la estadística y la computación para mostrar en sus resultados patrones y comportamientos de un determinado objeto de estudio, a partir de la recolección, extracción, almacenamiento y análisis estadístico de grandes volúmenes de información.

Conclusión

Compartimos, por último, la siguiente reflexión: de acuerdo con cifras del Inegi, en 2018, México alcanzó los 74.3 millones de internautas. Si realizáramos una dinámica, que al menos 50% de estos usuarios de internet solicitaran su carta de los derechos ARCO, podríamos conocer la eficiencia que tiene nuestro país para

con la protección de datos personales. Y pensar ¿cómo será el actuar de nuestras leyes ante la plenitud del IoT? ¿La minería de datos es una disciplina emergente en la solución al manejo de la protección de datos personales? Respuestas que se confirmarán en un futuro cercano.

Referencias

Bibliografía

Frosini, V. (1982). *Cibernética, derecho y sociedad*. Tecnos, Garriga, Madrid.

Garriga Domínguez, Ana (2010). *Tratamiento de datos personales y derechos fundamentales: desde Hollerith hasta internet,* Universidad de Vigo, España.

Kuneva, M. (2009). *Discurso de apertura ponencia dictada en la Mesa redonda sobre recopilación de datos en línea, focalización y perfiles,* Comisión Europea.

Latorre Ariño, Marino (2018). *Historia de las web,1.0, 2.0, 3.0 y 4.0,* Universidad Marcelino Champagnat, Perú.

Pérez Maldonado, V. (2012). *Protección de datos personales en la administración de justicia federal* en Ferrer Mac-Gregor, E. (coord.), *Procesalismo científico. Tendencias contemporáneas*, UNAM, México,

Romero García, María Teresa (2017). *La protección de los datos ante el internet de las cosas.* Tesis de ingeniería, Universidad Politécnica de Madrid, España.

Troncoso Reigada, A. (2010). *La protección de datos personales en busca del equilibrio.* Tirant lo Blanch, España.

Mesografía

Cámara de Diputados del H. Congreso de la Unión (2017). "Ley general de protección de datos personales en posesión de sujetos obligados", *Diario Oficial de la Federación*, [en línea]. Disponible en http://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf, consultado el 14 de mayo de 2017.

Cambronero, Fátima (2018). "México adhiere al Convenio 108", [en línea]. Disponible en https://www.riosabogados.com/convenio-108/mexico-adhiere-al-convenio-108/, consultado el 14 de mayo de 2019.

Casagras (2014). "RFID and the inclusive model for the Internet of Things", [en línea]. Disponible en https://www.rfidjournal.com/articles/view?4461/3, consultado el 12 de agosto de 2019.

Consejo de Europa (2001). *Protocolo adicional de Convenio 108 para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y relativo a transferencias de datos*, Francia, Consejo de Europa, [en línea]. Disponible en https://www.oas.org/es/sla/ddi/docs/U12%20convenio%20n%20108.pdf, consultado el 14 de junio de 2019.

Comisión Europea (1998). *La información del sector público: un recurso clave para Europa. Libro verde sobre la información del sector público en la sociedad de la Información*, Francia, Consejo de Europa, [en línea]. Disponible en https://gobiernoabierto.navarra.es/sites/default/files/opendata/libro_verde_informacion.pdf, consultado el 14 de mayo de 2019.

Diario Oficial de la Federación (2018). *Decreto promulgatorio del protocolo adicional al convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, a las autoridades de control y a los flujos transfronterizos de datos, hecho en Estrasburgo, Francia, el ocho de noviembre de dos mil uno.* Disponible en https://dof.gob.mx/nota_detalle.php?codigo=5539474&fecha=28/09/2018, consultado el 12 de septiembre de 2018.

García Flores, Marcos (2016). "Los datos que tenemos en la nube ¿están seguros? [en línea]. Disponible en https://u-gob.com/los-datos-tenemos-en-la-nube-estan-seguros/, consultado el 2 de mayo de 2020.

Ifai, Instituto Federal de Acceso a la Información Pública (2019). *Guía práctica para la atención de solicitudes de ejercicio de los derechos ARCO*. Disponible en http://inicio.ifai.org.mx/Publicaciones/02GuiaAtencionSolicitudesARCO.pd, consultado el 12 de julio de 2019.

Inai, Instituto Nacional de Acceso a la Información y Protección de Datos (2019). *Convenio 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* en *Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*, [en línea]. Disponible en http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf, consultado el día 19 de enero de 2019.

Inegi, Instituto Nacional de Estadística y Geografía (2019). "Estadísticas a propósito del Día Mundial del Internet (17 de mayo). Datos nacionales" Disponible en https://www.inegi.org.mx/contenidos/saladeprensa/aproposito/2019/internet2019_Nal.pdf, consultado el 3 de agosto de 2019.

Infoem, Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios (2019). "¿Qué es una solicitud de derechos arco?", [en línea]. Disponible en http://www.infoem.org.mx/src/htm/queEsArco.html, consultado el 3 de julio de 2019.

Noda Camacho, Esther María (2013). "Internet de las cosas: beneficios y privacidad, un difícil equilibrio", [en línea]. Disponible en http://docplayer.es/19451537-Titulo-internet-de-las-cosas-beneficios-y-privacidad-un-dificil-equilibrio.html, consultado el 6 de septiembre de 2019.

Remolina Angarita, Nelson (2010). "¿Tiene Colombia un nivel adecuado de protección de datos personales a la luz del estándar europeo?, *Revista Colombiana de Derecho Internacional*, pp. 489-524, [en línea]. Disponible en https://revistas.javeriana.edu.co/index.php/internationallaw/article/view/1384, consultado el 11 de enero de 2019.

VI

AUSENCIA DE DATOS DEL DESPLAZAMIENTO FORZADO POR LA VIOLENCIA CRIMINAL: EL ESTADO DE MÉXICO EN LA PERSPECTIVA NACIONAL

Martha Elisa Nateras González

Introducción: Desplazamiento Interno Forzado (DIF): contexto y qué es

Desde la declaratoria de guerra al narcotráfico y a la delincuencia organizada por parte de Felipe Calderón a finales de 2006, de 2007 a 2018 se han registrado 407,340 homicidios, de los cuales el 14% aproximadamente fueron asesinados a raíz de la ola de la violencia criminal." Esto es porque la declaratoria de guerra la hizo en diciembre de 2006 y la cifra de homicidios es del periodo de 2007 a 2018. Una de las consecuencias más graves del combate frontal a la delincuencia organizada y de la descontrolada violencia criminal son los llamados *daños colaterales*, que terminan por afectar a la población civil de muchas formas, una de ellas es el desplazamiento de personas, debido a que son o han sido víctimas de la coacción directa y las amenazas físicas (CNDH, 2016).

Este fenómeno apenas se empieza a reconocer como un problema social, pues históricamente nuestro país ha sufrido de desplazamiento y migración, pero motivados por cuestiones económicas, políticas, étnicas o religiosas; no obstante, en la actualidad, la proporción de personas que abandonan municipios violentos es entre cuatro o cinco veces mayor que la de personas que abandonan municipios por otro tipo de motivaciones. Desde hace varios años, tanto la Comisión Nacional de Derechos Humanos (CNDH) como otros organismos, han venido señalando la importancia de un registro oficial, para tener los datos precisos sobre desplazamiento forzado interno.

Este problema, no obstante, no se ha reconocido sólo por miopía institucional, también porque

> el desplazamiento interno por violencia no es una diáspora homogénea que parte de un origen único y sigue el trazo de caminos establecidos, tampoco se impone solo a sectores desposeídos en términos económicos, ni a población vulnerable desde el punto de vista socioeconómico; afecta desde individuos, familias, pasando por comunidades, hasta abarcar municipios o regiones enteras, pertenecientes a los más diversos estratos económicos y culturales (Díaz y Romo, 2019: 20-21).

Según el *Informe Especial sobre Desplazamiento Forzado Interno en México*, que presentó la CNDH en mayo de 2016, de 35 433 víctimas de desplazamiento forzado, 90% es por la delincuencia, los municipios más afectados con esta problemática se ubican en la zona fronteriza del país; no obstante, los municipios que están despoblándose se reparten en todo el país, pero hay tres zonas principales de despoblamiento debido a conflictos entre organizaciones criminales:

1. Noroeste y occidente: por la presencia del Cártel del Pacífico.
2. Noreste: por ser zona de influencia del Cártel de los Zetas.
3. Sur-sureste: por la Familia Michoacana y los Caballeros Templarios

El problema principal de este fenómeno es que no estaba visibilizado; por ello, amenaza con crecer porque se ha potencializado el dominio territorial de los cárteles de la droga y lo etéreo de éste dificulta su registro, de tal suerte que no existe una instancia institucional que concentre esta información, dificultando la generación de políticas públicas para su atención. Por tanto, el objetivo de este capítulo es llevar a cabo una primera revisión de cuál es la situación actual del Estado de México, en el contexto nacional, en materia de desplazamiento forzado por la violencia criminal, así como el crecimiento de los grupos delictivos en esta entidad.

Según datos del Banco Mundial (2014), la violencia es una de las principales causas de muerte entre la población de 15 a 44 años, pues anualmente alrededor de 1.6 millones de personas pierden la vida violentamente en todo el mundo. En este orden de ideas, América se caracteriza por ser un continente con altos niveles de violencia, en específico América Latina, región que registra la tasa de homicidios más alta. El problema se potencializa porque los elevados niveles de homicidio,

en esta zona del mundo, están asociados con la delincuencia organizada y las pandillas. Esta asociación, lamentablemente, acrecienta el carácter destructivo de la violencia, debido a que su expansión tiene inmensos costos en la medida que atenta cada vez más contra las solidaridades colectivas e impacta de manera negativa en la confianza que la ciudadanía debería tener en las instituciones encargadas de la seguridad y la impartición de justicia (Nateras, 2018).

El registro oficial del desplazamiento, así como la protección de los datos de las personas que se encuentran huyendo de la violencia es fundamental; respecto al registro, destaca la labor que está llevando a cabo el Inegi en el censo de población 2020, pues en esta emisión se está explorando respecto a esta problemática, y el reto es contar con datos veraces y por supuesto proteger esa información para salvaguardar la vida y la integridad de las personas que temen que los alcancen las redes de poder de los grupos delictivos.

Si se parte de la premisa de que no hay guerra justa, pues aunque el Estado tenga razones legítimas para entrar en guerra, amparado en el *Ius ad Bellum,*[1] inevitablemente la sociedad civil sufrirá las consecuencias de ésta, por eso algunos organismos internacionales, como la Organización de Naciones Unidas (ONU), al concluir la Segunda Guerra Mundial, han venido generado distintos acuerdos para salvaguardar a la población de dicho sufrimiento provocado por las guerras. El primer esfuerzo que se llevó a cabo fue en la *Convención sobre el Estatuto de los Refugiados*, de 1951; en esta reunión, varios países manifestaron su voluntad para hacer frente al tema del Desplazamiento Interno Forzado (en adelante DIF), reconociendo sobre todo la figura de refugiado. Treinta años después, en la *Declaración de Cartagena sobre Refugiados*, de 1984, se solicita que en esta figura de refugiado se incluya a las personas que huyen de las amenazas que representa la violencia generalizada, la agresión extranjera, los conflictos internos, la violación masiva de los derechos humanos u otras circunstancias que hayan perturbado gravemente el orden público (Albuja, 2014 [en línea]).

El problema de enfocar la atención a la figura del refugiado es que las personas que se ven obligadas a salir de sus comunidades, sin salir de sus países, tienden a ser menos visibles que los refugiados y por consiguiente son más vulnerables, pues

[1] Término que se refiere a las legítimas razones que un Estado tiene para entrar en guerra.

no existe ninguna convención internacional vinculante que atienda a las Personas Internamente Desplazadas (en adelante PID), ya que sólo se cuenta con los Principios Rectores sobre Desplazamiento Interno de la ONU, el inconveniente es que éstos dependen de la buena voluntad de los gobiernos para ser respetados. La invisibilidad de las PID se debe a varios factores, entre las que destacan: al salir de sus comunidades se instalan con familiares o amigos; el desplazamiento ocurre de manera gradual o *gota a gota*, esta situación dificulta la capacidad de detección por parte de las autoridades; los DIF son fácilmente de confundir con otros tipos de migración interna y, finalmente, porque con frecuencia no quieren ser identificados por temor a las represalias de la comunidad, de las autoridades gubernamentales y los grupos armados de los que están huyendo. Este último factor, que conlleva cierto grado de violencia, es el que hace necesario que el DIF se visibilice para garantizarles a las PID ayuda humanitaria (Rubio, 2014 [en línea]).

El DIF es un mecanismo de supervivencia de poblaciones civiles en situaciones extremas, frente a regímenes de violencia interna que evidencia la incapacidad de las instituciones gubernamentales para garantizar la vida de los que se ven obligados de huir de sus lugares de origen. Dicha incompetencia se puede caracterizar como una decisión política frente a un escenario territorial en conflicto y con actores hegemónicos en disputa y amenazantes, quienes exigen acatamiento, obediencias y complicidades en dinámicas de clandestinidad y omisión; lo anterior implica que las personas o la comunidad amenazada deben tomar las riendas de su situación frente a las instancias gubernamentales que no les pueden garantizar sus derechos y salir del peligro que representan los poderes fácticos que violentan su permanencia. Así, el DIF es un proceso de varias movilizaciones, con la mayor cantidad posible de personas, que salen con el mayor sigilo y con pocas pertenencias, esperando regresar cuando mejore la situación (Salazar y Castro, 2014).

El DIF, según Luz María Salazar y José María Castro (2014), ha sido reconocido desde tres perspectivas: 1) como el resultado de conflictos sociales; 2) como un problema sociológico y 3) como un problema considerado en el derecho humanitario internacional.

Al respecto, la CNDH menciona:

> Los organismos y órganos internacionales que estudian los fenómenos migratorios desde la perspectiva del derecho internacional de los derechos humanos y el derecho internacional humanitario, han considerado tradicionalmente a la migración forzada como el tipo de movilidad humana provocada por anomalías o conflictos que no tienen que ver directamente con procesos económicos.
>
> Esta noción del DIF se articula en tres elementos principales: 1. la condición de urgencia y apremio que obliga a las personas para desplazarse de su lugar o comunidad de origen; 2. las características de las condiciones contextuales en el lugar de residencia que motivan a las personas a desplazarse; y 3. el aspecto geográfico que diferencia este fenómeno y a sus víctimas, de los refugiados y de las personas con necesidad de protección internacional.
>
> De acuerdo con la Comisión Nacional de Derechos Humanos (CNDH) las diferentes causas del DIF deben entenderse a la luz del Derecho Internacional Humanitario, que clasifica diversas situaciones que conllevan distintos niveles de violencia, así como constatando la estrecha vinculación que existe entre el origen y desarrollo de las normas de protección de los desplazados internos con el derecho internacional de los refugiados.
>
> Las diferentes causas del DIF señaladas en los Principios Rectores del Desplazamiento Interno Forzado de la ONU son: conflicto armado; violencia generalizada; violaciones de los derechos humanos; catástrofes naturales o provocadas por el ser humano, y proyectos de desarrollo. Por tanto, son PID aquellas personas que se han visto forzadas u obligadas a escapar o huir de su hogar o de su lugar de residencia habitual, como resultado o para evitar los efectos de un conflicto armado, de situaciones de violencia generalizada, de violaciones a los derechos humanos o de catástrofes naturales o provocadas por el ser humano, y que no han cruzado una frontera estatal internacionalmente reconocida (CNDH, 2016: 8-10, 16).

Según estos principios rectores para que se pueda considerar a los individuos como PID debe existir coacción; no obstante, algunas personas se desplazan cuando su fuente de ingresos ha disminuido o se ha visto vulnerada a casusa del clima de violencia e inseguridad, sin que necesariamente hayan sido violentados directa o abiertamente, pero esa decisión no ha sido del todo libre (Albuja, 2014).

En la actualidad, el DIF, de acuerdo al Observatorio de Desplazamiento Interno del Consejo Noruego para Refugiados (IDMC: International Displacement Monitoring Centre, por sus siglas en inglés) 33.3 millones de personas han sido desplazadas al interior de sus países en todo el mundo a causa de la violencia, situación que, sin duda, representa una tragedia en términos humanitarios, sobre todo porque ha pasado inadvertida, lo que —como ya se dijo— los ubica en un estatus de extrema vulnerabilidad. Esta fragilidad se manifiesta de varias maneras, entre ellas: la falta de protección física; el resarcimiento del daño ocasionado por la pérdida de sus seres queridos; la pérdida de sus medios de subsistencia y su patrimonio familiar; en la búsqueda de un lugar más seguro, se enfrentan a situaciones desconocidas, a nuevos riesgos y a una serie de carencias: servicios de salud, vivienda, trabajo y educación; la invisibilidad, de la que ya se hizo referencia, y la destrucción del tejido social, provocando desarraigo y pérdidas irreparables que en el corto y largo plazo promueven daños psicológicos de gran impacto para amplios sectores de la población. En este sentido, este proceso deja a los DIF en el limbo legal, por tanto la responsabilidad de brindarles protección por parte del Estado se diluye, debido a que no traspasan fronteras internacionales, imposibilitándolo para brindarles la atención, seguridad y asistencia que requieren; pero también por la debilidad del Estado que no los protegió previamente para evitar el desplazamiento (Rubio, 2014).

En esta lógica, como señala Laura Rubio (2014) en la mayoría de los países, con grandes problemas de DIF no existe el andamiaje conceptual, legal e institucional necesario para atender esta situación o para prevenirla; esto se debe en parte porque la mayoría de los gobiernos no reconocen que tienen graves problemas de violencia generalizada que está ocasionando DIF. Debido a ello, la crisis de DIF en el ámbito mundial tardará décadas en atenderse y resolverse, lo grave es que desampara a miles de personas y las condena a permanecer en situación de DIF prolongado, con todo lo que esto implica. Por ello, la CNDH manifiesta:

> La comunidad internacional ha acogido los Principios Rectores como el marco normativo en el tema. Estos Principios recogen los derechos contenidos en varios instrumentos internacionales de derechos humanos y de derecho internacional humanitario, muchos de los cuales ha suscrito México y por ende constituyen derecho positivo en nuestro país (2016: 19).

El DIF es un problema que suele estar asociado a la guerra o a un conflicto armado en cualquier modalidad, por tanto es común encontrarlo en los países que viven o han vivido una situación de esta naturaleza, pues desde la década de 1980 se ha registrado el traslado de miles de personas como resultado de las guerras civiles en Centroamérica y los problemas de guerrillas; en la última década, la situación se ha incrementado como resultado de la violencia y la inseguridad que han provocado el crimen organizado y el narcotráfico (Rubio, 2014). En el ámbito global, América Latina ocupa el tercer lugar entre las regiones con más desplazados internos en el mundo con aproximadamente 6.3 millones de personas en 2014 (Rubio, 2014).[2] En 2015 se registró un incremento de 8.6 millones de personas, en 2016 disminuyó a 6.9 millones de personas (Díaz y Romo, 2019).

En este sentido, el DIF se entiende como la huida o escape de una persona, una familia o un grupo de personas que son forzadas a dejar su residencia habitual para huir de conflictos armados, situaciones de violencia generalizada o violaciones sistemáticas de sus derechos humanos. Se puede argumentar que las causas que generan los desplazamientos forzados no permiten ningún tipo de decisión planeada, ya que por lo general estos procesos se dan intempestivamente y con escasas pertenencias, pues es una estrategia de sobrevivencia y puede ser de manera temporal o definitiva (Gómez *et al.,* 2003; Gámez, 2013; Salazar y Castro, 2014).

El primer movimiento de desplazamiento, según Salazar y Castro (2014), se lleva a cabo al interior de un país y por lo regular cercano a la localidad que los expulsó, debido a que se piensa que es una medida temporal y que pronto estarán de vuelta, lo cual es cada día más complicado ante el panorama y la situación de conflicto que lejos de disminuir, en el corto plazo, se tiende a agudizar. Debido a que esta problemática tiene su origen en las violencias; en el índice delictivo; problemas de seguridad humana y material; riesgos; amenazas; incertidumbres; abusos y violación de los derechos humanos, que se traduce en una crisis humanitaria, de la cual son corresponsables los poderes fácticos y los actores militarizados institucionales.

[2] Según las cifras de la Agencia de la ONU para los Refugiados (ACNUR), en 2015 se registró un incremento acumulado en el ámbito mundial de 40.8 millones de personas internamente desplazadas, de las cuales 8.6 millones se desplazaron ese año; Colombia fue el primer lugar, con 6.9 millones; le siguió la República Árabe de Siria, con 6.6; después Irak, con 4.4; Sudán, con 3.2 y Nigeria, con 2.2 millones (Díaz y Romo, 2019).

El DIF en México por causas delictivas

Las causas del DIF son múltiples, complejas y entreveradas. En México se pueden tipificar en cinco rubros: 1. Políticas (represión), 2. Religiosas, 3. Agrarias, 4. Delictivas y 5. Extractivistas. También las hay por desastres naturales (CNDH, 2016).

Aquellos que se mudan a otro lugar en busca de una fuente de ingresos, pero que no lo habrían hecho de no ser por el impacto negativo de la inseguridad y la violencia sobre sus medios de vida, tienen el derecho legítimo de solicitar protección como desplazados internos con el argumento de que se vieron obligados a marcharse por el clima de inseguridad (Albuja, 2014).

En México se tiene registro de DIF desde la década de 1970, pero como resultado de la intolerancia religiosa, de conflictos comunales, así como por pugnas por tierras y recursos naturales en estados como Nayarit, Hidalgo, Oaxaca, Guerrero y Chiapas, entre otros. En 1994 por causa del levantamiento zapatista en Chiapas se presentó un enorme DIF en el país, el cual se combina con la creciente inseguridad; se estima que, hasta 2014, más de 30 000 personas se encontraban en condición de DIF permanente, debido a que no habían recibido la atención necesaria (Rubio, 2014).

Si bien es cierto que la violencia y la inseguridad no requieren de un contexto de guerra o conflicto armado para que se presenten, la situación de violencia que vive en la actualidad México se asemeja a la de una guerra, pues reúne los criterios establecidos por el Derecho Internacional Humanitario (DIH) y por tanto es equiparable a la de una crisis humanitaria (Albuja, 2014).

En el caso de México, el desplazamiento de civiles ha sido una de las más importantes consecuencias de las violencias derivadas del crimen organizado y de la guerra contra éste por parte del Estado. Según información del Secretariado Ejecutivo del Sistema Nacional de Seguridad Pública (SESNSP) 47 000 personas fueron asesinadas a raíz de la ola de intensa violencia criminal que se inició de 2007 a 2018. Los cálculos se elevaron a 70 000 civiles para abril de 2012 (Albuja, 2014). Según la CNDH "en los últimos años, es una violencia diferente la que provoca la movilidad de las personas, pues se relaciona con grupos armados que están azotando diversas partes del territorio nacional; esta violencia no se ha podido frenar por parte de las autoridades, lo que ha provocado desprotección de las víctimas" (2016: 3).

De acuerdo con las cifras del SESNSP, desde la declaratoria de guerra al narcotráfico y a la delincuencia organizada por parte de Felipe Calderón, de 2007 a 2018 se han registrado 407 340 homicidios, se presume que de este total, 14% al menos fueron asesinados a raíz de la ola de la violencia criminal. Si bien es cierto que la incidencia delictiva se disparó desde entonces, una de las consecuencias más graves del combate frontal a la delincuencia organizada y de l*a descontrolada violencia criminal* es el desplazamiento de personas, debido a que son o han sido víctimas de la coacción directa y han sido amenazadas físicamente. Por ello, el DIF es otra de las consecuencias de la violencia estructural en México, que no se ha dimensionado, puesto que apenas se empieza a reconocer como un problema social. Una de las razones de esta falta de visión es que históricamente nuestro país ha sufrido de desplazamiento y migración, pero motivados por cuestiones económicas; no obstante, actualmente la proporción de personas que dejan municipios violentos es entre cuatro o cinco veces mayor que la de personas que abandonan municipios por otro tipo de motivaciones.

Hasta 2013, la CNDH incluyó en su agenda el tema de DIF derivado de la violencia del crimen organizado y reconoció la existencia de 150 000 personas víctimas del DIF, señalando también que las entidades más afectadas por esta situación eran Chihuahua, Tamaulipas, Michoacán, Durango y Sinaloa y separa el caso de Chiapas, estado que padece esta realidad desde la década de 1990 (Salazar y Castro, 2014). Sin embargo el registro no es confiable y por tanto no existe un diagnóstico sólido que oriente las políticas de protección y asistencia, conforme a los estándares internacionales.

Los municipios más afectados con esta problemática, por un lado, son los que se ubican en la zona fronteriza del país; sin embargo, este fenómeno amenaza con crecer debido al incremento de la delincuencia, tanto la común, como la organizada, pero sobre todo porque ha crecido el dominio territorial de los cárteles de la droga. Entre 2010 y 2015, se redujo de 6.1 a 5.4 la proporción de personas desplazadas, al respecto también se observaron cambios, entre ellos: una disminución en la atracción en los estados de Baja California, Estado de México y Nuevo León; en cambio Campeche, Colima, Hidalgo, Querétaro y Yucatán fueron centros de atracción y en Michoacán se incrementó la expulsión (Díaz y Romo, 2019).

Por otro lado, según el *Informe Especial sobre Desplazamiento Forzado Interno en México*, que presentó la CNDH en mayo del 2016, los municipios que están despoblándose se reparten en todo el país, pero la mayor parte se concentran en tres polígonos ubicados en las principales zonas de conflicto entre organizaciones criminales: el noroeste y occidente, dominado por el Cártel del Pacífico; el noreste, controlado por el Cártel de los Zetas; y en el sur-sureste, en los estados dominados por la Familia Michoacana y los Caballeros Templarios.[3]

El mismo informe señala que de un total de 35 433 víctimas de desplazamiento forzado, 90% es por la delincuencia, pues los grupos criminales cuando se instalan en una nueva comunidad comienzan a reclutar de manera forzada a los jóvenes y adultos para "trabajar" con ellos mediante la amenaza y actos de violencia extrema, situación que lleva a muchas personas a abandonar su lugar de residencia. Esto se puede observar por la tendencia de decrecimiento de la población que están experimentado los municipios en México, fenómeno que comenzó en la última década.

La década de 2010 está marcada por la lucha contra el narcotráfico por parte de Felipe Calderón, por una fallida estrategia de seguridad y por la lucha entre los cárteles de la droga, lo que en su conjunto ha provocado la fragmentación de los grupos delictivos, división que ha estado mediada de luchas internas y entre grupos por el control territorial, los cuales se han expandido a lo largo y ancho del territorio nacional. Al dividirse estas organizaciones también se amplía la cartera de actividades delictivas; los cárteles más grandes mantienen el control del tráfico transnacional de drogas y los grupos que han surgido de esta fragmentación centran su actividad criminal en delitos, como el secuestro, la extorsión, el

[3] Laura Rubio menciona: "por ejemplo, en 2010, la violencia entre los cárteles de la droga, y de éstos con las fuerzas de seguridad pública fue particularmente aguda en Tamaulipas debido al enfrentamiento de los Zetas y el Cártel del Golfo por el control de las rutas del narcotráfico. En noviembre de ese año, después de que los Zetas emitieron una amenaza en contra de los habitantes de Ciudad Mier, 400 personas salieron huyendo. También en Michoacán, en mayo de 2011, un enfrentamiento en la tierra caliente entre la Familia Michoacana y los Caballeros Templarios provocó tanto la muerte de varias decenas de personas, como el desplazamiento de un gran número de familias que buscaron refugio en ciudades aledañas. Desde 2013, en este estado, al igual que en Guerrero, han ocurrido varios episodios de desplazamientos masivos como resultado de la proliferación de fuerzas de autodefensa y la profundización de los enfrentamientos entre éstas, bandas delictivas y fuerzas del Estado" (2014: 120).

cobro de derecho de piso, microtráfico y otras actividades ilegales, pero que les permiten tener el control de un territorio en específico (Rubio, 2014). Por tanto, el DIF de decenas de miles de personas se ha debido al crecimiento de la violencia criminal, a la expansión y división de los grupos delictivos y a las operaciones militares para combatirlos.

Esta ampliación de actividades por parte del crimen organizado ha derivado en una sistemática violación a los derechos humanos de miles de civiles que han muerto debido al fuego cruzado o como víctimas directas de estos criminales, al ser en ellos en quienes recaen sus acciones delictivas. Esto ha terminado por crear un clima generalizado de inseguridad, desesperanza e impotencia, que aderezado con la corrupción e impunidad que caracterizan a las instituciones del Estado, han orillado al DIF, por tanto, a ser un recurso tanto reactivo, como preventivo (Rubio, 2014).

En el *Informe sobre la Situación de los Derechos Humanos en México* que publicó la Comisión Interamericana de Derechos Humanos (CIDH) el 31 de diciembre de 2015, entre otros temas que preocupan es que la violencia relacionada con el crimen organizado ha conllevado a que miles de personas se hayan visto forzadas a desplazarse internamente en México durante los últimos años, pero sobre todo, se insiste en la gravedad del problema del DIF en nuestro país, pues esto se incrementa por la ausencia de cifras oficiales y la falta de reconocimiento por parte de las autoridades mexicanas de la existencia de este problema, lo que provoca su invisibilidad.

Las estadísticas del Instituto Nacional de Estadística y Geografía (INEGI) señalan que entre 2010 y 2015 el número de municipios que redujeron su población llegó hasta 691 (de 2 446 municipios, esto equivale a 28%); no obstante, sólo 1% migró por violencia. Este fenómeno fue documentado en octubre de 2015 por una delegación de la Comisión Interamericana de Derechos Humanos que visitó México. Después informó que la existencia de graves violaciones a los derechos humanos se debe a diversas formas de violencia en México, durante los últimos años, vinculadas al DIF. Según el propio organismo, esta violencia la ejerce el crimen organizado, grupos que por lo general están coludidos con las distintas organizaciones policiacas del Estado. De acuerdo con Sebastián Albuja:

> Este desamparo de las víctimas, incluidas las que migran como consecuencia de la violencia criminal, resulta significativo en contextos de violencia criminal intensa como es el caso de México. El marco de protección internacional existente [...] pone el debido énfasis en los derechos, las necesidades y las vulnerabilidades de las víctimas, incluidas aquellas que se mudan a otros lugares por culpa de la violencia criminal o a quienes les afecta. Pero los esquemas de protección se centran en los desplazamientos forzados o por culpa de la coacción (2014: 29).

Según el informe de 2017 de la Comisión Mexicana de Defensa y Promoción de Derechos Humanos (CMDPDH), durante ese año se registraron 25 episodios de DIF masivo en nuestro país, las entidades que padecieron esta problemática fueron Guerrero, Michoacán, Sinaloa, Chihuahua, Durango, Chiapas y Oaxaca, afectando a 20 390 personas, de éstas 12 323 eran población indígena. El estado con más PID fue Chiapas, con 6 090 personas (29.87%); en segundo lugar fue Guerrero, con 5 948 (29.17%) y en tercer lugar se ubicó Sinaloa, con 2 967 PID (14.55%). Del total de PID, 55.09% se desplazó debido a la violencia generada por grupos armados organizados, ya sea por ataques armados en contra de la población civil o por enfrentamientos armados entre delincuentes. Lo que identifica este informe es que 15 de los 19 episodios registrados la PID permaneció en la misma entidad federativa, y el resto se trasladó a diferentes entidades federativas (CMDPDH, 2018).

El caso de México, como se puede observar, no se sale de la dinámica o de la forma como se desenvuelve en otras latitudes, es decir, los estados con mayor índice delictivo es donde se experimenta DIF *por goteo*, pues la población sale de sus comunidades de manera individual o con su familia, lo que complica su identificación, así como los motivos que tuvieron para mudarse. Aunado con lo anterior, el Estado mexicano se ha mostrado indiferente o reacio a reconocer este fenómeno, que sin duda requiere de mucha atención. Asimismo, muchas PID cuando salen, lo hacen con la esperanza de regresar a sus lugares de origen y recuperar su patrimonio, pero muchas veces los grupos delictivos se apoderan de sus bienes. Esto constituye un incentivo para que las organizaciones delictivas provoquen el desplazamiento para apoderarse de los bienes de los desplazados (Mercado, 2016).

El DIF como causa y efecto de la delincuencia y de la inacción política

Como se ha venido señalando, la invisibilidad del DIF y por ende de las PID provoca que el Estado no ponga atención a esta situación tan complicada y trágica para la población que la padece, debido a que está en juego la vida de cientos de personas, que ante las circunstancias se ven obligadas a salir de su entorno con nada en las manos o con lo mínimo si tienen suerte.

Esta miopía política lo único que ha generado es inacción pública, haciendo que crezca este conflicto debido a que las personas se mueven dentro de los límites del mismo país, por lo que el problema sólo se traslada geográficamente. Hasta ahora la respuesta del gobierno mexicano al DIF ha sido nula o mínima, en el mejor de los casos, porque no ha querido reconocer que la violencia provocada por el narcotráfico y la delincuencia organizada está induciendo a que la gente se desplace —ya sea bajo coacción o no— y por ende no ha generado acciones públicas para responder a estos desplazamientos desde que la violencia penetró en algunos territorios (Albuja, 2014).

Por ejemplo, en Sinaloa la violencia del narco y del ejército provocaron desde la década de 1980 la desaparición de pueblos enteros en la sierra; estas PID emigraron a las ciudades de la frontera como Tijuana y California (Lizárraga, 2004). De esta forma, el narcotráfico extendió su dominio, estimulado en parte por la base social de apoyo que fue creando, la cual surge como resultado "natural" de que éste se aprovechó del vacío que dejaba la ausencia de programas gubernamentales de corte social, y por una narcocultura que fue permeando en el entorno simbólico y ha logrado penetrar en el imaginario social de los jóvenes.

En esta lógica, debido a que el DIF, vinculado con la violencia y como fenómeno muy localizado, su visibilización es directamente proporcional al reconocimiento oficial e institucional, pues mientras éste no sea formal, las acciones que lleven a cabo otros actores no estatales para apoyar a las PID serán de corte asistencialista. Por ello, ante la falta de una respuesta estatal para las PID afectadas por la violencia, algunas agencias humanitarias han orientado sus acciones a proteger a las personas que se han visto obligadas a moverse por esta razón. El dilema es, según Sebastián Albuja (2014), que ninguno de los organismos humanitarios instalados

en México, como la Agencia de la Organización de las Naciones Unidas para Refugiados (ACNUR), ha creado programas de apoyo para atenuar los impactos de la violencia criminal en comunidades específicas. Esto se debe en parte a que estos programas no se encuentran en su agenda, pero también por la falta de reconocimiento por parte del gobierno mexicano, pues en caso de que admitiera que existe un clima de violencia provocado por los cárteles de la droga, sería aceptar que el país se enfrenta a una crisis humanitaria y que se requiere de la ayuda de organismos internacionales, demostrando con ello incompetencia. Lo cierto es que uno de los reclamos que la población desplazada hace a las autoridades mexicanas es el de no atender sus demandas y necesidades. Esto ha provocado recelo en las instituciones del Estado, no sólo de los que padecen esta situación, sino también de la mayor parte de la sociedad. Esta desconfianza es resultado de la falta de políticas públicas, pero también debido a que en algunos espacios territoriales los ciudadanos no distinguen entre los integrantes de la delincuencia y los que forman parte de las distintas instancias de gobierno debido a la complicidad, protección y por el intercambio entre bandos (Díaz y Romo, 2019).

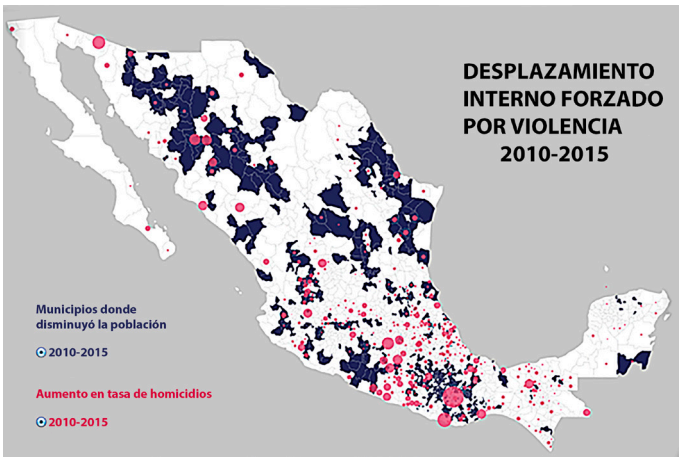
Una respuesta, que no deja de ser elemental, ante esta problemática tan compleja, es la creación en 2017 del *Protocolo para la atención y protección de las víctimas del DIF*, cuyo objetivo es establecer los lineamientos y criterios básicos que deben considerar los funcionarios de los tres órdenes de gobierno, para proteger y garantizar los derechos de las personas desplazadas. Los esfuerzos coordinados de las autoridades son fundamentales en esta labor. El problema es la ausencia de un marco jurídico que ampare las acciones para la protección de las víctimas de esta movilidad involuntaria (Díaz y Romo, 2019). Pero, como se ha venido planteando, la visibilización es el primer paso para generar las estrategias de atención de las PID.

Debido al incremento de PID en algunas regiones, en redes sociales, medios de comunicación, periodismo de investigación, autoridades religiosas, entre otros, se ha empezado a visibilizar y difundir distintos episodios de DIF. No obstante, como se ha señalado, no existen cifras confiables al respecto; por ello, las estimaciones se hacen sobre la magnitud del conflicto, la capacidad de ofensiva militar, la amenaza de los actores y sus exigencias a grupos de población, la población censal en las

localidades expulsoras, el incremento de población en las comunidades receptoras, y las narrativas de algunos eventos de violencia en donde se detecta que hubo desplazados (Salazar y Castro, 2014).

El mapa 1 muestra los datos del periodismo de investigación, el cual se dedica a recabar datos que las organizaciones gubernamentales no han querido documentar. En éste se muestra la relación entre tasa de homicidio y DIF.

Mapa 1

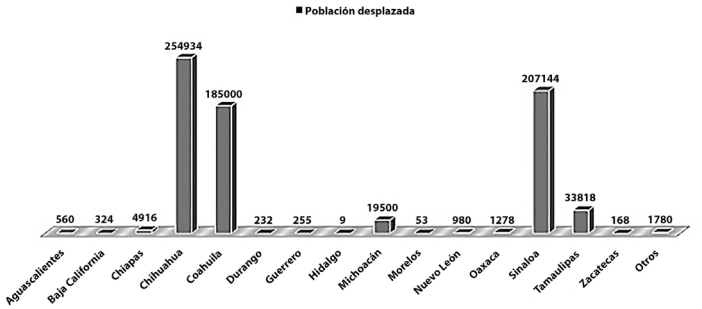


Fuente: Animal Político, 2017.

Cabe aclarar que para llevar a cabo esta investigación, sus bases de datos las construyen a partir de las estadísticas oficiales de población y homicidios, elaboradas por el INEGI, con estos datos hacen un comparativo entre los municipios que registraron un descenso poblacional entre 2010 y 2015, tomando como base los resultados del Censo General de Población y Vivienda 2010, con los de la Encuesta Intercensal en Hogares (2015) y la tasa de homicidio en el mismo periodo.

Gráfica 1

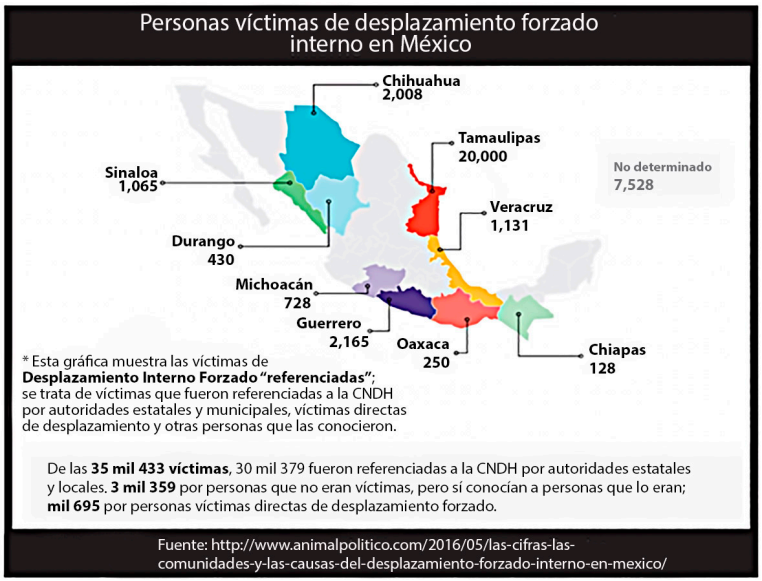
Desplazamiento forzoso por entidad federativa (2007-2012)



Fuente: Salazar y Castro, 2014: 65.

Como se observa, lo que distintas investigaciones llevan a cabo son aproximaciones; de esta manera, se puede visualizar la dimensión que ha adquirido el fenómeno. Pues como señalan Salazar y Castro (2014), el DIF en México se visualiza *a posteriori*, cuando se detecta que las comunidades de recepción de PID no pueden asumir el volumen de estas movilizaciones y se convierte en un problema social visible que afecta la dinámica de la localidad receptora. La decisión individual de quedarse en los primeros destinos, o moverse a otros lugares, los convierte en DIF por la violencia o si la decisión es de regresar a su lugar de origen, con todos los riesgos que ello implica, incluso la pérdida de su vida, los vuelve en víctimas silenciadas del DIF. De esta última situación, no hay registro ni investigaciones, porque no hay un reconocimiento de que estos flujos migratorios, y con características similares, representen un riesgo significativo para la población en general, por lo que se tiende a minimizar. Esto genera un subregistro; no obstante, a partir de la contabilización cotidiana que llevaron a cabo dichos autores de la noticia de los desplazamientos por violencia del crimen organizado durante un periodo de seis años (2006-2012) pudieron hacer un estimado de 700 000 desplazados no documentados, pero sí confirmados por distintas fuentes. En lo que sí coinciden estos estudios es que, en general, las víctimas son campesinos, indígenas, personas cuya economía es de subsistencia, activistas y defensores de derechos humanos, pequeños propietarios de negocios, empresarios, políticos, funcionarios y periodistas.

Mapa 2



Fuente: Animal Político, 2017.

Otro dato que aportan las investigaciones periodísticas es el número de PID de las distintas entidades federativas que más víctimas registran. Como se observa en el mapa 2, Tamaulipas es el estado que en 2016 registró un mayor número de víctimas, superando con mucho a los estados que también padecen esta problemática y el que menos registró fue Chiapas, es decir, el DIF en este estado representó sólo 0.6% de lo que sufrió Tamaulipas en ese año.

La respuesta de esta diferencia tan marcada se puede encontrar en lo que señalan Díaz y Romo (2019). Estos autores documentaron que las causas del desplazamiento por violencia varían entre las distintas regiones, pues no todos viven la misma problemática; por ejemplo en los estados del norte del país, que comparten frontera con Estados Unidos, el DIF está vinculado con el crimen organizado, sobre todo por la disputa de territorios para llevar a cabo la distribución y el tráfico de droga, cuyo destino es el vecino país del norte, así como por la guerra de las instituciones gubernamentales contra esta actividad ilícita. En el centro del país, los actos violentos se cometen contra individuos y pocas veces contra colectividades,

es decir, no necesariamente esta actividad delictiva se asocia con los grupos criminales, ya que pueden ser células de éstos, pandillas o de delincuentes que operan de manera aislada, que no buscan vincularse a los grupos poderosos, pero que incluso pueden decir que operan a nombre de éstos; por lo tanto, la afectación es más individual que colectiva. En este sentido, los principales delitos a los que se enfrentan las personas son pérdida patrimonial, secuestro o intento de secuestro, robo a casa habitación, robo de auto, extorsión, fraude, asociación con el crimen organizado, lavado de dinero, cobro por protección, narcotráfico y guerra contra el narcotráfico. La región sur tiene una complejidad diferente; por ejemplo, en el estado de Chiapas, los conflictos provocados son por la intolerancia religiosa, los intentos por constituir municipios autónomos, la militancia en partidos políticos de oposición y el movimiento armado zapatista. Todo ello ha generado numerosas tensiones sociales desde hace varias décadas.

La percepción de inseguridad y la gestión del miedo son elementos fundamentales en e DIF, pues

> quienes operan en la delincuencia avanzan a partir de instaurar el miedo, así logran deconstruir la identidad de sus víctimas. Al desterrar la tranquilidad, la cohesión del tejido social se fragmenta y los canales de comunicación se deterioran, creando un clima de desconfianza generalizada y temor donde impera el silencio, el cual imposibilita toda acción de defensa organizada. La denuncia representa más peligro que solución y se visualiza como un camino inútil. Al llegar a este punto, todo se percibe inseguro y reina la confusión (Díaz y Romo, 2019: 89).

Grupos delictivos en el Estado de México y DIF

Como lo muestran los mapas 1 y 2, así como la gráfica 1, el Estado de México no figura entre las principales zonas que registran despoblamiento debido a conflictos entre organizaciones criminales; no obstante, la migración en las comunidades rurales de esta entidad federativa no es nueva, se viene desarrollando desde hace varios años, principalmente en la zona sur de la entidad, que es la región con mayor tradición migratoria.

La migración de los mexiquenses del sur del Estado de México está determinada por varios factores, entre los que destacan: la práctica migratoria determinada por las condiciones socioeconómicas de la región; los escenarios de atracción-expulsión que han hecho sumamente atractiva la estrategia de emigrar y la construcción de redes sociales, sobre todo de tipo familiar, que provoca que este fenómeno se reproduzca.

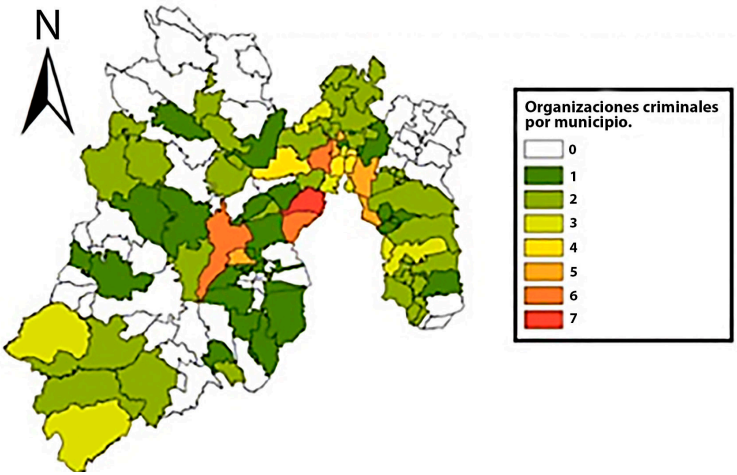
No obstante, a este fenómeno de desplazamiento se incorpora también el DIF motivado por el dominio territorial de distintos grupos delictivos. Pero, como sucede en el ámbito nacional, el Estado de México no es la excepción, es decir, el DIF no está documentado, por tanto para poder inferir la dimensión de este problema es necesario recurrir a otros datos. En este caso, se revisa el incremento de la presencia de grupos delictivos en la entidad.

Según Víctor Manuel Sánchez (2017) desde el 2009, se ha extendido e incrementado la presencia de organizaciones criminales en los 125 municipios del Estado de México debido a tres factores: 1. La fragmentación de las organizaciones criminales que operaban en el Estado de México. 2. El arribo de nuevos competidores a dicha entidad y 3. La concurrencia de varios grupos criminales en algunos de los municipios del estado. Esto, como se puede ver, no es exclusivo del Estado de México, más bien es el resultado de la guerra declarada al narcotráfico en 2006, que terminó por dispersar a los grupos delictivos y los puso a competir de manera más feroz, tanto por los liderazgos como por los territorios.

Retomando el recuento que hace Sánchez (2017) hasta mayo de 2014, había nueve organizaciones criminales que operaban en al menos 81 de los 125 municipios del Estado de México, tres años después, es decir, en 2017, su presencia se incrementó a 14 organizaciones criminales y se amplió su cobertura de operación a 96 municipios. Lo grave, para algunos espacios territoriales, es que la competencia entre éstos ha provocado que, en un mismo territorio, operen más de un grupo delictivo. Esto sucede con al menos 70 de los 96 municipios. Al respecto, los casos paradigmáticos son Ecatepec, allí operan ocho organizaciones criminales; en Nezahualcóyotl y Naucalpan se han registrado hasta siete; en Tejupilco, Tlalnepantla y Valle de Bravo operan seis y en Cuautitlán Izcalli y Coacalco, cinco (mapa 3). Si se hace una análisis superficial, lo que se puede observar es que son muchas organizaciones delincuenciales las que operan en una misma entidad;

sin embargo, como bien señala Sánchez (2017) en el centro de México no hay un cártel dominante, como sucede en otras partes del país, más bien esta región se caracteriza por la existencia de una compleja combinación de pequeñas bandas, que se han refugiado en estos territorios, debido a la fragmentación de las grandes organizaciones criminales. Este fenómeno es conocido como el efecto cucaracha.

Mapa 3. Número de grupos delictivos por municipio, 2014



Fuente: Sánchez, 2014.

El crecimiento registrado en los últimos tres años lo que muestra, revisando la información de Sánchez (2017), es que no por el hecho de que sean organizaciones relativamente pequeñas, no quiere decir que sus delitos sean de menor impacto; al contrario, pues sus actividades laceran directamente a la ciudadanía, de manera individual y colectiva, debido a que se concentran en actividades como la extorsión, el secuestro, el narcomenudeo, la trata de personas, el cobro del derecho de piso a los negocios y el comercio de productos piratas. Aunado con lo anterior, como sus ingresos se derivan de esas actividades ilícitas, son más combativos al cuidar su demarcación, afectando con esta disputa por el territorio a la población civil.

La organización criminal que tiene mayor presencia en el Estado de México es la Familia Michoacana, en la actualidad opera en 80 de los municipios. Las primeras

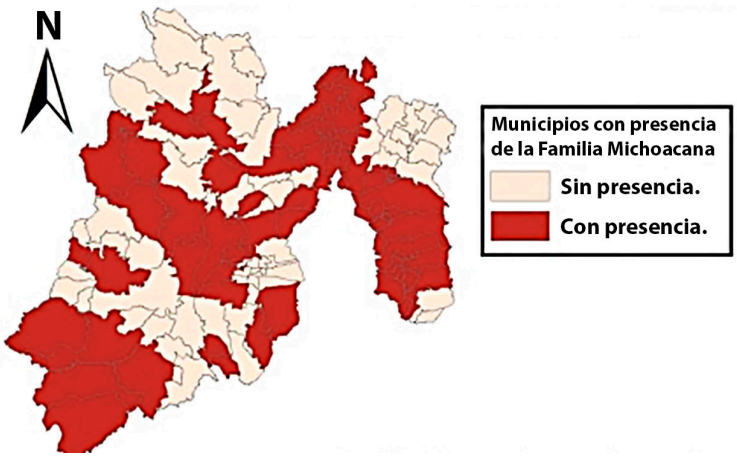
células de esta organización se instalaron en los municipios de Tejupilco, Toluca, Ecatepec, Nezahualcóyotl, La Paz y Valle de Chalco, posteriormente incrementó su ámbito de influencia al unirse con otras bandas locales (Sánchez, 2017) (mapa 4). Lo interesante de este grupo delictivo es que ha sobrevivido a los embates de sus conflictos internos, en este punto es importante señalar que desde su aparición en 2006, en Michoacán, mantuvo el dominio en esta entidad hasta 2010, pero después de una serie de disputas internas acompañado de una secuela de ejecuciones, en marzo de 2011, se anunció el surgimiento de una nueva organización denominada los Caballeros Templarios[4] (Nateras, 2018). Parte de su subsistencia se debe a que trasladó su centro de operaciones del sur de Michoacán, al Estado de México y a Guerrero, además de que su forma de operar es por medio de pequeñas bandas; por tanto, es una organización más horizontal, es decir, funciona como una especie de franquicia, esto permite un alto grado de independencia entre ésta (Sánchez, 2017). Actualmente, según la Procuraduría General de la República (PGR) tiene dos células operativas y sólo tiene presencia en Morelos, Guerrero y Estado de México.

La organización criminal que sigue en orden de importancia son los Caballeros Templarios;[5] sin embargo, de 2014 a la fecha ha registrado un descenso debido al abatimiento de la mayor parte de sus líderes. En 2014, tenían presencia en 40 municipios del Estado de México (mapa 5), en fechas recientes, todo parece indicar que su zona de influencia se concentra en los Valles de Toluca y México (Sánchez, 2017).

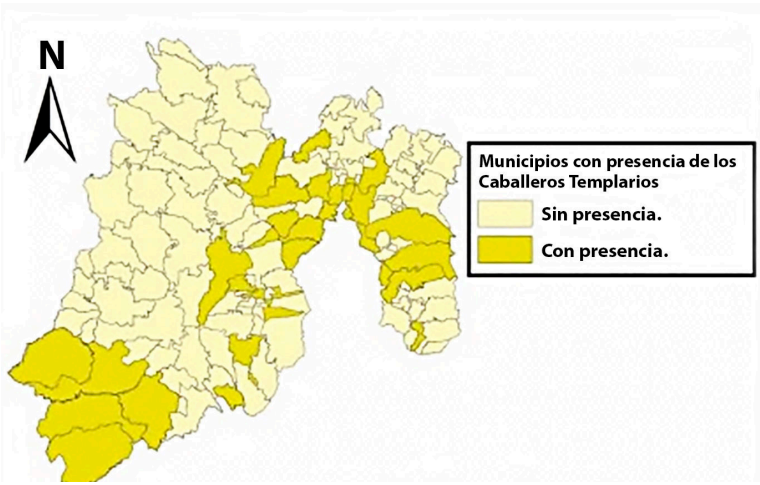
[4] A finales del 2010 circuló la noticia de que fue abatido Nazario Moreno, el Chayo, el principal fundador y pionero del cártel de la Familia Michoacana. Esa supuesta muerte, junto con la detención de José de Jesús Méndez, el Chango, el 21 de junio del 2011, fracturaron al grupo, hasta que Servando Gómez Martínez, la Tuta, se separó del grupo y se llevó consigo a Enrique Plancarte, Kike, con el que fundó la nueva organización de los Caballeros Templarios, que anunció públicamente su aparición en marzo de 2011, reproduciendo las mismas tácticas y estrategias de penetración política y social de la Familia Michoacana (Carrasco y Castellanos, 2012).

[5] La aparición pública de los Caballeros Templarios fue igual de espectacular que la de la Familia Michoacana, cuando en junio de 2011, colgaron los cuerpos de dos jóvenes de unos puentes peatonales en tierra caliente. Entre la segunda y tercera semanas de junio, de ese año, la pugna entre ambas agrupaciones se agudizó, el resultado de ésta fue la muerte de alrededor de 40 personas. Asimismo, iniciaron las amenazas contra los funcionarios públicos, provocando la renuncia de distintas autoridades, dejando los poderes públicos acéfalos (Maldonado en Nateras, 2018).

Mapa 4. Municipios del Estado de México con presencia de la Familia Michoacana, 2014



Mapa 5. Municipios del Estado de México con presencia de los Caballeros Templarios, 2014

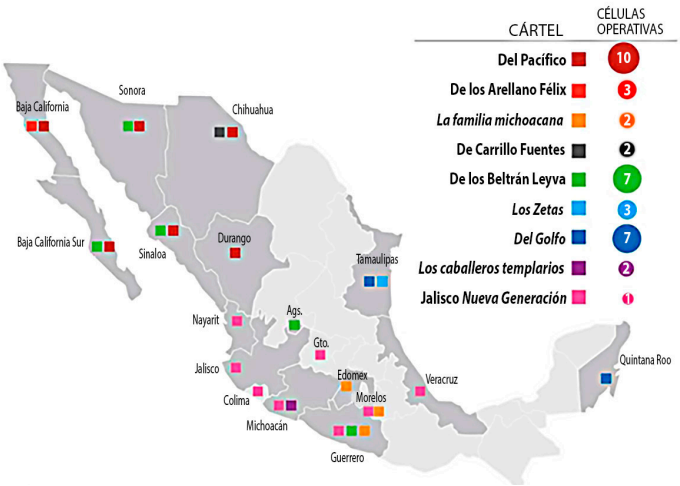


Fuente: Sánchez, 2014.

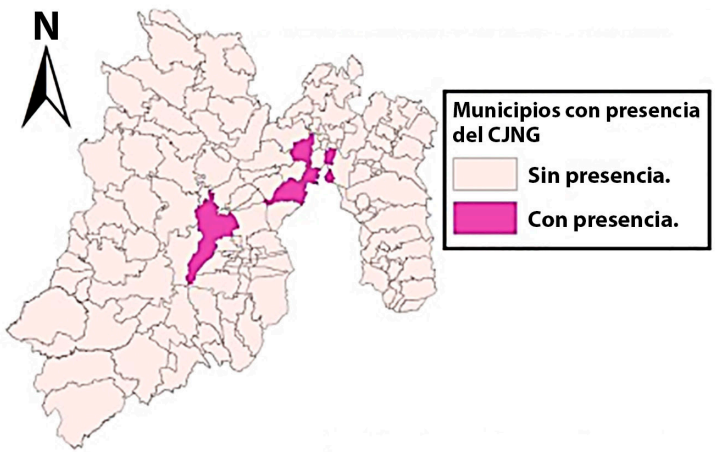
El cártel que más crecimiento registró durante la presidencia de Enrique Peña Nieto, según información de la propia PGR, fue el CJNG, el cual tiene presencia en los estados de Nayarit, Colima y Michoacán, en tanto que también ejerce

influencia en Mexicali y otros estados del centro del país como el Estado de México, Querétaro y una parte de San Luis Potosí, Veracruz, Guerrero y Oaxaca (Nájar, 2017) (mapa 6).

Mapa 6. Mapa del narcotráfico en México, 2017



Mapa 7. Mapa del Estado de México con presencia del CJNG, 2014



Su crecimiento se debe, de acuerdo con información de la PGR, a su capacidad de trasiego de droga tanto en los ámbitos nacional como internacional, en sólo siete años ha expandido su dominio. En 2011, surgió como organización delictiva en los estados de Jalisco, Nayarit y Colima; actualmente, tiene presencia también en Michoacán, Guanajuato, Guerrero, Morelos, Veracruz y Ciudad de México (mapa 6).

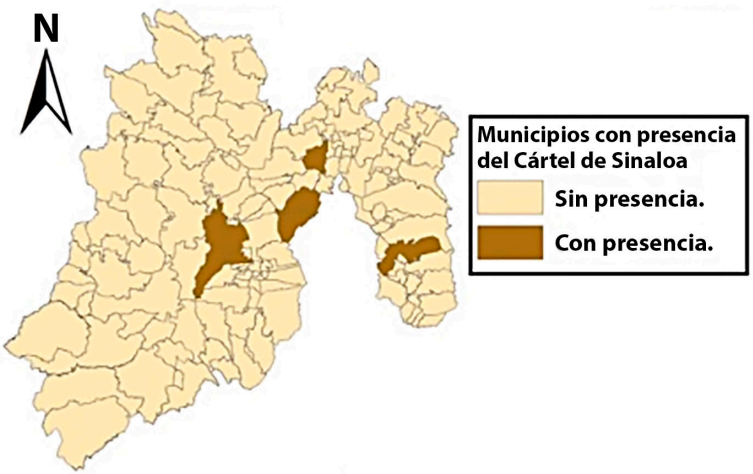
En el caso del Estado de México, a pesar de que la PGR no reconoce su presencia en esta entidad, el CJNG ha registrado un crecimiento exponencial, dinámica de crecimiento acorde con la que tiene en los ámbitos nacional e internacional. En 2014 sólo tenía representación en cinco municipios del Estado de México (mapa 7), tres años después se incrementó a 23[6] (Sánchez, 2017). La DEA y el Departamento del Tesoro de Estados Unidos señalan que es la única organización criminal con presencia en estados tanto del Golfo de México como del Océano Pacífico, de la frontera norte y la frontera sur del país. Coinciden también en que un factor clave de su rápida expansión es que comparten operaciones con el grupo delictivo de los Cuinis,[7] expertos en el tráfico de cocaína y metanfetaminas pero, sobre todo, en el lavado de dinero (Montalvo, 2016).

Los Zetas, que han perdido presencia, no sólo en el país, también en el Estado de México en 2014 tenían representación en 43 municipios y en 2017 sólo en 22, entre los que destacan: Huehuetoca, Tepotzotlán, Tequixquiac y Zumpango. Sus principales actividades son la extorsión a migrantes, el robo de combustible y el narco menudeo. Otra de las organizaciones criminales con representación en el Estado de México es el Cártel de Sinaloa, que opera en nueve municipios (mapa 8); la organización de los Beltrán Leyva, que mediante varias de sus células como el Cártel del Centro trabaja en nueve municipios del Estado de México, así como el Cártel del Golfo, que opera en ocho municipios del Estado de México (mapa 9).

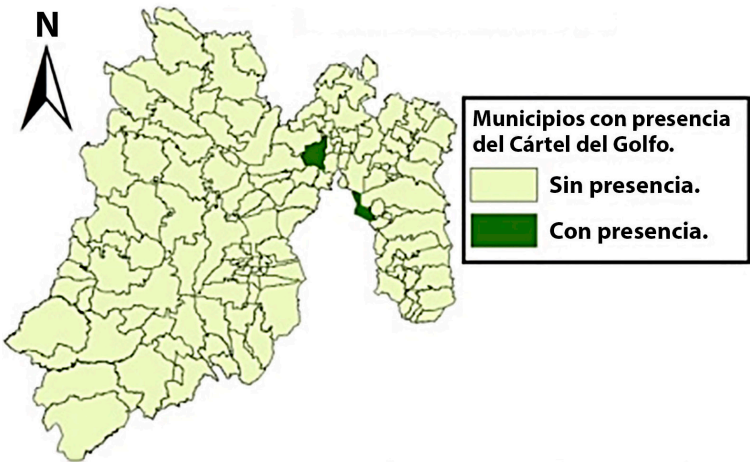
[6] Estos municipios son Atizapán, Atizapán de Zaragoza, Coacalco, Coyotepec, Cuautitlán, Cuautitlán Izcalli, Ecatepec, Huehuetoca, Ixtapaluca, La Paz, Melchor Ocampo, Metepec, Nezahualcóyotl, Nicolás Romero, Tecámac, Temascaltepec, Texcoco, Tlalnepantla, Tultepec, Tultitlán, Valle de Bravo, Zinacantepec y Zumpango (Sánchez, 2017).

[7] El líder de los Cuinis, Abigael González Valencia —antes integrante del desaparecido Cártel del Milenio y detenido en México en febrero de 2015— es cuñado de Nemesio Oseguera Cervantes, el Mencho (Montalvo, 2016).

Mapa 8. Municipios del Estado de México con presencia del Cártel de Sinaloa, 2014



Mapa. 9. Municipios del Estado de México con presencia del Cártel del Golfo, 2014



Fuente: Sánchez, 2014.

También, con una presencia considerable, se encuentra la organización de los Guerreros Unidos, que operan en 15 municipios del sur del Estado de México, entre los cuales se encuentran Tlatlaya, Tejupilco, Luvianos, Sultepec y Amatepec, todos ellos en colindancia con el estado de Guerrero. (Sánchez, 2017). Al respecto, Víctor Manuel Sánchez menciona:

> Hay cuatro organizaciones criminales que sólo tienen presencia en el Estado de México: la primera es el Cártel del Estado, un grupo presente en tres municipios y que se encuentra en vías de desaparición; los Rojos, que operan en dos municipios; la Nueva Empresa, que es una escisión de la Familia Michoacana, la cual opera en dos municipios y los Tequileros, que también se separaron de la Familia y que tienen su base de operación en el norte de Guerrero y cuentan con presencia en Tejupilco y Tlatlaya (2017: s/p).

Conclusión

El marco de protección internacional se centra en los desplazamientos forzados en contextos de violencia criminal, sobre todo entre países; sin embargo, las circunstancias que obligan a una persona o a un grupo de personas a moverse de su lugar de residencia es más compleja que poner atención en sus derechos; por tanto, el primer paso para su atención es el reconocimiento de la existencia del desplazamiento interno forzado provocado por la violencia de los cárteles, ya que la gente se mueve en busca de seguridad y protección o anticipándose a amenazas de los grupos criminales. En palabras de Sebastián Albuja:

> La respuesta al DIF en México por parte del gobierno se ha limitado ante la negación sistemática del problema, restringiendo así la posibilidad de abordarlo. Es por eso que las acciones han sido mínimas, dos excepciones son la Procuraduría Social de Atención a las Víctimas de Delitos (Províctima) que se creó por decreto presidencial en septiembre de 2011 con el objetivo de auxiliar a las personas afectadas por secuestros, desapariciones forzadas, homicidios, extorsión y trata de personas, y la CNDH que desde 2011 ha recogido quejas de personas desplazadas por la violencia y en 2016 presentó un informe especial sobre desplazamiento forzado interno en México (2014: 30).

Este fenómeno ha crecido de manera alarmante debido a que la violencia ejercida por los grupos del crimen organizado provoca miedo y temor entre la población, la cual no encuentra apoyo en las instituciones responsables de la seguridad, sobre todo cuando están coludidas con los grupos delictivos. Aunado con esto, faltan datos, diagnóstico y un análisis integral del fenómeno en cuestión, para poder responder de manera integral a esta problemática tan compleja.

El reconocimiento del problema —como ya se dijo— es el primer paso, lo cual ya se produjo, y el segundo paso es generar confianza entre la población que vive o ha vivido el DIF para hacer el registro respectivo y contar con los datos necesarios para la generación de políticas de atención para las personas que padecen esta problemática; en esta tarea, la protección de su identidad es fundamental, debido a que ésta es una de las razones por la cual prefieren pasar inadvertidas, desdibujando con esto el sentido social de su atención, quedando en un problema de orden individual, por las características del propio desplazamiento.

Referencias

Bibliografía

Lizárraga Hernández, Arturo (2004). *Nos llevó la ventolera: El proceso de la emigración rural al extranjero en Sinaloa. Los casos de Cosalá, San Ignacio y El Verde,* Facultad de Estudios Internacionales y Políticas Públicas-Universidad Autónoma de Sinaloa, México.

Hemerografía

Carrasco, J. y F. Castellanos (2012). "Michoacán bárbaro", *Proceso*, núm. 1837, México.

Mesografía

Albuja, Sebastián (2014). "Violencia criminal y desplazamiento en México", *Migraciones Forzadas*, núm. 45, marzo, pp. 28-3. Refugee Studies Centre Oxford Department of International Development University of Oxford, [en línea]. Disponible en https://rua.ua.es/dspace/bitstream/10045/36480/1/RMF_45.pdf, consultado el 13 de mayo de 2019.

Animal Político (2017). "10 años de guerra: cómo hemos cambiado", [en línea]. Disponible en http://www.animalpolitico.com/diez-de-guerra/desplazados.html, consultado el 13 de mayo de 2019.

cndh, Comisión Nacional de los Derechos Humanos (2016). "Informe especial sobre desplazamiento forzado interno en México". Disponible en http://www.cndh.org.mx/sites/all/doc/Informes/Especiales/2016_IE_Desplazados.pdf, consultado el 23 de mayo de 2016.

Comisión mexicana de defensa y promoción de los derechos humanos, A.C. (2018). "Episodios de desplazamiento interno forzado masivo en México. Informe 2017". Disponible en http://www.cmdpdh.org/publicaciones-pdf/cmdpdh-episodiosde-desplazamiento-interno-forzado-en-mexico-informe-2017.pdf, consultado el 23 de marzo de 2018.

Díaz Pérez, Ma. Cristina y Raúl Romo Viramontes (2019). *La violencia como causa de desplazamiento interno forzado. Aproximaciones a su análisis en México*. Segob, Conapo Unfpa. Disponible en https://www.gob.mx/cms/uploads/attachment/file/456109/Desplaz_2019_web_color-comp.pdf, consultado el 14 de mayo de 2019.

Gámez Gutiérrez, Jorge (2013). *Aproximación al desplazamiento forzado por la violencia*, [en línea]. Disponible en http://www.scielo.org.co/pdf/rlb/v13n2/v13n2a09.pdf, consultado el 14 de mayo de 2019.

Gómez Buendía, Hernando (2003). *El conflicto, callejón sin salida*, [en línea]. Disponible en http://hdr.undp.org/sites/default/files/colombia_2003_sp.pdf, consultado el 15 de febrero de 2019.

Mercado Mondragón, J. (2016). "El desplazamiento interno forzado en México", *El Cotidiano,* [en línea], pp. 181-192. Disponible en http://www.redalyc.org/articulo.oa?id=32548630016, consultado el 13 de febrero de 2016.

Montalvo, Tania L. (2016). "Cómo es que el Cártel Jalisco cobró tanta fuerza en el gobierno de Peña". Disponible en https://www.animalpolitico.com/2016/09/cartel-jalisco-nueva-generacion-mas-grande/, consultado el 23 de junio de 2016.

Mosso, Rubén (2017). "Nueve cárteles operan en México: PGR", *Milenio,* [6 de noviembre de 2017, México, [en línea]. Disponible en http://www.milenio.com/policia/nueve-carteles-operan-en-mexico-pgr, consultado el 13 de mayo de 2017.

Nájar, Alberto (2017). "Los mapas que muestran los radicales cambios de influencia territorial de los carteles del narcotráfico en México", [en línea]. Disponible en https://www.bbc.com/mundo/noticias-america-latina-40576103, consultado el 13 de mayo de 2017.

Nateras González, Martha (2018). "Las autodefensas en Michoacán, México: ¿rescate de la ciudadanía ante la violencia?", *Opinión Jurídica*, vol. 17, núm. 33, [en línea]. Disponible en https://revistas.udem.edu.co/index.php/opinion/article/view/2464, consultado el 13 de mayo de 2018.

Rubio Díaz Leal, Laura (2014). "Desplazamiento interno inducido por la violencia: una experiencia global, una realidad mexicana, ITAM, México", [en línea]. Disponible en http://www.cmdpdh.org/publicacionespdf/libro_desplazamiento_una_realidad_mexicana.pdf, consultado el 14 de mayo de 2014.

Salazar Cruz, Luz y José María Castro Ibarra (2014). "Tres dimensiones del Desplazamiento Interno Forzado en México", *El Cotidiano,* [en línea]. Disponible en http://www.redalyc.org/articulo.oa?id=32529943008, consultado el 2 de mayo de 2018.

Sánchez Valdés, Víctor Manuel (2014). "¿Por qué aumentó la violencia en el Edomex?", [en línea]. Disponible en https://www.animalpolitico.com/blogueros-causa-en comun /2014/05/05/por-que-aumento-la-violencia-en-el-edomex/, consultado el 2 de mayo de 2018.

_____ (2017). "Los cárteles que operan en el centro de México", [en línea]. Disponible en https://www.animalpolitico.com/blogueros-causa-en-comun/2017/07/25/las-organizaciones-criminales-operan-centro-mexico/, consultado el 23 de julio de 2017.

REFLEXIONES FINALES

Vivimos en una época en la que el valor de la información y los datos se han vuelto trascendentales para comprender los medios por los que la sociedad se entrelaza de forma análoga a las relaciones neuronales. Estas conexiones se han convertido en los vínculos más cotidianos entre las personas, algunas veces incluso de mayor manera que los contactos cara a cara. La sistematización de la información se ha simplificado significativamente gracias a los avances tecnológicos de los últimos años, lo cual hace más sencillo recabar, almacenar y transferir información entre diferentes actores económicos y gubernamentales. En esta era informacional, la sociedad fluye por los canales de datos.

En el caso de México, la recopilación de datos personales, se ha justificado en años recientes con el argumento de garantizar la seguridad de la población, como resultado de los intentos infructuosos por combatir al crimen organizado, el cual vale la pena decir se ha convertido en una industria diversificada que en algunas zonas del país le disputa al Estado el monopolio de la violencia. No han valido los distintos cambios de gobierno en el Ejecutivo Federal o las diferentes composiciones en el Legislativo para combatir exitosamente a los cárteles de la droga. Y esto resulta más preocupante cuando se toman en cuenta dos aspectos fundamentales: por un lado, el gran número de delitos que no se reportan y que constituyen una importante cifra negra, y por otro lado los altos niveles de impunidad que representan una tasa de castigo a delincuentes muy baja, lo cual colocaría al país en el cuarto lugar entre los más impunes según el Índice Global de Impunidad que elabora la Universidad de las Américas Puebla en 2018.

El ascenso de la violencia en México se encuentra enmarcado en un proceso de democratización de las instituciones políticas y en la alternancia de los gobiernos en distintos niveles (federal, estatal y municipal). La confrontación entre los grupos criminales por la disputa de territorios y la corrupción en distintas esferas del gobierno han dispuesto de un escenario en donde la transformación política y el ascenso de la violencia no sólo coexisten, sino que de hecho se complementan explicativamente.

Es necesaria la construcción de una agenda de discusión acerca del tema de la privacidad en México por medio de la apertura de las reglas a las que deben atenerse tanto el Estado como las empresas financieras y comerciales en su papel de agentes administradores de datos; como condición necesaria para tales fines, se requiere elaborar una legislación que regule con certeza el uso de datos biométricos y que al mismo tiempo garantice el derecho a la identidad que establece la *Constitución*, en un entorno en el que la migración de grandes números de personas transitan por nuestro país, implica el reto de salvaguardar la soberanía y de preservar los derechos humanos de ciudadanos mexicanos y de personas en tránsito por el país. Hasta este momento, el siglo XXI puede ser definido como la nueva era de las migraciones, con el adicional de que ahora son globales y principalmente se encuentran motivadas por guerras, crimen y pobreza.

Por un lado, lo anterior implica la discusión de la agenda social sobre la privacidad, pero sobre todo se traduce en la necesidad de un pacto social en el que la sociedad en general se inserte en la discusión; así se amplíe el debate para que todos podamos validar este derecho y superar la falsa disyuntiva entre seguridad y privacidad, para el fortalecimiento de los mecanismos administrativos; pero, sobre todo, para trasladar al debate público esta discusión que hasta ahora se observa acotada a círculos muy limitados; ante ello, la sociedad mexicana se mantiene en general al margen y, por lo tanto, no se ha convertido en un plano de debate cotidiano, como sí sucede en otras latitudes.

Por otro lado, vale la pena resaltar la necesidad de manejar eficazmente y con transparencia la información de los beneficiarios de programas sociales y de las transferencias directas en las cuales se sustenta gran parte de la política social en la actualidad. Estos datos tan sensibles requieren fines claros en su uso, ya que un manejo inadecuado de éstos puede traducirse en una estigmatización de los grupos menos favorecidos o en implementar mecanismos de uso electoral de la pobreza.

Sin duda, la agenda sobre el tema se encuentra abierta y esta obra busca contribuir a la discusión por medio de distintos casos en los que se analiza la problemática de la privacidad desde diferentes ópticas y por medio de diferentes actores y casos relevantes. Como habrá notado el lector, la privacidad representa no sólo una polémica en el ámbito académico, ya que también nos orienta a replantear la narrativa en torno a la seguridad nacional, el combate al crimen organizado, la

atención humanitaria de los migrantes, la eficiencia de la política social e incluso la atención en situaciones de emergencia como desastres naturales. De ahí que este libro exponga distintos enfoques del tema, con ángulos contrastantes en algunos casos, complementarios en otros. Sirvan estas investigaciones para establecer parámetros de una agenda social en construcción: la privacidad en México.

Vigilancia e instituciones en México. La agenda pendiente de la privacidad y la protección de datos personales coordinado por Vanessa Lizbeth Lara Carmona se terminó de editar el 13 de noviembre de 2020. Por disposición del Reglamento de Acceso Abierto de la UAEM, se publica la versión PDF de este libro en el Repositorio Institucional de la Máxima Casa de Estudios Estatal.

Este libro reúne discusiones que vinculan los proyectos de seguridad ciudadana con la agenda internacional de protección de datos personales tanto en México como en América Latina. Se enfatizan las características y repercusiones que la debilidad institucional supone para salvaguardar el derecho de los ciudadanos a la privacidad.

Un interés común entre los autores es la contextualización de las principales líneas de debate internacional en torno a la privacidad y a la protección de datos personales. Con base en este contexto general, se realiza un ejercicio que pretende esquematizar los ejes principales de la discusión en México, con la finalidad de ubicar su especificidad en diversos ámbitos y dimensiones.