Democracia, privacidad y protección de datos personales

María Solange Maqueo Ramírez
Alessandra Barzizza Vignau

41

INE
Instituto Nacional Electoral

Democracia, privacidad y protección de datos personales

María Solange Maqueo Ramírez
Alessandra Barzizza Vignau

INE
Instituto Nacional Electoral

CUADERNOS DE DIVULGACIÓN DE LA CULTURA DEMOCRÁTICA

Democracia, privacidad y protección de datos personales

María Solange Maqueo Ramírez
Alessandra Barzizza Vignau

41

INE
Instituto Nacional Electoral

CUADERNOS DE DIVULGACIÓN DE LA CULTURA DEMOCRÁTICA

Democracia, privacidad y protección de datos personales
María Solange Maqueo Ramírez
Alessandra Barzizza Vignau

Primera edición, 2019
Primera edición en este formato, 2020

ISBN obra completa impresa: 978-607-8772-11-7
ISBN volumen impreso: 978-607-8772-52-0
ISBN obra completa electrónica: 978-607-8772-90-2
ISBN volumen electrónico: 978-607-8790-08-1

Contenido

Presentación

En México, desde la última década del siglo pasado y las casi dos que han transcurrido del siglo XXI, se han registrado importantes avances en el ámbito público gracias a la creación de organos autónomos que impactan en diversos aspectos que involucran a la sociedad. En ocasiones, han sido avances que, dados de forma tan vertiginosa, no se han alcanzado a dimensionar en su totalidad y tampoco se han encontrado las convergencias entre unos y otros.

A partir de dichos avances, también han surgido importantes cuestionamientos como los que se formulan a continuación: ¿Cuáles son los límites que signan la pequeña franja de lo público y lo privado? ¿Es o debe ser público todo aquello que concierne a un funcionario público? ¿El estado de salud de un funcionario o legislador debe ser conocido por la ciudadanía o sus electores o, por el contrario, ser motivo de reserva por considerarse un dato sensible y merecedor de una salvaguarda especial? ¿Qué nivel de

protección debe brindarse a la privacidad de los ciudadanos? ¿Los expedientes clínicos o los padrones de los programas sociales deben ser públicos? ¿La revolución de la información y la comunicación conlleva un nuevo estadio de la democracia?

En los últimos años, la mayoría de estas preguntas, con formulaciones semejantes o idénticas, han estado presentes en la discusión nacional. No es un hecho fortuito, ya que la construcción de la democracia, el ejercicio pleno del derecho al sufragio libre y secreto, así como la alternancia en el poder, demandaron información, implicaron participación social y exigieron instituciones autónomas, de Estado, garantes de éstos y otros derechos. Es en un marco de tales características que se crea el Instituto Federal Electoral, actual INE, y el ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

No obstante, para llegar a ello, hubo un arduo camino que transitar: desde que los medios de comunicación tradicionales funcionaban como plataformas de difusión de los partidos políticos, hasta la llegada del internet y las redes sociales que implicaron un cambio significativo en la forma de transmitir información y propaganda electoral, así como el surgimiento de nuevos retos para garantizar la privacidad y la protección de los datos personales.

Mediante este cuaderno de María Solange Maqueo Ramírez y Alessandra Barzizza Vignau, el Instituto Nacional Electoral invita a sus lectores a incursionar en la relación que existe entre la democracia, el acceso a la información, la privacidad y la protección de datos; vinculación ineludible que demanda un esfuerzo constante a las instituciones encargadas de su garantía.

Instituto Nacional Electoral

Introducción

La relación entre democracia y privacidad, en el sentido común de ambos conceptos, no resulta necesariamente evidente. De hecho, las dimensiones en que ambas se proyectan podrían parecer inicialmente contradictorias. Por una parte, la democracia suele definirse como "un conjunto de reglas (primarias o fundamentales) que establecen quién está autorizado para tomar las decisiones colectivas y bajo qué procedimientos".[1] En ese sentido, la democracia comprende la interacción de individuos que conviven en una sociedad organizada a través de instituciones y procedimientos para la toma de decisiones para la vida pública, que reflejen la voluntad popular sea de manera directa o a través de sus representantes. Se trata de una forma de gobierno del pueblo y para el pueblo, "del poder público en público",[2] en la

[1] Norberto Bobbio, *El futuro de la democracia,* México, Fondo de Cultura Económica, 1986, p. 14.

[2] *Ibid.*, p. 65.

que impera la llamada "regla de mayoría" para legitimar la toma de decisiones políticas.

Por otra parte, la privacidad evoca un sentido de solitud, de ausencia de los otros, de lo que pertenece a uno mismo, relativo a los sentimientos, emociones, vida familiar, entre otros.[3] Se trata, pues, de una concepción que supone la generación de espacios vitales que escapan del escrutinio público, misma que se relaciona de manera estrecha con el advenimiento del derecho a la protección de los datos personales, entendido como instrumento de la privacidad y, al menos inicialmente en nuestro país, como un mecanismo para clasificar con el carácter de confidencial la información personal en manos del poder público.

En estos términos, mientras que la democracia se manifiesta en la esfera de lo público, la privacidad se proyecta, valga la redundancia, en la esfera de lo privado o de lo íntimo; donde la *res publica* y la *res privata* se constituyen en conceptos históricamente antagónicos, separados de manera casi natural en la tradición romano-germánica y cuya herencia ha permeado en el desarrollo de los sistemas jurídicos occidentales, incluido el nuestro.

---

[3] Beate Roessler, "New Ways of Thinking about Privacy", en John Dryzek *et al.* (eds.), *Oxford Handbook of Political Theory,* 2009 (versión en línea).

No obstante, esta contradicción entre las distintas dimensiones de la democracia y la privacidad (incluida la vertiente relativa a la protección de datos personales) es tan sólo una mera apariencia que parte de una concepción reduccionista o convencional de ambos términos. Tanto el sentido de democracia como el propio sentido de la privacidad y la protección de datos personales, en términos actuales, han extendido sus alcances de tal manera que es factible afirmar la existencia de una estrecha relación entre ambas, donde la democracia importa para garantizar la privacidad y la protección de datos personales y, a su vez, la privacidad y la protección de datos personales se constituyen en una condición *sine qua non* de la democracia moderna.

El objetivo de esta obra consiste precisamente en explorar las distintas dimensiones en las que se proyectan cada una de estas categorías, a fin de destacar la relación de condicionamiento recíproco entre ellas que hace que sin una no puedan existir las otras, y a la inversa. Además, por supuesto, de advertir aquellos espacios de posible tensión que requieren de la adopción de mecanismos y criterios generales que permitan generar condiciones adecuadas para su propia coexistencia.

Ciertamente no se trata de abordar exhaustivamente cada una de las dimensiones de la democracia, la privacidad

y la protección de datos personales, sino sólo de aquellas en las que se hace evidente su interrelación. Tampoco se pretende establecer el sentido histórico y cronológico del proceso evolutivo de cada uno de estos conceptos, aunque incidentalmente hagamos alusión a ello. Nuestra intención es mucho más modesta. Consiste en advertir aquellos aspectos que, sea por oposición o por su imbricación, permiten demostrar la necesidad de generar equilibrios que armonicen su existencia mutua o convivencia natural.

Marco conceptual: democracia, libertad y privacidad

La democracia entendida en los términos establecidos por Abraham Lincoln en su discurso de la batalla de Gettysburg como "el gobierno del pueblo, por el pueblo y para el pueblo", ha admitido diversas interpretaciones según el lugar y el momento histórico e ideológico en el que nos encontremos. No obstante, dada su propia generalidad, esta frase resulta compatible con el sentido moderno de democracia, que la opone a los gobiernos autoritarios[4] y le otorga un lugar privilegiado a los regímenes constitucionales.

Este sentido moderno de democracia se proyecta en dos dimensiones. La primera reconoce que la ciudadanía determina, por sí misma o a partir de sus representantes, las normas bajo las cuales deben regirse los poderes

[4] Luis Salazar y José Woldenberg, *Principios y valores de la democracia,* México, Instituto Nacional Electoral (Cuadernos de Divulgación de la Cultura Democrática, núm. 1), 2016, p. 48.

e instituciones que configuran el aparato gubernamental, como la propia sociedad civil. Esto es precisamente lo que constituye el gobierno del pueblo y por el pueblo, a partir de la previa definición jurídica de los mecanismos para la adopción de las "decisiones colectivas con el máximo consenso y el mínimo de imposición".[5]

En otras palabras, esta primera dimensión de la democracia implica el aspecto formal o procedimental a través de la determinación del quién –el pueblo y sus representantes– y el cómo de las decisiones –mediante el sufragio universal y la regla de mayoría–.[6] Se trata, pues, del establecimiento de "los procedimientos para formar gobiernos y para autorizar determinadas políticas",[7] a partir de la configuración normativa de los órganos de gobierno, las reglas con base en las cuales se adoptan las decisiones colectivas y el establecimiento de medidas que permitan la efectiva participación ciudadana.

La segunda dimensión del sentido moderno de democracia se refiere a que el régimen constitucional y, en general, el ordenamiento jurídico que emana del mismo deben

---

[5] Pedro Salazar, *La democracia constitucional*, México, Fondo de Cultura Económica, 2006, p. 48.

[6] Luigi Ferrajoli, *Poderes salvajes. La crisis de la democracia constitucional,* Madrid, Trotta, 2011, p. 27.

[7] Luis Salazar y José Woldenberg, *op. cit.*, p. 48.

reconocer y garantizar las más altas aspiraciones de una sociedad, a fin de que el gobierno sea efectivamente para el pueblo. Su objetivo consiste en incrementar en la mayor medida posible el bienestar de la ciudadanía. Así, no sólo importa el "quién" y el "cómo" de las decisiones, sino también el "qué" se puede o no decidir colectivamente, esto es, el contenido o sustancia de las decisiones públicas.[8] Detrás de esta dimensión de la democracia se encuentra el reconocimiento de los derechos humanos y la implementación de garantías que permitan su efectiva realización a través del régimen constitucional. Sólo así podría considerarse que el gobierno está verdaderamente al servicio de la sociedad.

La definición de qué puede o no decidirse está, entonces, necesariamente sujeta a límites, identificados precisamente por el respeto a los derechos humanos. Si bien suelen enfatizarse estos límites hacia el poder público, lo cierto es que también delimitan el contenido de las decisiones que cuentan con el respaldo ciudadano. En estos términos, la regla de mayoría e incluso la participación ciudadana en la toma de decisiones, no son condición suficiente para alterar o infringir los derechos humanos reconocidos a través del pacto social.

[8] Luigi Ferrajoli, *op. cit.,* p. 33.

En virtud de lo anterior, este modelo de democracia parte y depende de una noción de "gobierno del poder público en lo público",[9] el cual presupone la existencia de mecanismos que permiten que la ciudadanía conozca el contenido de las decisiones políticas y, en general, el rumbo y razonamiento que prevalece detrás de cada una de las actuaciones del aparato gubernamental. Así, la participación ciudadana, sea para la elección de sus representantes o, incluso, para la toma de decisiones colectivas sujeta a los límites autoimpuestos a partir del pacto social, está sujeta a que haya personas debidamente informadas y capaces de discernir o disentir respecto de las alternativas que se les presentan. De esta forma, a partir de la obtención y aprovechamiento de esta información, la sociedad está realmente posibilitada para controlar los actos del Estado y juzgarlos con la finalidad de determinar su nivel de satisfacción o insatisfacción con el mismo.

Lo anterior permite explicar por qué la "libertad" se constituye en uno de los valores básicos de la democracia constitucional. El adecuado funcionamiento de este régimen requiere tanto del respeto y protección de los derechos humanos en general, como de aquellos que permiten la construcción de una ciudadanía capaz de opinar o manifestarse de manera libre y sin temor a represalias sobre los asuntos públicos, y de participar de manera activa en la

[9] Norberto Bobbio, *op. cit.,* p. 65.

elección de sus representantes y en la toma de las decisiones colectivas; todo lo cual precisa de la conformación de un sentido propio de la personalidad que permita desplegar todas sus potencialidades como individuo.

Así, la libertad como valor intrínseco de las democracias modernas adquiere, por lo menos, un doble sentido: por una parte, supone la posibilidad de que los individuos se desenvuelvan sin interferencias indebidas o arbitrarias (sea por parte de las autoridades o de cualquier otra persona física o jurídica) y, por la otra, significa que éstos sean capaces de autodeterminarse o autogobernarse.[10]

En ese sentido, la libertad se proyecta a partir del reconocimiento de los derechos inherentes a la persona que permitan su desenvolvimiento tanto en el ámbito de lo público como en el ámbito de lo privado. En el primer caso, la libertad de expresión, de asociación, de pensamiento o los derechos políticos, por citar sólo algunos, son indispensables para que las personas puedan participar de manera activa en la vida política de un país.[11] Su

[10] Luis Salazar y José Woldenberg, *op. cit.,* pp. 30-33.

[11] La Carta Democrática Interamericana, aprobada en el 28º Periodo Extraordinario de Sesiones, el 11 de septiembre de 2001, en Lima, Perú, establece en su artículo 4 que "[s]on componentes fundamentales del ejercicio de la democracia la transparencia de las actividades gubernamentales, la probidad, la responsabilidad de los gobiernos en la gestión pública, el respeto por los derechos sociales y la libertad de expresión y de prensa".

efectiva realización no sólo se constituye en la razón de ser de un régimen democrático, sino que, además, es fundamental para el propio sostenimiento del régimen. Pero para que la realización de esos derechos sea posible es necesario garantizar la existencia de ciertas esferas íntimas o privadas, diferenciadas de la vida pública, que posibiliten el libre desenvolvimiento de la persona, que la doten de espacios vitales que le permitan desarrollar su autonomía e identidad y, con ello, desplegar su potencial como individuos capaces de relacionarse con otros y adoptar juicios, criterios y decisiones propias.[12]

Es precisamente a partir de este sentido de libertad que el derecho a la vida privada y, con ello, el derecho a la protección de datos personales como instrumento de la privacidad se relacionan intrínsecamente con la democracia. De hecho, la propia conceptualización del derecho a la vida privada presupone la libertad en sus dos acepciones.

Desde sus orígenes, a partir de su construcción en el modelo anglosajón, el derecho a la privacidad evoca, al menos inicialmente, la idea de solitud, el derecho a ser dejado solo, de acuerdo con la frase acuñada por el juez Thomas Cooley en 1888.[13] Se trata, pues, de crear espacios ajenos a cualquier

[12] Alan Westin, *Privacy and freedom,* Nueva York, Ig Publishing, 1967, p. 26.

[13] Samuel Warren y Louis Brandeis, "The Right to Privacy", en *Harvard Law Review,* vol. IV, núm. 5, Cambridge, diciembre de 1890, p. 389.

intrusión o injerencia indebida por parte de la autoridad pública o de terceros y limitar la divulgación o publicidad de hechos o situaciones que coloquen a las personas bajo la mirada pública en sus asuntos privados o de reclusión.[14]

Este concepto inicial irá expandiéndose a partir del propio proceso evolutivo de la tecnología de la información y comunicación. La aparición de los sistemas de cómputo y, posteriormente, el desarrollo e incorporación del internet a la vida cotidiana dan lugar a incluir en este concepto de vida privada el derecho de las personas "para determinar por sí mismas cuándo, cómo y en qué medida se comunica a otros la información sobre ellas".[15] Ello introduce una nueva dimensión del derecho a la vida privada, como parte de las libertades de los individuos conformada por el derecho a la autodeterminación informativa.

Ambas dimensiones de la privacidad permiten, entonces, establecer con mayor precisión los bienes jurídicos que, en términos de la Comisión Interamericana de Derechos Humanos, tutela:

> En primer lugar, el derecho a contar con una esfera de cada individuo resistente a las injerencias arbitrarias del Estado o de terceras personas. En segundo lugar, el derecho

[14] William Prosser, "Privacy", en *California Law Review,* vol. 48, núm. 3, California, 1960.

[15] Alan Westin, *op. cit.,* p. 7. Traducción de las autoras.

> a gobernarse, en ese espacio de soledad, por reglas propias definidas de manera autónoma según el proyecto individual de vida de cada uno. En tercer lugar, el derecho a la vida privada protege el secreto de todos los datos que se produzcan en ese espacio reservado, es decir, prohíbe la divulgación o circulación de la información capturada, sin consentimiento del titular, en ese espacio de protección reservado a la persona. Y, finalmente, la protección de la vida privada protege el derecho a la propia imagen, es decir, el derecho a que la imagen no sea utilizada sin el consentimiento del titular.[16]

Con ello, las dimensiones en las que se proyecta el derecho a la privacidad o, en términos más amplios, la vida privada,[17] irradian en el sentido de libertad como valor democrático. No basta garantizar ciertos espacios de solitud de las

---

[16] Catalina Botero, *Libertad de expresión e internet. Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA, s.l.*, OEA/CIDH, 2013, pp. 62 y 63.

[17] La Corte Interamericana de Derechos Humanos (Corte IDH) ha señalado que el derecho a la vida privada y el derecho a la privacidad no son sinónimos. El primero tiene un alcance mucho mayor, por lo que, en consecuencia, comprende al segundo. Asimismo, dado el desarrollo jurisprudencial que ha tenido el derecho a la vida privada en los distintos sistemas regionales de derechos humanos y la inclusión del derecho a la protección de datos personales en distintas normas constitucionales, puede entenderse que, a pesar de su carácter autónomo, este último guarda un vínculo estrecho con el derecho a la vida privada. Sobre el particular véase a María Maqueo *et al.*, "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", en *Revista de Derecho (Valdivia),* vol. XXX, núm. 1, Chile, junio 2017, p. 79.

personas, a partir del cumplimiento de obligaciones negativas que implican la no injerencia abusiva o arbitraria por parte de la autoridad o de terceros; es necesario, además, generar obligaciones positivas del Estado que permitan dotar a las personas de cierto poder de control y disposición de la información que les concierne. Ésta es la idea central sobre la que pone énfasis Westin,[18] donde el control sobre qué información se proporciona, a quién, cuándo y cómo, se erige en el eje rector de la privacidad como libertad de las personas. Así, la autodeterminación se constituye en un elemento definitorio de la privacidad, mediante la cual se concede un poder de control fundamentalmente a través, pero no exclusivamente, del consentimiento.[19]

De esta forma, el derecho a la vida privada y, con ello, la privacidad cobran un sentido expansivo cuyos alcances se relacionan de manera directa con "la dignidad del individuo, incluyendo, por ejemplo, la capacidad para desarrollar la propia personalidad y aspiraciones, determinar su propia identidad y definir sus relaciones personales. El concepto de vida privada engloba aspectos de la identidad física y social, incluyendo el derecho a la autonomía personal, desarrollo personal y el derecho a establecer y desarrollar relaciones con

[18] Alan Westin, *op. cit.*

[19] José Luis Piñar Mañas, *¿Existe la privacidad?*, Madrid, CEU Ediciones, 2008, p. 8.

otros seres humanos y con el mundo exterior".[20] Así, tal concepto presenta tanto una dimensión personal, como una dimensión colectiva.

Este sentido amplio de la privacidad permite, entonces, comprender por qué resulta de vital importancia para promover la libertad de acción de los individuos y su propia autonomía. "La privacidad es una condición de independencia respecto de la influencia y el poder de otros".[21] A partir de este derecho las personas gozan de ciertas esferas que permiten su desenvolvimiento, libre de interferencias, presiones y represalias, y con ello se promueve su autonomía para valorar de manera reflexiva y crítica las diversas situaciones que se les presentan, así como para elaborar juicios propios, ejecutarlos o, incluso, reaccionar ante circunstancias que no se ajustan a sus propias valoraciones, aun cuando éstas gocen de cierta popularidad.[22] Todos estos argumentos que destacan el valor de la privacidad como motor de la libertad presentan un aspecto en común: "la privacidad permite a los individuos hacer aquello que de otra forma

---

[20] Corte Interamericana de Derechos Humanos, *Caso Artavia Murillo y otros ("Fecundación in vitro") vs. Costa Rica,* Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 28 de noviembre de 2012, párr. 143.

[21] José Luis Piñar Mañas, *op. cit.,* p. 11.

[22] Ruth Gavison, "Privacy and the Limits of Law", en *The Yale Law Journal*, vol. 89, núm. 3, Massachusetts, enero de 1980, pp. 448 y 449.

no harían por el temor a la desagradable reacción hostil [o desaprobatoria] por parte de otros".[23]

A partir de estas ideas en diversos sistemas jurídicos, incluido el nuestro, se configura el derecho a la protección de datos personales como un derecho humano autónomo pero interrelacionado con el derecho a la vida privada, cuya característica distintiva consiste en el énfasis puesto en el debido tratamiento de los datos personales. Surge en el contexto de un desarrollo económico y tecnológico galopante, en el que se acentúan las preocupaciones por proteger los derechos y libertades fundamentales de las personas físicas, especialmente el derecho a la vida privada, frente a los riesgos que supone la creciente capacidad del Estado y de las empresas para recolectar, almacenar, usar, procesar, transferir y difundir información. Se trata, así, de un medio para garantizar que el ámbito privado de las personas esté exento o inmune de injerencias abusivas o arbitrarias por parte de terceros (sean del sector público o del sector privado), a partir de su información personal. A todo lo cual se añade, en congruencia con el sentido progresivo del derecho a la vida privada, la capacidad de autodeterminación informativa, es decir, el reconocimiento de un cierto poder de control y disposición sobre los propios datos personales. Para esos efectos, el derecho

[23] *Ibid.*, p. 451.

a la protección de datos personales incorpora como parte de su contenido esencial los derechos de acceso, rectificación, cancelación y oposición (llamados genéricamente derechos ARCO), así como el derecho a la portabilidad de los datos personales.

Si bien tanto el derecho a la vida privada como el derecho a la protección de datos personales presentan un contenido común relacionado con la salvaguarda de la información personal, es este último derecho el que se circunscribe a este ámbito. Cualquier intromisión ilegítima u obstáculo al libre desarrollo de la personalidad que vaya más allá del tratamiento de la información, sería materia exclusiva del derecho a la vida privada y no del derecho a la protección de datos personales.

Así, este último se configura en un derecho cuyo origen está directamente relacionado con el concepto de "información personal" y con el reconocimiento de los riesgos que implica su tratamiento dado su carácter de "bien susceptible de comercio y de tráfico jurídico".[24]

[24] Manuel Heredero Higueras, "La sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983", en *Documentación administrativa DA,* núm. 198, España, Instituto Nacional de Administración Pública, 1983, p. 143.

No obstante, el derecho a la protección de datos personales no es una mera proyección del derecho a la privacidad, toda vez que a través de un vasto desarrollo normativo y el establecimiento de autoridades de control independientes establece las condiciones bajo las cuales el tratamiento de la información personal puede considerarse legítimo.[25] Este derecho pone especial énfasis en ciertos elementos que no se encuentran en el centro del derecho a la privacidad,[26] tales como el principio de responsabilidad demostrable, el principio de información o la transparencia en las políticas internas de gestión documental. Ello explica su reconocimiento diferenciado del derecho a la vida privada en algunos sistemas jurídicos y la especificidad de su contenido relativo al procesamiento de la información personal.

De esta forma, la protección de datos personales se constituye tanto en un derecho humano que fortalece el resguardo del ámbito de privacidad de las personas a partir de la información que les concierne (y por lo cual comparte con este algo de su contenido esencial), como en un derecho con contenido propio, directamente relacionado con el tratamiento de los datos personales durante todo su ciclo de vida (esto es, desde su recolección hasta la supresión

[25] Paul De Hert y Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", en Serge Gutwirth *et al.* (eds.), *Reinventing Data Protection?,* Utrecht, Springer, 2009, cap. 1, secc. 1.1.1.

[26] *Ibid.*, secc. 1.1.3.

o borrado del dato). Ciertamente, no se trata de impedir u obstaculizar el tratamiento de datos personales, sino de evitar que el mismo sea injustificado o desproporcionado.[27]

El desarrollo del derecho a la protección de datos personales presenta, además, un componente de adaptación al cambio tecnológico, a fin de establecer mecanismos de protección y seguridad acordes con el avance de las tecnologías de la información y comunicación. Si bien es cierto que surge en la década de los setenta de la mano con la popularización del uso de los sistemas computacionales en la era preinternet, su mayor impulso deviene del advenimiento del internet. Parte de sus objetivos se centra, al igual que el derecho a la vida privada, en contener los efectos negativos del uso de la tecnología, entre los cuales, sin duda alguna, se encuentra el peligro de la vigilancia masiva y, con ello, el llamado Estado vigilante.

Así, a partir de la asunción de la libertad como valor democrático se pone de manifiesto la estrecha relación entre democracia, privacidad y protección de datos personales, de tal forma que existe entre ellas una relación recíproca en la que sin privacidad no puede existir libertad, sin libertad no puede existir democracia y sin democracia no pueden existir ni libertad ni privacidad.

---

[27] *Ibid.,* secc. 1.1.1.

Democracia y privacidad: una relación dialéctica

De acuerdo con lo anterior, la democracia constitucional constituye "el marco institucional, político y cultural por antonomasia para lograr la vigencia de los derechos humanos",[28] pues la realización efectiva de estos últimos conforma la esencia de lo que persiguen los regímenes democráticos. Ello explica la relación de interdependencia de la democracia frente a la privacidad y la protección de datos personales, en cada uno de los sentidos antes indicados.

Por lo que hace al sentido más tradicional de la democracia, el principio de soberanía popular y, con ello, la consagración del poder decisional ascendente que parte de la voluntad ciudadana hacia los órganos gubernamentales de decisión política,[29] crea serios obstáculos para el ejercicio arbitrario

[28] Rodolfo Cerdas, "Democracia y Derechos Humanos", en *Estudios de Derechos Humanos,* tomo I, San José, Instituto Interamericano de Derechos Humanos, 1994, p. 301.

[29] Pedro Salazar, *op. cit.,* p. 46.

o abusivo del poder. Ello supone no sólo la incorporación de los valores éticos y políticos socialmente compartidos, entre los que la libertad ocupa un lugar destacado, sino también el establecimiento de claros límites al poder público, que comprenden, sin duda alguna, el reconocimiento de ciertas esferas que protegen al individuo de injerencias injustificadas en su ámbito íntimo o privado, lo cual es precisamente parte del contenido esencial del derecho a la privacidad. Además, el poder de autodeterminación comprendido en el mismo supone necesariamente la exclusión del control por parte de terceros, implica el reconocimiento de "una condición de independencia respecto [de] la influencia y el poder de otros".[30]

Lo anterior permite explicar por qué el autoritarismo, como una forma de gobierno incompatible con un sentido moderno de democracia, se caracteriza por la ausencia de privacidad e, incluso, de protección de datos personales. En él, la centralización del poder en una sola o varias personas (pero no en la mayoría) facilita el establecimiento de medidas de control y persecución a través de la disolución del espacio vital para la realización de las personas y el tratamiento indebido de la información personal. No es casual que los Estados totalitarios, e incluso los autoritarios, ocupen gran parte

[30] José Luis Piñar Mañas, *op. cit.,* p. 11.

de sus esfuerzos y recursos en la construcción de registros, bases de datos o censos poblacionales que van más allá de lo razonable y legítimamente justificado, y donde el individuo se encuentra subordinado al poder público y a la toma de decisiones políticas distanciadas del inexistente poder soberano del pueblo. De hecho, los orígenes inmediatos del derecho a la protección de datos personales suelen vincularse a la necesidad de adoptar medidas de protección respecto del tratamiento de la información personal que impidan la repetición de los horrores cometidos durante el nazismo alemán.[31]

Así, en los Estados totalitarios se percibe a los individuos como sujetos que deben vivir por y para el régimen, y sujetarse a los ideales impuestos por éste. Existe una publicidad mínima de los actos del Estado y una alta exigencia de apertura respecto de los individuos que gobierna. Cualquier persona que pretenda aislarse del escrutinio público se arriesga a ser percibida como sospechosa. Ello justifica la implementación de sistemas secretos de vigilancia y espionaje. La finalidad de todas estas medidas no es otra que controlar las acciones de

[31] Una empresa de tecnología de los Estados Unidos de América y su subsidiaria en Alemania diseñaron complejos procedimientos para cruzar datos obtenidos de tarjetas del censo poblacional de este país. Posteriormente, los pusieron a disposición del régimen nazi a fin de identificar y localizar de manera efectiva a los judíos que se encontraban en su territorio. Al respecto, véase Edwin Black, *IBM and the Holocaust,* Estados Unidos de América, Crown Books, 2001.

los individuos, generar miedo a represalias y así mantener el orden y la permanencia del régimen.

En ese sentido, bajo una exigencia de absoluta lealtad al régimen, los Estados totalitarios "niegan la privacidad, destruyen las relaciones confidenciales tradicionales, introducen sistemas extendidos de vigilancia y de informantes, y recopilan expedientes completos de millones de ciudadanos".[32] Además, no permiten la formación de organizaciones autónomas con libertad de pensamiento y de expresión desde las cuales sea posible criticar al régimen. Más bien, el Estado promueve una relación cercana entre los individuos y el propio gobierno con la finalidad de que éstos se desarrollen y relacionen entre sí, de acuerdo con un ideal o deber ser que el mismo Estado impone. De esta manera es posible eliminar, o bien reprimir, cualquier oposición que genere o implique una amenaza para la propia subsistencia del régimen.

Sin embargo, así como los Estados totalitarios hacen prevalecer la vigilancia y la plena apertura del individuo y de sus relaciones sobre la privacidad, los regímenes democráticos se caracterizan por establecer mecanismos que, por una parte, garanticen la privacidad individual y colectiva y, por la otra, limiten tanto la divulgación de la

[32] Alan Westin, *op. cit.,* p. 25.

información personal como los sistemas de vigilancia y monitoreo.[33] De ahí que la propia instauración de los regímenes democráticos mantenga como base de su estructura la salvaguarda de un sentido de privacidad que garantice estos espacios de libertad de la persona para su realización plena y la construcción y manifestación individual o colectiva de su autonomía. Ello permite, por una parte, garantizar la existencia de ciertos ámbitos de exclusión de interferencias ajenas, incluyendo al propio Estado y, por la otra, otorgar a las personas la facultad de controlar la información que les concierne, con la finalidad de autodeterminarse frente al resto de la sociedad.

Esta autonomía se proyecta a partir de la posibilidad de conformar ciudadanos capaces de participar activamente en la vida pública del país. Una sociedad democrática requiere necesariamente de demócratas. En ese sentido, la privacidad permite el desenvolvimiento de la persona como un ser humano con una identidad propia, diferenciada de los demás, lo cual conlleva su capacidad para desarrollar juicios, criterios y decisiones autónomas, y para conformar relaciones y asociaciones con otros individuos.[34] Todo ello redunda, a su vez, en la conformación de una ciudadanía capaz de ejercer de manera efectiva sus derechos civiles y políticos.

[33] *Ibid.*, p. 26.

[34] *Ibid.*, p. 28.

La interdependencia entre el derecho a la libertad de pensamiento y de expresión, por una parte, y la privacidad y la protección de datos personales, por la otra, son un claro ejemplo de lo anterior, donde estas últimas permiten generar "espacios libres de amedrentamientos y de represalias", en los cuales las personas "puedan formarse libremente una opinión y expresar sus ideas, así como buscar y recibir información sin ser forzadas a identificarse o a revelar sus creencias y convicciones o las fuentes que consulta".[35] Ello implica el establecimiento de garantías para la protección del discurso anónimo, a fin de asegurar el ocultamiento de la identidad de quien participa en el debate público, cuestiona a las autoridades, promueve alguna manifestación o movilización social, o bien se organiza políticamente.[36] Además, supone la implementación de medidas que permitan garantizar el debido tratamiento de los datos personales y el ejercicio de los derechos ARCO tanto por parte de los particulares como de la propia autoridad. Por otra parte, no cabe duda de que el Estado democrático supone y privilegia la existencia de electores bien informados, por lo cual existe una tensión constante entre la privacidad de los personajes públicos y el derecho a la información que indudablemente asiste a la ciudadanía. La resolución de este tipo de tensiones es, sin duda alguna, uno de

[35] Catalina Botero, *op. cit.,* p. 63.

[36] *Ibid.,* p. 64.

los mayores desafíos para determinar el alcance de la privacidad, toda vez que la democracia también exige la transparencia y la divulgación de información necesaria para garantizar la conducción racional y responsable de los asuntos públicos.[37]

Otro aspecto en el que se manifiesta claramente la privacidad y la protección de datos personales como condición necesaria para la adopción de prácticas democráticas lo constituye la secrecía del voto. Se trata de un componente indispensable de cualquier sistema electoral en los Estados democráticos a través del cual se garantiza el anonimato de quienes emiten su voto. No se trata de ocultar el sentido del voto, el cual es necesariamente público, sino de disociarlo de manera irreversible de quienes lo emiten. Con ello, se pretende evitar la intimidación y la coacción como medios para influir en la toma de decisiones y, por supuesto, la captura de votantes por parte de ciertos grupos de interés, sindicatos o grupos étnicos.[38] Este espacio de participación política ciudadana es irreductible. Bajo ninguna circunstancia podría justificarse una intromisión o injerencia en el mismo por parte de terceros,

---

[37] Alan Westin, "Social and Political Dimensions of Privacy", en *Journal of Social Issues,* núm. 2, Nueva Jersey, 2003, p. 432.

[38] *Cfr.* ACE Proyecto. Red de Conocimientos Electorales, Voz "Secrecía del Voto", Versión 2.0, disponible en http://aceproject.org/main/espanol/ei/eie12a.htm (fecha de consulta: 27 de octubre de 2018).

ni siquiera por lo que hace a las autoridades electorales o a los partidos políticos.

El alcance del sufragio secreto es amplio, no se reduce a la mera emisión del voto para la elección de los representantes o de un partido político en las democracias representativas, también comprende cualquier acto en el cual se manifieste la voluntad política de una persona como expresión de las democracias participativas. La participación ciudadana que implique la revelación de cualquier preferencia política a través del voto, sea para apoyar una determinada medida o elegir una alternativa propuesta, debe ser libre y, en consecuencia, secreta. Esto no significa, más allá del voto, que se impida la libre manifestación de ideas, preferencias y opiniones políticas de las personas que han optado por expresarlas revelando su propia identidad, pues ello atentaría precisamente contra el propio valor democrático de la libertad en el ámbito de lo público, sino que la ciudadanía cuenta con la posibilidad de elegir entre el anonimato y la identificación personal.

Todas estas ideas permiten explicar por qué nuestro sistema jurídico, a través del derecho a la protección de datos personales, le otorga una protección reforzada al tratamiento de la información que incluye las preferencias y opiniones políticas de las personas físicas, identificadas

o identificables.[39] Se trata de datos personales categorizados como "datos personales sensibles", en atención a su relación con la esfera más íntima de sus titulares y al reconocimiento del grave riesgo que entrañaría para éstos el acceso no autorizado a esta información, su divulgación, pérdida o destrucción y, en general, su tratamiento indebido o injustificado.

La inclusión de las preferencias u opiniones políticas dentro de la categoría de datos personales sensibles implica, por una parte, que su tratamiento está sujeto al consentimiento expreso y por escrito de su titular. Por regla general el consentimiento puede ser expreso o tácito, sin embargo, tratándose de datos sensibles como en el presente caso, es necesario que conste de manera escrita, a menos que se presente alguno de los supuestos específicamente establecidos por la ley en los que no se requiere ningún tipo de consentimiento, a saber:

[39] Véase el artículo 3, fracción X, de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017, que define los datos personales sensibles como: "Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar lugar a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual".

I. Cuando una ley así lo disponga, debiendo dichos supuestos ser acordes con las bases, principios y disposiciones establecidos [por la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados], en ningún caso, podrán contravenirla;

II. Cuando las transferencias que se realicen entre responsables, sean sobre datos personales que se utilicen para el ejercicio de facultades propias, compatibles o análogas con la finalidad que motivó el tratamiento de los datos personales;

III. Cuando exista una orden judicial, resolución o mandato fundado y motivado de autoridad competente;

IV. Para el reconocimiento o defensa de derechos del titular ante autoridad competente;

V. Cuando los datos personales se requieran para ejercer un derecho o cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

VI. Cuando exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

VII. Cuando los datos personales sean necesarios para efectuar un tratamiento para la prevención, diagnóstico, la prestación de asistencia sanitaria;

VIII. Cuando los datos personales figuren en fuentes de acceso público;

IX. Cuando los datos personales se sometan a un procedimiento previo de disociación, o

X. Cuando el titular de los datos personales sea una persona reportada como desaparecida en los términos de la ley en la materia.[40]

Por otra parte, el carácter sensible de las preferencias u opiniones políticas supone que su tratamiento por parte de las autoridades, los partidos políticos o los fideicomisos y fondos públicos, se considera como "intensivo o relevante"; de ahí que todos ellos, como responsables del tratamiento de dichos datos personales, están obligados a adoptar medidas preventivas adicionales o reforzadas, entre las que se encuentran: 1) la realización y presentación ante el órgano garante del derecho a la protección de datos personales competente de una evaluación de

[40] Artículo 22 de la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017.

impacto en la protección de datos personales, cuando pretenda poner en operación o modificar políticas públicas, sistemas o plataformas electrónicas, aplicaciones electrónicas o cualquier otra tecnología, y 2) preferentemente, la designación de un oficial de protección de datos personales especializado en la materia.[41]

Esta cuestión ha resultado particularmente relevante en México con motivo de los requisitos establecidos para acceder a una candidatura independiente, regulados por el Instituto Nacional Electoral a través de una aplicación informática que, por supuesto, implicó la recolección de millones de datos personales vinculados a la preferencia política. Lo mismo ha ocurrido durante los ejercicios, privados u oficiales, de consulta a la ciudadanía. Es claro que las políticas de robustecimiento de la protección de datos personales habrán de ser bienvenidas en el futuro inmediato de nuestra democracia.

Finalmente, cabe destacar que el ámbito de libertad propio de los regímenes democráticos que salvaguardan los derechos a la privacidad y a la protección de datos personales, a partir de la prohibición de injerencias arbitrarias

[41] *Cfr.* Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (SNT), "Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto a la protección de datos personales", publicado en el *Diario Oficial de la Federación* el 23 de enero de 2018.

o abusivas y el desarrollo de la autonomía personal, comprende la libre determinación de las preferencias electorales y de la intención de voto ciudadano en lo particular. Es por esta razón que tales derechos cobran especial relevancia en los procesos electorales, a fin de evitar que el tratamiento de los datos personales sirva para finalidades distintas de aquellas para las cuales fueron recabados. Ello implica un especial esmero por parte de cada uno de los actores en estos procesos para salvaguardar el debido tratamiento de datos personales, a fin de evitar la utilización de la información personal como herramienta para influir en las decisiones políticas de la ciudadanía. Las estrategias de comunicación política personalizadas están sujetas a límites, y esos límites se imponen precisamente a partir de los derechos a la vida privada y a la protección de datos personales.

El padrón electoral, la información de la que disponen los partidos políticos en el cumplimiento de sus objetivos legítimos y, en general, cualquier información personal, incluida aquella que se encuentra disponible en fuentes de acceso público, no pueden ser utilizados para construir perfiles ideológicos que coarten la libertad de las personas, de manera maniquea, para expresar sus opiniones o preferencias políticas en los procesos electorales. El tratamiento de los datos personales está sujeto tanto a los principios que informan el derecho a la protección de

datos personales como a los deberes y obligaciones de los responsables y encargados del tratamiento que emanan del mismo. Es a partir del análisis de estos elementos que logra establecerse la línea divisoria entre el tratamiento de datos personales necesario para garantizar la confianza de los electores, la integridad misma de las elecciones y el cumplimiento de los objetivos legítimos de los actores políticos[42] y el tratamiento abusivo e injustificado de los datos personales en las campañas (o precampañas) electorales.

A ello hay que añadir la indispensable protección de los principios electorales, principalmente del encargado de proteger la equidad en la contienda y de aquellos subordinados a la obtención de una voluntad popular que pueda ser calificada de auténtica (principio de autenticidad). La violación de cualquiera de estos dos principios cardinales a través del mal uso de los datos personales se ha entendido en el derecho comparado como potencial causal de nulidad de elecciones. En México, al haber sido eliminada la causal abstracta de nulidad en una de nuestras innumerables reformas en materia electoral, el punto, infortunadamente, no resulta claro ni pacífico. En otras palabras, habremos de esperar a una violación grave y sistemática de la privacidad de los electores para

[42] *Cfr.* Information Commissioner´s Officer (ICO), *Democracy Disrupted? Personal information and political influence,* Londres, Inglaterra, 11 de julio de 2018, p. 3.

saber si nuestras instancias de calificación electoral se pronunciarán o no por la nulidad de los comicios y por la sanción ejemplar a los responsables del tratamiento de los datos. Pensemos, por ejemplo, en la pérdida de registro de un partido político.

Límites del derecho a la privacidad y de la protección de datos personales

El derecho a la vida privada y, con ello, a la privacidad, está sujeto a ciertos límites. Su reconocimiento como un derecho humano en su sentido tradicional, es decir, como una obligación negativa de la autoridad pública –posteriormente extendida hacia terceros–, no ampara una absoluta imposibilidad de realizar ciertas intromisiones por parte de la autoridad pública o de terceros en el ámbito privado de las personas, sino que estas interferencias sean válidas constitucional o convencionalmente, es decir, que no sean arbitrarias o abusivas y, en ese sentido, que sean compatibles con los valores propios de las sociedades democráticas.

La definición de la licitud de las posibles intromisiones a la vida privada de las personas se establece precisamente a partir de ciertos criterios o parámetros que permiten justificar dichas intrusiones, mismos que han sido desarrollados no sólo a través de los instrumentos

jurídicos de reconocimiento del propio derecho, sino fundamentalmente a partir del desarrollo jurisprudencial tanto en el plano internacional como nacional.

En el plano internacional, el Sistema Universal de Derechos Humanos y los sistemas regionales (europeo, interamericano y, con ciertas particularidades, el africano)[43] reconocen el derecho a la vida privada. Por lo que hace al primero, cabe mencionar a la Declaración Universal de Derechos Humanos (artículo 12), el Pacto Internacional de Derechos Civiles y Políticos (artículo 17), la Convención sobre los Derechos del Niño (artículo 16) y la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y sus Familiares (artículo 14). Todos estos instrumentos internacionales, en términos generales, hacen referencia a que nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o reputación.

[43] La Carta Africana de Derechos Humanos y de los Pueblos de 1986, del Sistema Africano de Derechos Humanos, no contempla ninguna disposición relativa al derecho a la vida privada ni de otros derechos directamente relacionados, como el de la honra y la reputación. No obstante, sí cuenta con instrumentos internacionales que hacen una referencia explícita y ampliamente desarrollada del derecho a la protección de datos personales. Éste es el caso de la Convención de la Unión Africana sobre Ciberseguridad y la Protección de Datos Personales de 2014.

Al respecto, el Comité de Derechos Humanos de la Organización de las Naciones Unidas, en alusión al artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, ha precisado que esta disposición prohíbe las injerencias tanto "ilegales" como "arbitrarias". Ello supone, en términos del propio Comité, que las injerencias no sólo tienen que estar previstas en la ley a fin de no ser ilegales, sino, además, que las mismas no sean arbitrarias aun cuando estén comprendidas en un ordenamiento jurídico. Específicamente el Comité de Derechos Humanos ha señalado que la principal diferencia entre la ilegalidad y la arbitrariedad de una medida restrictiva de un derecho humano reside en que la primera se refiere a aquello que se encuentra expresamente establecido y permitido en la legislación aplicable. En cambio, el concepto de "arbitrariedad" no debe equipararse con el de "contrario a la ley", sino que deberá interpretarse de manera más amplia, de modo que incluya consideraciones relacionadas con la inadecuación, la injusticia, la imprevisibilidad y las debidas garantías procesales, además de consideraciones relacionadas con la razonabilidad, la necesidad y la proporcionalidad.[44]

Por lo tanto, una injerencia en el derecho a la privacidad o la protección de datos personales de una persona puede

[44] Comité de Derechos Humanos de la Organización de las Naciones Unidas, Observación general No. 35, adoptada en el 112º periodo de sesiones, 2014.

ser ilegal y no arbitraria, o bien legal pero arbitraria. En ese sentido, el Comité señala que "con la introducción del concepto de arbitrariedad se pretende garantizar que incluso cualquier injerencia prevista en la ley esté en consonancia con las disposiciones, los propósitos y los objetivos del Pacto y sea, en todo caso, razonable en las circunstancias particulares del caso".[45]

De lo anterior se desprende que no es suficiente establecer a través de la legislación los supuestos y las condiciones bajo los cuales podría llevarse a cabo una injerencia por parte del Estado (o, incluso, de los particulares) en la vida privada de las personas, sino que es necesario que esta previsión sea conforme al sentido y ámbito de protección de los tratados internacionales de derechos humanos. Estas consideraciones pueden hacerse extensibles al derecho a la protección de datos personales, pues la violación del derecho a la privacidad reconocido en el Sistema Universal de Derechos Humanos alcanza tanto a "la vigilancia y la interceptación ilícitas o arbitrarias de las comunicaciones" como a "la recopilación ilícita o arbitraria de los datos personales", como ha puesto de manifiesto

[45] Comité de Derechos Humanos de la Organización de las Naciones Unidas, Observación general No. 16, adoptada en el 32º periodo de sesiones, 1988. Sobre esta interpretación formulada en la Observación general No. 16 y la distinción entre injerencias ilegales y arbitrarias, también véase la Comunicación adoptada por el propio Comité de Derechos Humanos en Communication No. 488/1992. Toonen v. Australia, ONU Doc. CCPR/C/50/D/488/1992, 31 de marzo de 1994.

la Asamblea General de las Naciones Unidas en sus resoluciones 68/167 (2013) y 69/166 (2014).[46]

Ahora bien, en lo que se refiere a los sistemas regionales, en el ámbito tanto del Sistema Europeo como del Sistema Interamericano de Derechos Humanos también se reconoce de manera expresa el derecho a la vida privada; en el primer caso, se encuentra comprendido en el artículo 8 del Convenio Europeo de Derechos Humanos, el cual establece que:

1. Toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia.

2. No podrá haber injerencias de la autoridad pública en el ejercicio de este derecho sino en tanto en cuanto esta injerencia esté prevista por la ley y constituya una medida que, en una sociedad democrática, sea necesaria para la seguridad nacional, la seguridad pública, el bienestar económico del país, la defensa del orden y la prevención de las infracciones penales, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás.[47]

[46] Asamblea General de las Naciones Unidas, Resolución 68/167 "El derecho a la privacidad en la era digital", aprobada en su 68º período de sesiones el 18 de diciembre de 2013; y Resolución 69/166 "El derecho a la privacidad en la era digital", aprobada en su 69º período de sesiones el 18 de diciembre de 2014.

[47] Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, Roma, Italia, 4 de noviembre de 1950.

Así, como puede observarse en el citado texto, el Convenio Europeo de Derechos Humanos (CEDH) no sólo comprende un contenido abierto del derecho a la vida privada, lo que ha permitido expandir sus alcances a través de la jurisprudencia,[48] sino que, además, establece las condiciones a las que se sujeta cualquier injerencia en la vida privada de las personas, a efecto de que ésta sea conforme al propio Convenio.

La primera condición para que una interferencia se considere en apego a los términos establecidos en el citado artículo 8 del CEDH, es que la misma esté prevista en la ley, además de que sea accesible y suficientemente clara respecto de las condiciones en las cuales puede producirse o ejecutarse esta intromisión.[49]

---

[48] *Cfr.* Tribunal Europeo de Derechos Humanos (TEDH), *Niemietz v. Germany,* Sentencia de 16 de diciembre de 1992, párr. 29. En esta resolución el Tribunal Europeo manifiesta que "[…] no considera posible o necesario intentar elaborar una definición exhaustiva de la noción de 'vida privada'. Sin embargo, sería muy restrictivo limitar esta noción al 'círculo íntimo' en el cual la persona vive su vida personal como lo elija y excluir de él completamente al mundo exterior no contemplado en ese círculo".

[49] TEDH, *Roman Zakharov v. Russia,* Sentencia de 4 de diciembre de 2015, párr. 229; TEDH, *Malone v. The United Kingdom,* Sentencia de 2 de agosto de 1984, párr. 63 y ss., TEDH, *Kruslin v. France,* Sentencia de 24 de abril de 1990, párr. 27 y ss.; TEDH, *Valenzuela Contreras v. España,* Sentencia de 30 de julio de 1998; párr. 46; TEDH, *Weber and Saravia v. Germany,* Sentencia de 29 de junio de 2006, párr. 95; TEDH, *Association for European Integration and Human Rights and Ekimdzhiev v. Bulgaria,* Sentencia de 28 de junio de 2007, párr. 76; entre otros.

Una segunda condición hace referencia a que la medida restrictiva del derecho a la privacidad de las personas atienda a fines legítimos, es decir, a fines constitucional y convencionalmente válidos. El propio CEDH establece las pautas sobre qué puede ser considerado como un fin legítimo, esto es, por razones de seguridad nacional, seguridad pública, prevención del delito y la defensa del orden social, la protección de la salud o la moral, la salvaguarda del bienestar económico del país y, de manera genérica, la protección de los derechos y las libertades de los demás. Ciertamente los Estados tienen un amplio margen de discrecionalidad para interpretar el alcance de estas finalidades; ello se hace muy patente en temas de seguridad y en la salvaguarda de otros derechos de terceros. No obstante, su sola mención como justificación para la adopción de este tipo de medidas no es razón suficiente para restringir la privacidad de las personas.

En ese sentido, el fin legítimo perseguido sólo podrá servir como justificación si la medida restrictiva de la privacidad es, en una sociedad democrática, necesaria para su realización. Ello implica la tercera condición a que se refiere el CEDH, la cual supone que existe una necesidad social específica, la proporcionalidad de la medida para alcanzar dichos fines y la existencia de razones

relevantes y suficientes que la justifiquen en razón de otras posibilidades.[50]

Por su parte, en el ámbito del Sistema Interamericano de Derechos Humanos, la Declaración Americana de los Derechos y Deberes del Hombre (1948) y la Convención Americana sobre Derechos Humanos (1969) reconocen el derecho a la vida privada. Esta última prevé en su artículo 11 que:

1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.

2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.

3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques.[51]

Al igual que en el caso del Sistema Europeo de Derechos Humanos, la Convención Americana sobre Derechos

[50] *Cfr.* María Maqueo *et al., op. cit.,* p. 77 y **ss.**

[51] Convención Americana de Derechos Humanos, San José, Costa Rica, 22 de noviembre de 1969, artículo 11.

Humanos (CADH) adopta un sentido amplio de vida privada, situación que ha sido constatada por la jurisprudencia de la Corte Interamericana de Derechos Humanos (Corte IDH).[52] En términos generales, este órgano jurisdiccional no sólo ha extendido los alcances de este derecho, a fin de comprender un ámbito de protección que vaya más allá del ámbito familiar, el domicilio, la correspondencia o las comunicaciones, sino que además presenta un contenido obligacional al que se sujeta tanto a la autoridad pública como a terceros.

Adicionalmente, cabe advertir que en términos del artículo 11 de la CADH y de su interpretación jurisprudencial, no existe una prohibición para que los Estados implementen medidas que pudieran restringir o limitar el derecho a la vida privada; de hecho pueden hacerlo siempre que estas medidas no sean "abusivas o arbitrarias". Ello significa que el derecho a la vida privada no es un derecho humano absoluto, por lo que los Estados pueden restringirlo siempre que se cumpla con las debidas condiciones para hacerlo, es decir, que dichas medidas "[estén] previstas en ley, [persigan] un fin legítimo y [cumplan] con los requisitos

[52] *Cfr.* Corte IDH, *Caso Artavia Murillo y otros (Fecundación "in vitro") vs. Costa Rica, op. cit.,* párr. 143; Corte IDH, *Caso Fontevecchia y D´Amico vs. Argentina,* Sentencia de 29 de noviembre de 2011, párrs. 48 y 49; Corte IDH, *Caso Atala Riffo y niñas vs. Chile,* Sentencia de 24 de febrero de 2012, párrs. 161 y 162.

de idoneidad, necesidad y proporcionalidad, es decir, [que sean] necesarias en una sociedad democrática".[53]

Estas condiciones o parámetros establecidos para valorar las medidas restrictivas a la vida privada toman como base de construcción la teoría de Alexy. Así, la Corte IDH adopta, por una parte, el principio de proporcionalidad en sentido amplio, mismo que incluye los subprincipios de necesidad, idoneidad y proporcionalidad en sentido estricto, y, por la otra, el principio de legalidad conformado por los requisitos de que la medida restrictiva esté prevista en la ley y que, a su vez, persiga un fin legítimo.[54]

Los criterios emitidos por la Corte IDH han sido adoptados también por la Suprema Corte de Justicia de la Nación con respecto a la legitimidad de las intromisiones por parte del Estado en la vida privada de los individuos,[55] al establecer

[53] Corte IDH, *Caso Tristán Donoso vs. Panamá,* Sentencia de 27 de enero de 2009, párr. 56; Corte IDH, *Caso Atala Riffo y niñas vs. Chile, op. cit.,* párr. 164 y Corte IDH, *Caso Escher y otros vs. Brasil,* Sentencia de 6 de julio de 2009, párr. 116.

[54] Robert Alexy, "Constitutional Rights and Proportionality", en *Revus, Journal for constitutional theory and philosophy of law,* núm. 22, Eslovenia, 2014, p. 52.

[55] Suprema Corte de Justicia de la Nación, Amparo en Revisión 237/2014, Primera Sala, ministro Arturo Zaldívar Lelo de Larrea. En el engrose del proyecto de Amparo en Revisión, la Suprema Corte de Justicia de la Nación hace referencia al principio del libre desarrollo de la personalidad, con la finalidad de señalar aquellos ámbitos de la vida del individuo que no deben ser regulados por el Estado. Sin embargo, en aras de ser consistentes con el lenguaje utilizado a lo largo de este escrito, nos referimos al derecho a la vida privada como elemento relacionado directamente con el principio que se menciona en la sentencia.

expresamente las condiciones que deben satisfacerse para que se puedan restringir uno o varios derechos. Para esos efectos, es necesario superar "las cuatro gradas del test de proporcionalidad: (1) constitucionalidad de los fines perseguidos; (2) idoneidad; (3) necesidad; y (4) proporcionalidad en su sentido estricto".[56] Así, podría decirse que el test de proporcionalidad, en sentido amplio y en sentido estricto, constituye un parámetro de análisis jurídico universal para analizar la constitucionalidad o convencionalidad de las medidas adoptadas por los Estados que restringen o limitan el derecho a la vida privada y, en general, los derechos humanos.

Como puede observarse de lo antes expuesto, tanto el Sistema Europeo como el Sistema Interamericano de Derechos Humanos presentan notorias similitudes en el tratamiento que le conceden al derecho a la vida privada y sus límites. Incluso, es frecuente encontrar en los fallos de la Corte IDH referencias explícitas a resoluciones emitidas por el Tribunal Europeo de Derechos Humanos (TEDH). Todo lo cual no obsta para reconocer que existen ciertas diferencias entre ambos sistemas, las cuales se observan tanto en el texto de sus respectivos tratados internacionales de derechos humanos, como en su desarrollo jurisprudencial.

[56] *Idem.*

Por lo que se refiere a las diferencias en el texto de las convenciones de ambos sistemas, cabe observar que el artículo 11 de la CADH, distintamente a lo que ocurre con el artículo 8.2 *in fine* de la CEDH, no establece aquellos supuestos que pudieran llegar a constituir un fin legítimo que justifique la implementación de medidas limitativas o restrictivas de la privacidad. Por ese motivo, serán los órganos jurisdiccionales nacionales y, en última instancia, la Corte IDH, los encargados de realizar un análisis de control de la regularidad convencional, con el objeto de definir los extremos que contengan el fin legítimo que autorice a limitar o restringir el ejercicio absoluto del derecho a la vida privada.

Ahora bien, en cuanto a las diferencias en el desarrollo jurisprudencial del TEDH y de la Corte IDH, cabe advertir la existencia de asimetrías entre ambos órganos jurisdiccionales respecto de la interpretación que han realizado específicamente en materia de protección de datos personales. Mientras que la Corte Interamericana no ha realizado ningún pronunciamiento específico en la materia, el TEDH, o Tribunal de Estrasburgo, aun cuando el CEDH no prevé explícitamente el derecho a la protección de datos personales, ha sido muy prolífico en abordar el vínculo de este derecho con el derecho a la vida privada. Al respecto, el Tribunal Europeo ha manifestado en reiteradas ocasiones que bajo el concepto de vida privada previsto en

el CEDH puede quedar amparada toda información relativa a una persona física identificada o identificable (lo cual constituye precisamente el concepto de dato personal).

Más allá de los argumentos vertidos por las partes en conflicto y el derecho doméstico de los Estados parte, el impulso del derecho a la protección de datos personales en las resoluciones del TEDH se logra explicar tanto por la cercanía entre el Sistema Europeo de Derechos Humanos y la Unión Europea, como por la emisión del Convenio 108 del Consejo de Europa, del 28 de enero de 1981, para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal, concebido como el primer y único instrumento internacional jurídicamente vinculante en la materia.

Por lo que se refiere a la cercanía entre la Unión Europea y el Sistema Europeo de Derechos Humanos cabe advertir que todos los Estados miembros de aquélla son, a su vez, parte de este Sistema. Ello ha propiciado que exista una influencia y una constante referencia recíproca entre el TEDH y el máximo órgano jurisdiccional de la Unión Europea, esto es, el Tribunal de Justicia. Este último tiene como fundamento y base de análisis en materia de derechos humanos la Carta de los Derechos Fundamentales de la Unión Europea, emitida en el año 2000, la cual reconoce el derecho a la protección de datos personales como un

derecho humano autónomo del derecho a la vida privada y familiar, como se observa en el tratamiento diferenciado que les concede en sus artículos 7 y 8.

Respecto al impulso provocado por la adopción del Convenio 108 en el seno del Consejo de Europa, no debemos olvidar que tanto éste como el TEDH son parte del Sistema Europeo de Derechos Humanos, por lo que sus acciones, aun cuando son independientes entre sí en cuanto a sus atribuciones, persiguen un mismo objetivo, consistente en promover y tutelar los derechos humanos, sea a través de la vía convencional o de la jurisdiccional, según corresponda. Además, si bien es cierto que el CEDH es el instrumento más importante de reconocimiento de los derechos humanos dentro de dicho Sistema, en el que esencialmente basa su labor de control e interpretación el TEDH, también lo es que el Convenio 108 del Consejo de Europa ha sido objeto de análisis del propio órgano jurisdiccional como parámetro para valorar las debidas salvaguardas de la proyección informativa del derecho a la vida privada en la legislación doméstica de sus Estados parte.[57]

De hecho, los derechos y obligaciones del Convenio 108 del Consejo de Europa encuentran su fundamento en el derecho a la vida privada reconocido en el CEDH.

[57] *Cfr.* TEDH, *Case of Z v. Finland,* Sentencia de 25 de febrero de 1997, párr. 95.

Como se advierte en su artículo 1, este tratado internacional tiene por objeto "garantizar, en territorio de cada Parte, a cualquier persona física sean cuales fueren su nacionalidad o 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 [...]".[58]

Para dichos efectos, este tratado internacional desarrolla los principios que deben adoptarse en el tratamiento automatizado de datos personales, la obligación de los Estados parte de establecer en su derecho interno garantías apropiadas para categorías particulares de datos (entre las que se incluyen las opiniones políticas y otras convicciones) y la previsión de ciertas garantías para la persona concernida. Adicionalmente, este Convenio introduce las mismas limitaciones previstas por el CEDH respecto del derecho a la vida privada para el cumplimiento de sus disposiciones, de tal forma que sus disposiciones podrán ser exceptuadas sólo a través de medidas que se encuentren "previstas por ley" y que "sean necesarias en una sociedad democrática" cuando: "a) tengan por objeto la protección de la seguridad

[58] Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, Estrasburgo, Francia, 28 de enero de 1981, artículo 1, p. 2.

del Estado, de la seguridad pública, para los intereses monetarios del Estado o para la represión de infracciones penales; b) para la protección de la persona concernida y de los derechos y libertades de otras personas".[59]

Dado todo lo anterior, resulta comprensible por qué el TEDH abre las puertas para armonizar sus decisiones respecto del derecho a la vida privada con las previsiones adoptadas tanto en el ámbito de la Unión Europea en materia de protección de datos personales, como en el Convenio 108 del Consejo de Europa, emitido dentro del propio Sistema Europeo de Derechos Humanos. Sin embargo, es necesario precisar que si bien en la Unión Europea existe abiertamente un tratamiento diferenciado entre derechos,[60] como se advierte en su Carta de los Derechos Fundamentales, en el marco del Sistema Europeo de Derechos Humanos el derecho a la protección de datos personales se construye con base en la dimensión exclusivamente informativa del derecho a la vida privada. Ello es así no sólo porque el CEDH no prevé explícitamente el derecho a la protección de datos personales, sino además porque el Convenio 108 del Consejo de

[59] *Ibid.,* artículo 9. Excepción y restricciones, p. 5.

[60] El sistema jurídico mexicano ha recibido una fuerte influencia del modelo de la Unión Europea en lo que se refiere a la recepción del derecho a la protección de datos personales, como se observa en los artículos 6º y 16 de la Constitución Política de los Estados Unidos Mexicanos y la legislación secundaria en la materia.

Europa manifiestamente introduce en las consideraciones sobre su adopción, el deseo de los Estados miembros por "ampliar la protección de los derechos y de las libertades fundamentales de cada uno, concretamente el derecho a la vida privada [...]".[61] Así, el derecho a la protección de datos personales adquiere dentro del Sistema Europeo de Derechos Humanos un carácter instrumental para dotar de efectividad al derecho a la vida privada.

En ese sentido, la postura del TEDH consiste en reconocer que "la protección de datos personales [...] es de fundamental importancia para que una persona disfrute de su derecho al respeto a la vida privada y familiar, como lo garantiza el artículo 8 del Convenio [Europeo de Derechos Humanos]".[62] De lo anterior se deriva que tanto el contenido como los límites del derecho a la protección de datos personales pueden ser analizados también a la luz del derecho a la vida privada (y la privacidad), al menos, por lo que hace a la autodeterminación informativa a través del ejercicio de los derechos ARCO y al debido tratamiento de datos personales.

Todas estas consideraciones adquieren relevancia para nuestro país. Por una parte, los artículos 6º y 16 de la

[61] Convenio 108 del Consejo de Europa, p. 2.

[62] TEDH, *Case of Z v. Finland,* Sentencia de 25 de febrero de 1997, párr. 95. Traducción de las autoras.

Constitución Política de los Estados Unidos Mexicanos reconocen específicamente el derecho a la protección de datos personales, a semejanza del modelo de la Unión Europea. Por otra parte, México ha ratificado su adherencia al Convenio 108 del Consejo de Europa y su Protocolo Adicional.[63] De tal forma que estos instrumentos internacionales se constituyen en un referente obligatorio para salvaguardar la privacidad y la protección de los datos personales de cualquier persona en nuestro país, por lo que pasan a formar parte del "compendio de Tratados internacionales celebrados por el Estado mexicano en materia de derechos humanos".[64]

Esta situación implica, entre otras cosas, que nuestro país introduce en su sistema jurídico las limitaciones previstas en este tratado internacional, mismas que coinciden con las establecidas en el CEDH. De esta forma, dichas limitaciones o excepciones a los principios y garantías

[63] El 29 de junio de 2018 México depositó el instrumento de adhesión al Convenio 108 del Consejo de Europa y de su Protocolo Adicional ante la Secretaría General del Consejo de Europa.

[64] Senado de la República, "Dictamen de las Comisiones Unidas de Relaciones Exteriores, Europa; de Relaciones Exteriores; y de Anticorrupción y Participación Ciudadana, con proyecto de decreto por el que se aprueba la adhesión de México al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y a su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos Personales, hechos el veintiocho de enero de mil novecientos ochenta y uno y el ocho de noviembre de dos mil uno, respectivamente", México, 18 de abril de 2018.

propias del derecho a la protección de datos personales adquieren el carácter de finalidades legítimas, para efectos del llamado test de proporcionalidad.

Así, las disposiciones del Convenio 108 y, por ende, las propias excepciones que establece para la aplicación del derecho a la protección de datos personales son parte del orden constitucional del sistema jurídico mexicano. Ello se desprende del artículo 1º de la Constitución Política de los Estados Unidos Mexicanos, a través del cual se le otorga esta posición en la jerarquía normativa de nuestro país, ya que dicho tratado contiene obligaciones internacionales vinculantes en materia de derechos humanos, específicamente en materia de protección de datos personales. En consecuencia, el contenido del Convenio 108 resulta directamente vinculante para las autoridades mexicanas por tratarse de normas que gozan de rango constitucional dentro del sistema jurídico mexicano.

Lo anterior tiene implicaciones importantes para determinar los efectos de las resoluciones que en la materia emita tanto el TEDH como el Tribunal de Justicia de la Unión Europea (el cual ha sido el más prolífico en interpretar las disposiciones de este tratado internacional), en el propio sistema jurídico mexicano.

Dado que el Convenio 108 no implica el sometimiento por parte del Estado mexicano al ámbito de aplicación del CEDH o a la jurisdicción del TEDH, cuestión innegable dado su exclusivo carácter regional, no puede considerarse que la jurisprudencia emitida por dicho tribunal sea directamente vinculante para éste. Sin embargo, desde la perspectiva del derecho internacional público, podría implicar que los Estados parte tienen la obligación de atender a la interpretación del Convenio 108 a la luz de la jurisprudencia emitida por el TEDH para efectos de implementar las obligaciones contenidas en el Convenio. Dicha obligación se deriva del artículo 31, numeral 3, inciso b de la Convención de Viena sobre el Derecho de los Tratados, el cual establece, *inter alia*, que "toda práctica ulteriormente seguida en la aplicación del tratado por la cual conste el acuerdo de las partes acerca de la interpretación del tratado"[65] deberá ser tomada en cuenta al momento de interpretar el mismo. Desde esta óptica, podría *prima facie* considerarse que, en caso de que un tribunal mexicano tuviese que llevar a cabo un control de constitucionalidad de fuente convencional en materia de protección de datos personales, la jurisprudencia europea podría constituirse en un importante y necesario referente para México en términos

[65] Convención de Viena sobre el Derecho de los Tratados, Comisión de Derecho Internacional de las Naciones Unidas, Viena, entrada en vigor el 27 de enero de 1980, artículo 31, numeral 3, inciso b.

del derecho internacional público.[66] En otros términos, si bien los criterios emitidos por los tribunales europeos anteriormente mencionados no resultan por sí mismos vinculantes para el Estado mexicano, es factible que los mismos deban ser tomados en consideración para efectos de interpretar e implementar las obligaciones y excepciones establecidas por el Convenio 108.

Lo anterior podría darse aun en el caso de que éstos pudieran presentar una contradicción con los criterios jurisprudenciales emitidos por la Corte IDH, siempre que México no haya sido la parte en el proceso contencioso que dio lugar a la emisión de dichos criterios. En caso contrario, estos últimos serían directamente vinculantes para nuestro país.

---

[66] Lo antes expuesto no deja de ser un punto controvertido en la doctrina del derecho internacional público. De hecho, hay quienes sostienen que los criterios emitidos por un tribunal internacional que interpreta obligaciones establecidas en un tratado regional no necesariamente resultan siquiera indirectamente vinculantes para los Estados parte. Su fuerza vinculante depende de la medida en la que el criterio refleje "un entendimiento común" de los Estados parte sobre determinada interpretación, es decir, del grado de consistencia con el que se haya sostenido, observando, asimilado y respetado [el criterio] por los Estados parte del tratado en cuestión. Sobre este debate véase a André Nollkaemper y Rosanne van Alebeek, "The Legal Status of Decisions by Human Rights Treaty Bodies in National Law", en H. Keller y G. Ulfstein (eds.), *Human Rights Treaty Bodies*, Amsterdam, Cambridge University Press, 2011, p. 410. Asimismo, dado que México no formaba parte del Convenio 108 al momento de la formulación e implementación de los mencionados criterios, su fuerza vinculante para este país es ampliamente debatible. Sin embargo, hasta la fecha la Corte IDH no se ha pronunciado en cuestiones de protección de datos personales, por lo que los únicos criterios jurisprudenciales que podrían servir para orientar la implementación de las obligaciones del Convenio 108 son los emitidos por los tribunales europeos.

Cabe señalar que, de acuerdo con la Suprema Corte de Justicia de la Nación, la obligatoriedad de los criterios emitidos por la Corte IDH en aquellos casos en los que el Estado mexicano no formó parte del proceso contencioso que dio origen a la sentencia, serán considerados con carácter vinculante únicamente cuando sean aplicables al caso concreto y se trate del criterio que brinde a la persona involucrada la protección más amplia.[67] En un sentido opuesto, esta resolución implica que los criterios emitidos por la Corte IDH no son directamente vinculantes cuando no brindan al involucrado la protección más amplia que en derecho corresponda.

De esta forma, es factible suponer que para la interpretación y aplicación del Convenio 108, México puede utilizar como referente los criterios jurisprudenciales emitidos en el marco del derecho internacional europeo cuando éstos resulten aplicables al caso concreto, aun cuando pudieran existir otros criterios emitidos en el marco del Sistema Interamericano de Derechos Humanos. No obstante, para que esta opción sea conforme al principio pro persona establecido en el artículo 1º de la Constitución mexicana y, por ende, válida, es necesario que los referentes europeos impliquen una protección más amplia para las personas que los previstos

[67] Suprema Corte de Justicia de la Nación, Contradicción de tesis 293/2011, Pleno.

por la Corte IDH. En cualquier caso, en virtud de este criterio constitucional, México está obligado a preferir la interpretación más protectora para la persona. Este cimiento de nuestro Estado democrático, combinado con el criterio en contra de la discriminación negativa del quinto párrafo del propio artículo 1º constitucional, viene a corroborar, también en la materia que nos ocupa, el renovado pluralismo horizontal de las fuentes del ordenamiento constitucional mexicano.

Finalmente, cabe decir que si bien hasta el momento la Corte IDH no se ha pronunciado específicamente sobre el derecho a la protección de datos personales, como ya hemos mencionado anteriormente, es factible asumir que tarde o temprano tendrá que hacerlo, ya que en los últimos años este derecho se ha ido incorporando en gran parte de los ordenamientos jurídicos nacionales de los países que forman la región. Dadas las divergencias en el alcance e importancia que se concede al derecho a la protección de datos personales y al derecho a la libertad de expresión e información entre el modelo europeo y el americano, dicho pronunciamiento podría tener implicaciones importantes para lo que hemos asentado líneas arriba, especialmente en situaciones en las que se analice una posible tensión entre estos derechos.

En cualquier caso, la resolución de tensiones entre derechos y el análisis de los límites y restricciones a los que se sujete el derecho a la vida privada, la privacidad y la protección de datos personales, serán acordes con la dimensión sustantiva de la democracia, siempre que se cumplan los principios de legalidad y proporcionalidad que se han ido desarrollando en la doctrina y en la jurisprudencia nacional e internacional. En caso contrario estaríamos ante una vulneración de estos derechos humanos y, por ende, de nuestro sistema democrático constitucional.

Privacidad y protección de datos personales en la era del *big data*

El avance tecnológico y, con ello, el advenimiento de internet, han dado lugar a un crecimiento exponencial del volumen de la información a la que tienen acceso tanto las personas como los gobiernos. De igual forma, la variedad (o complejidad) y la velocidad de su procesamiento se han magnificado. Los beneficios que esto supone para el ejercicio de la democracia en su dimensión procedimental y sustantiva pueden ser infinitos. Por una parte, permiten mejorar los procesos electorales y, con ello, la fiabilidad de las elecciones al reducir la posibilidad de fraude electoral, además, reducen el tiempo para la obtención de resultados más certeros. Como ejemplo, suele citarse el caso de Brasil, donde los procesos electorales se realizan mediante el uso de las denominadas "urnas electrónicas", programas y sistemas de cómputo que no sólo almacenan la selección de los electores

previamente identificados y autorizados, sino que además suman los resultados finales de la votación.[68]

Por otra parte, el uso de las tecnologías de la información y comunicación permite la realización de otros derechos humanos directamente relacionados con los principios democráticos. La estrecha relación entre internet y los derechos a la libertad de expresión e información son buena muestra de ello. Su accesibilidad a una ingente cantidad de información, sin límites de fronteras, así como su capacidad de almacenar y difundir ideas, opiniones y noticias, incluso en tiempo real, hacen de internet una plataforma sin precedentes para ejercer los derechos a la libertad de expresión y de información.[69] Incluso, la relevancia que se le concede ha sido reconocida en los diversos sistemas internacionales de derechos humanos, como queda asentado en la Declaración conjunta sobre Universalidad y el Derecho a la Libertad de Expresión, del relator especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la relatora especial de la OEA para

[68] Fernando Galindo, "Democracia, internet y gobernanza: una concreción", en *Seqüência,* núm. 65, Brasil, 2012, p. 40.

[69] Tribunal Europeo de Derechos Humanos (Sección IV), *Barbulescu v. Rumania,* Sentencia de 12 de enero de 2016 [Voto disidente del Juez Pinto de Albuquerque].

la Libertad de Expresión y la relatora especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), adoptada en París el 6 de mayo de 2014, en la cual se establece que:

> [...] Debido al alcance global y la efectividad de Internet, así como su relativo poder de accesibilidad en comparación con otras plataformas de comunicación, este medio desempeña un rol clave para posibilitar la universalidad de la libertad de expresión. En este contexto, resultan de aplicación los siguientes principios:
>
> I. El derecho a la libertad de expresión, que no reconoce fronteras, protege a Internet al igual que a otras formas de comunicación.
>
> II. Las eventuales restricciones a la libertad de expresión en Internet y otras tecnologías digitales deberán efectuarse con suma cautela, teniendo en cuenta que estas acciones en una jurisdicción podrían tener repercusión en otras jurisdicciones.
>
> III. Los Estados deberían promover activamente el acceso universal a Internet sin distinción política, social, económica o cultural, entre otras, respetando los principios

> de neutralidad de la red y el carácter central de los derechos humanos para el desarrollo de Internet.[70]

Lo anterior permite vislumbrar el potencial de la tecnología como herramienta para fomentar el acceso a información oportuna y veraz que, a su vez, permita el fortalecimiento de ciudadanos más y mejor informados que sean capaces de optar libremente por lo que consideren su mejor opción, aunado, por supuesto, a un régimen de fiscalización de la gestión pública que promueva la participación ciudadana en la toma de decisiones colectivas.

No obstante, a pesar de los innegables beneficios que conlleva el desarrollo tecnológico para la democracia, lo cierto es que también presenta importantes riesgos, muchos de los cuales tienen que ver precisamente con el derecho a la privacidad y la protección de datos personales. Como ha puesto de manifiesto la Asamblea General de las Naciones Unidas a través de sus resoluciones, "el desarrollo tecnológico y la naturaleza global y abierta de internet incrementa las capacidades del gobierno, las empresas y de cualquier persona para la realización de actividades de vigilancia, interceptación y recopilación de datos, lo cual, a su vez, facilita las posibilidades de

[70] Declaración conjunta sobre Universalidad y el Derecho a la Libertad de Expresión, ONU/OSCE/OEA/CADHP, París, mayo de 2014.

incurrir en violaciones a los derechos humanos y concretamente del derecho a la privacidad".[71]

Además, las tecnologías de *big data* (así como la inteligencia artificial y el *machine learning*) suponen un tratamiento masivo de información personal. Sus características, usualmente definidas como la potenciación de las tres "V", esto es, la velocidad, el volumen y la variedad de la información tratada, imponen nuevos retos para garantizar los derechos humanos y, con ello, la democracia. Así, la inclusión de medidas que garanticen el legítimo tratamiento de datos personales y, a su vez, salvaguarden la privacidad de las personas, cobra una relevancia inusitada a fin de permitir que el uso de esta tecnología se destine efectivamente a los objetivos socialmente deseables para los que fue creada.[72]

En los últimos años hemos sido testigos de diversos problemas, con un alcance global, donde la tecnología ha acentuado la posibilidad de un control de los ciudadanos por parte de un Estado cada vez más potente y corrosivo

---

[71] Asamblea General de las Naciones Unidas, Resolución 68/167 "El derecho a la privacidad en la era digital", aprobada el 18 de diciembre de 2013, y Resolución 69/166 "El derecho a la privacidad en la era digital", aprobada el 18 de diciembre de 2014.

[72] ICO, *Big data, artificial intelligence, machine learning and data protection,* Versión 2.2, Londres, Inglaterra, ICO, 4 de septiembre de 2017, p. 6, disponible en https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf (fecha de consulta: 18 de noviembre de 2018).

que pudiera poner en grave situación de peligro al sistema democrático. Sólo a manera de ejemplo cabe mencionar algunos casos paradigmáticos que han puesto de manifiesto la necesidad de garantizar el derecho a la vida privada y la protección de datos personales, a fin de robustecer los regímenes democráticos tanto en su dimensión sustantiva como formal. Para esos efectos nos referiremos en líneas subsecuentes a los programas de vigilancia masiva implementados por los servicios de inteligencia de distintos países y al tratamiento de datos personales durante las campañas políticas que permiten individualizar la propaganda electoral e influir en la intención de voto de la ciudadanía.

Programas de vigilancia masiva

Un caso que sin duda marcó un hito histórico en la forma de comprender el derecho a la vida privada es el que se refiere a las revelaciones del excontratista de la Agencia de Seguridad Nacional de los Estados Unidos de América, Edward Snowden, respecto de los programas secretos de vigilancia de comunicaciones implementados por ésta y algunos países, tras los atentados terroristas de septiembre de 2011 en Nueva York. La divulgación de medidas restrictivas para la libertad de las personas, concretamente en relación con el registro de datos de llamadas telefónicas y el acceso a los servidores de internet más importantes a nivel global, tuvieron un alto impacto a escala internacional, toda vez que evidenciaron la capacidad real de recolección, utilización y procesamiento de la información personal por parte de las autoridades gubernamentales. De hecho, las razones que Snowden tuvo para realizar lo que podría considerarse como una de las más grandes revelaciones de secretos estatales en la historia, según

ha dicho en recientes declaraciones, obedecen a que "Antes el gobierno y el sector privado se alimentaban de nuestra ignorancia [...]. Sin embargo, las personas ahora son conscientes. Las revelaciones hicieron de ésta una pelea más justa".[73]

La filtración de estos documentos en diversos medios de comunicación tuvo varios efectos alrededor del mundo. Por una parte, impulsaron la revisión de acuerdos internacionales que implicaban el reconocimiento de un nivel adecuado de protección de datos personales por parte de la Unión Europea a ciertas empresas estadounidenses conforme a un esquema de autorregulación implementado por la Federal Trade Commission, a través del cual se permitía el libre flujo transfronterizo de información personal.[74] Por la otra, se incentivaron diversos cambios normativos en materia de vigilancia de comunicaciones alrededor del mundo y, en términos generales, se puso especial cuidado en valorar la implementación de este tipo de medidas bajo criterios de seguridad nacional.

[73] Ewen Mac Askill y Alex Hern, "Edward Snowden: 'The people are still powerless, but now they're aware'", en *The Guardian*, 4 de junio de 2018, disponible en https://www.theguardian.com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware (fecha de consulta: 19 de noviembre de 2018). Traducción de las autoras.

[74] Véanse las comunicaciones COM (2013) 846 y COM (2013) 847, del 27 de noviembre de 2013, a través de las cuales la Comisión Europea manifiesta la necesidad de revisar y fortalecer la Decisión de Adecuación 2000/520/CE de la Comisión del 26 de julio del año 2000, conocida como el Acuerdo de Puerto Seguro *(The Safe Harbour Privacy Principles)*.

A raíz de las publicaciones de Snowden sobre los programas de vigilancia masiva por los servicios de inteligencia, durante el periodo comprendido entre 2013 y 2015, también se impulsaron medidas jurisdiccionales por parte de la ciudadanía a fin de combatir estas prácticas que incumplen con los parámetros establecidos para limitar o restringir el derecho a la vida privada. De manera reciente el TEDH, en su fallo del 13 de septiembre de 2018, relativo al caso *Big Brother Watch and Others* contra el Reino Unido, promovido por periodistas y otras organizaciones de la sociedad civil, determinó que si bien la interceptación masiva de comunicaciones no contraviene *per se* el derecho a la vida privada y los gobiernos tienen amplia discrecionalidad para determinar su implementación, los servicios de inteligencia del Reino Unido no adoptaron las medidas necesarias que permitieran garantizar una supervisión independiente del proceso de interceptación y, específicamente, de la selección de la información vigilada. Además, el Tribunal consideró que esta información podía revelar mucho sobre los hábitos y los contactos de las personas.

Así, el fallo del Tribunal de Estrasburgo determinó que en este caso el Reino Unido no había cumplido con el requerimiento que exige que toda injerencia en la vida privada sea necesaria en una sociedad democrática. Consideró que la ausencia de salvaguardias adecuadas

también implicaba una violación al derecho a la libertad de expresión e información, dado que la interferencia en las comunicaciones repercutía en la confidencialidad de las comunicaciones de los periodistas y, con ello, en su material periodístico y sus fuentes. Tras la publicación de este fallo, el director general de una de las organizaciones civiles que promovieron la demanda, Silkie Carlo, declaró que "bajo la excusa de luchar contra el terrorismo, el Reino Unido instauró el programa de vigilancia más autoritario de los países de Occidente, corrompiendo no solamente la democracia en sí misma, sino los derechos del público británico".[75]

Este caso en particular sienta un precedente muy importante sobre el alto impacto de las medidas de vigilancia masiva en el ejercicio de los derechos a la vida privada, la protección de datos personales y la libertad de expresión e información, y debe tenerse en consideración, a manera de referente, para valorar el caso aún pendiente de resolución relativo a la demanda presentada por activistas, periodistas y académicos en nuestro país por espionaje gubernamental a través del uso del *software Pegasus.*

[75] Emma Woollacott, "UK Mass Survaillance Ruled Unlawful", en *Forbes,* 13 de septiembre de 2018, disponible en https://www.forbes.com/sites/emmawoollacott/2018/09/13/uk-mass-surveillance-ruled-illegal/#4b9deb146329 (fecha de consulta: 19 de noviembre de 2018). Traducción de las autoras.

Además, cabe enfatizar que la vigilancia masiva a través de la interceptación de comunicaciones en la era del *big data* tiene un alcance mucho mayor al que siquiera pudo haberse concebido en los propios orígenes del reconocimiento del derecho a la vida privada en los sistemas internacionales de derechos humanos y en nuestra Carta Fundamental. La información de la que disponen los prestadores de servicios de telecomunicaciones, sea de telefonía móvil o de internet, puede contemplar tanto el contenido de las comunicaciones como otros datos que se relacionan con las mismas, esto es, los metadatos, tales como el número telefónico de origen y destino, la hora, fecha y duración de la llamada telefónica, la localización de las antenas desde donde se obtuvo la señal de las comunicaciones, o bien la dirección IP o el encabezado de un correo electrónico, por citar algunos. El análisis y procesamiento de esta información, junto con otros datos que pudieran ser obtenidos de fuentes de acceso público, facilitan la elaboración de perfiles altamente detallados de las personas que permitan revelar sus aspectos más íntimos o privados.[76]

De esta forma, el riesgo de imponer medidas de vigilancia masiva en las que se incluyan obligaciones de recolección

[76] Jonathan Mayer y Patrick Mutchler, "MetaPhone: The Sensitivity of Telephone Metadata", *s.d.*, 12 de marzo de 2014, disponible en http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/ (fecha de consulta: 22 de noviembre de 2018).

y almacenamiento de información de manera generalizada e indiscriminada hacia estos prestadores de servicios es una cuestión sumamente delicada, que debe ser analizada cuidadosamente a la luz de los criterios o parámetros establecidos para valorar la legalidad y proporcionalidad de las medidas restrictivas al derecho a la vida privada. Además, no debe perderse de vista que el solo hecho de saber que los datos de las comunicaciones son recolectados y almacenados, aunque sea por un tiempo específico, puede tener un efecto intimidatorio que mine no solamente la esfera de privacidad sino la libertad con la que los individuos actúan y se expresan, tanto en el mundo material como en el virtual.[77]

Los casos anteriormente citados y el desarrollo tecnológico para el tratamiento de los grandes datos ponen de manifiesto los métodos y alcances que pueden llegar a tener los programas de vigilancia, así como el alto impacto que pudieran presentar tanto en la vida privada de las personas como en el propio funcionamiento de las estructuras democráticas. Si bien es cierto que en ocasiones estas medidas son indispensables para hacer frente a las amenazas y a los actos de carácter criminal, también pueden ser utilizadas de manera arbitraria

[77] Frank La Rue, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/23/40, 17 de abril de 2013, § 24.

o abusiva, o bien para fines que no están relacionados con el cumplimiento de las funciones propias del Estado. Esto no sólo pone en riesgo el ámbito de privacidad de las personas, sino también su libertad y, con ello, al Estado constitucional. Representan un enorme y directo reto a la calidad de la democracia.

Uso de información en campañas políticas e influencia en la intención de voto

Desde los comienzos del sufragio universal, a principios del siglo XX, los partidos políticos se han apoyado en diversos métodos propagandísticos para difundir sus posturas y persuadir a la ciudadanía en la toma de decisiones. En un inicio tendían a transmitir sus mensajes a viva voz, procurando hacerlo en lugares públicos altamente concurridos, a fin de llegar al mayor número posible de votantes. Sin embargo, con la llegada de la radio, el teléfono y la televisión, se hizo viable la posibilidad de hacer llegar los mensajes de manera masiva.

En un principio se pensaba que entre mayor fuera el número de personas a quienes se les pudiese hacer llegar la propaganda, las probabilidades de que el partido político en cuestión obtuviese la victoria eran mayores. Sin embargo, con el paso de los años, las técnicas de difusión y elaboración de propaganda política se han hecho cada vez más sofisticadas. Con el tiempo se han ido elaborando

técnicas de mercadotecnia específicas que consisten, más bien, en intentar modificar las preferencias de los consumidores o receptores de la información.[78] Si bien esta transformación comenzó en la época de la posguerra, ha evolucionado hasta llegar al uso de grandes empresas de mercadotecnia entre los años ochenta y noventa.[79] Así, los métodos y técnicas de propaganda electoral se han ido desarrollando y diversificando a la par del avance de la tecnología y las técnicas de investigación.

Los medios de comunicación tradicionales han desempeñado un papel crucial en el ejercicio del derecho al voto, ya que funcionan como plataforma de difusión de información que proviene de los partidos políticos y va dirigida a los electores. En un escenario ideal, los partidos políticos únicamente difunden información relevante que sirve para dar a conocer sus posturas, planes, políticas y estrategias. Al mismo tiempo, los medios ejercen su labor de manera imparcial y objetiva, con la finalidad de propiciar un ambiente en el que los ciudadanos puedan ejercer su derecho al voto en forma informada y, en consecuencia, libre.

---

[78] Dominic Wring, "Reconciling Marketing with Political Science: Theories of Political Marketing", en *Journal of Marketing Management,* Inglaterra, vol. 13, 1997, pp. 4 y 6.

[79] ICO, *Democracy Disrupted? Personal information and political influence, op. cit.,* pp. 9 y 10.

A lo anterior le debemos la existencia de leyes, reglas y lineamientos dirigidos a los partidos políticos y a los medios tradicionales de comunicación que buscan propiciar un ambiente objetivo e imparcial con la finalidad de garantizar los principios de equidad, neutralidad y objetividad en la contienda electoral. Incluye la normatividad dirigida específicamente a la prensa y a los canales de televisión, así como a los partidos políticos en cuanto al tiempo, modalidad y alcance de sus espacios publicitarios y a la sujeción de topes presupuestarios en gastos de campaña, entre otras medidas.

Sin embargo, el advenimiento de internet, el posterior surgimiento de sus plataformas y la proliferación del *big data* han implicado un cambio significativo en la forma en la que actualmente se recibe y transmite información y propaganda electoral. Además de los medios de comunicación tradicionales, las plataformas de internet se han convertido en un medio adicional para que los partidos políticos difundan información y los usuarios interactúen entre sí y compartan dicha información. Asimismo, han traído el surgimiento de nuevos modelos de negocio a través de los cuales las empresas privadas dedicadas, entre otras cosas, al análisis de grandes segmentos de información, proveen servicios de venta de publicidad a instituciones gubernamentales, partidos políticos y otras empresas o individuos.

El uso de este tipo de servicios ha permitido, a grandes rasgos, que los partidos dirijan su propaganda a los ciudadanos a través de una nueva técnica de mercadotecnia (*microtargeting*) que permite seleccionar a las personas o grupo de personas a quienes se desea dirigir un mensaje o anuncio con base en información sobre su edad, sexo, localización, intereses, comportamientos y preferencias.[80] De esta manera, cada usuario de la plataforma en cuestión puede recibir propaganda electoral personalizada dentro de su perfil, o bien sobre la página *web* que se encuentre utilizando o visitando en ese momento.

Así, en la sociedad moderna las elecciones se enmarcan en un contexto en el que la propaganda electoral es individualizada y se recibe en espacios aislados, con base en un análisis altamente detallado sobre el perfil de las personas que la reciben. En algunas ocasiones, los partidos políticos combinan la información obtenida en el padrón electoral con bases de datos o información pública con la finalidad de obtener rasgos distintivos de las personas que les permita dirigir sus anuncios publicitarios. En otras ocasiones, son las propias empresas las que prestan este servicio a los partidos y hacen un análisis y cruce de información obtenida de varias fuentes y procesada con fines que podrían permitir la obtención

[80] *Ibid.,* p. 34.

de un perfil ideológico, político y socioeconómico de las personas.[81] En este contexto, mientras que los partidos políticos actúan como "responsables del tratamiento de datos personales", toda vez que determinan los medios y las finalidades del tratamiento de los datos, las empresas contratadas por ellos para procesar la información, al menos en principio, adoptan el carácter de "encargados del tratamiento" de dichos datos, por lo que deben sujetarse a las indicaciones y medidas establecidas formalmente por los primeros. No obstante, en ambos casos, están obligados al cumplimiento de los principios y deberes previstos en materia de protección de datos personales, aun en el caso de que la información tratada haya sido obtenida de fuentes de acceso público.

En un escenario en el cual se cumple cabalmente con los principios de licitud, lealtad, consentimiento, información, finalidad, calidad, proporcionalidad y responsabilidad respecto del tratamiento de datos personales de los individuos, el uso de estos servicios y técnicas de *big data* en el procesamiento de información por parte de los partidos políticos puede tener consecuencias positivas para la democracia. En muchas ocasiones los espacios en línea funcionan como fuentes de información que contribuyen al libre intercambio de críticas e ideas

[81] *Ibid.*, pp. 38 y 39.

que sirven para el ejercicio pleno de los derechos políticos del electorado y el entendimiento de las prioridades ciudadanas por parte de los partidos políticos. Asimismo, la información y transparencia en las políticas de privacidad tanto de los partidos políticos, las candidaturas y las empresas relacionadas permiten el ejercicio efectivo del derecho a la autodeterminación informativa con lo cual, incluso, es factible la obtención y facilitación automatizada de opiniones, propaganda e información similares o compatibles con una determinada ideología compartida.

No obstante, el tratamiento indebido de datos personales con finalidades políticas bajo el uso de la tecnología actual puede tener diversas consecuencias negativas para la democracia. Al respecto, algunas autoridades de protección de datos han puesto especial énfasis en el impacto que ello supone para los procesos electorales y las campañas políticas.[82] Específicamente, estas preocupaciones hacen referencia a la posibilidad de identificar votantes considerados (incluso por vía automatizada y sin intervención humana) como fáciles de persuadir o manipular, así como a la factibilidad de la vigilancia

[82] *Ibid.*, p. 10. European Data Protection Supervisor (EDPS), *Opinion on online manipulation and personal data,* Opinión 3/2018, Bruselas, EDPS, 19 de marzo de 2018, p. 3.

electoral, misma que atañe directamente a la confidencialidad de las preferencias políticas de la ciudadanía.[83]

Aunado a lo anterior, se encuentra también el hecho de que estos espacios individualizados y técnicas de personalización de la información y la propaganda electoral puedan ser utilizados para finalidades ilegítimas, tales como la propagación de información falsa o engañosa por parte de los candidatos, representantes de partidos políticos, simpatizantes y medios de información poco serios. Para lograr lo anterior, se utiliza la información obtenida a través de un análisis del perfil de los electores, donde se obtiene información respecto de su posible acercamiento o distanciamiento de un determinado partido político. Posteriormente, se le envía información falsa o adversa respecto del candidato o partido con la finalidad de modificar su intención de voto.

Ciertamente las preocupaciones generadas en torno al tratamiento de datos personales para fines políticos no son nuevas, como lo demuestra la "Resolución sobre el Uso de Datos Personales para la Comunicación Política",

[83] Conviene enfatizar que las preferencias y opiniones políticas se constituyen en un ámbito especialmente protegido, pues no sólo se consideran parte del aspecto más íntimo de las personas, sino además tienen la característica de ser datos personales sensibles. Ello supone que el tratamiento de este tipo de información está sujeto a condiciones reforzadas, entre las que se encuentra la necesidad de obtener consentimiento expreso y por escrito para su tratamiento.

emitida en Montreux, Suiza, en el marco de la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad celebrada del 14 al 16 de septiembre de 2005. Al respecto, señala en sus considerandos que:

> [...] las organizaciones políticas recopilan continuamente una gran cantidad de datos personales y, en ocasiones, se procesan con modalidades agresivas, aplicando varias técnicas, incluyendo sondeos, recopilación de direcciones de correo electrónico a través de software / motores de búsqueda, solicitud de votos en ciudades o formas de tomas de decisiones políticas a través de la televisión interactiva y ficheros de aislamiento de votantes; [...] estos datos en ocasiones incluyen ilegalmente [...] datos sensibles relacionados con convicciones o actividades políticas o morales reales o supuestas, o con actividades de votación.
>
> [Además] existe la relación invasiva de perfiles de varias personas que actualmente están clasificadas (en ocasiones de forma imprecisa o en base a un contacto superficial) como simpatizantes, partidarios, adherentes o miembros de un partido, con vistas a aumentar la comunicación personalizada con grupos de ciudadanos [...].[84]

[84] Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad, "Resolución sobre el Uso de Datos Personales para la Comunicación Política", adoptada en Montreaux, Suiza, del 14 al 16 de septiembre de 2005.

Si bien esta resolución pone de manifiesto la relevancia de proteger la privacidad y garantizar el legítimo tratamiento de datos personales para alcanzar objetivos políticos, a fin de "evitar, con las medidas adecuadas, las intrusiones, daños o costes injustificados" y fomentar "un *marketing* responsable sin limitar por ello la circulación de ideas y propuestas políticas", lo cierto es que en el año de su emisión poco se advertían las capacidades tecnológicas actuales, entre las que se encuentran la inteligencia artificial y el *machine learning*, así como el creciente uso de las plataformas digitales, sea como estructuras de comunicación en tiempo real y de manera ilimitada, o bien como medios idóneos para la recolección de la más variada información personal.

De manera reciente, los riesgos e implicaciones que tiene para la democracia la posibilidad de realizar perfiles cada vez más sofisticados de las personas, el *microtargeting* y una mayor disponibilidad de información obtenida de diversas fuentes, ha cobrado relevancia a nivel global con el caso Cambridge Analytica.

En términos generales, los hechos de este caso se remontan al año 2013, cuando un profesor de la Universidad de Cambridge, Aleksandr Kogan, desarrolló un *software* en forma de aplicación de Facebook, el cual consistía en una prueba de personalidad que debían completar los usuarios

de esta red social. Esta aplicación no sólo recolectaba los datos de quienes participaban en la prueba, sino que además permitía el acceso a los datos personales de los amigos de estos en Facebook. Así, mediante el uso de este *software* Kogan logró recopilar información concerniente a aproximadamente 87 millones de usuarios alrededor del mundo, misma que puso a disposición de Cambridge Analytica. Esta empresa, según diversos medios de comunicación, realizó el cruce de esta información con información adicional obtenida de la propia red social, lo cual, según estos medios, permitió que ciertos actores y partidos políticos de diversos países obtuvieran un perfil altamente detallado de un gran segmento de la población, incluyendo su comportamiento electoral, preferencias y opiniones políticas.[85]

De acuerdo con la evidencia obtenida durante la investigación de este caso, la Information Commissioner´s Office (ICO) del Reino Unido concluyó que Cambridge Analytica incurrió en un indebido tratamiento de información personal, toda vez que utilizó datos personales sensibles de los usuarios de Facebook y de la aplicación desarrollada por Aleksandr Kogan para finalidades

[85] "5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día", en *BBC News,* 21 de marzo de 2018, disponible en https://www.bbc.com/mundo/noticias-43472797 (fecha de consulta: 13 de abril de 2019). Traducción de las autoras.

distintas a las que originaron su recolección. En particular, este organismo enfatizó que "los usuarios de Facebook que accedieron a la aplicación y sus amigos no fueron informados de que sus datos serían transferidos a Cambridge Analytica, que serían utilizados para fines de campañas políticas y que serían procesados con el objetivo de inferir sus opiniones y preferencias políticas, así como analizar su comportamiento electoral". Asimismo, afirmó que las condiciones para un tratamiento legítimo de la información personal no habían sido satisfechas, dado que la obtención de la información por parte de esta empresa, así como su uso para fines de *marketing* político, carecían del consentimiento por parte de los usuarios y sus amigos en la red social.[86]

Este caso pone en tela de juicio la posibilidad de diseñar e implementar medidas de propaganda electoral que permitan influir de manera decisiva en la orientación política y la opinión del electorado, susceptible de ser manipulado dada la información sensible recabada sobre su persona; a todo lo cual se suman las preocupaciones generadas en torno a este caso respecto de la posible utilización de información personal para generar y transmitir noticias

[86] ICO, *Investigation into the use of data analytics in political campaigns. A report to Parliament,* Londres, 6 de noviembre de 2018, pp. 34-36, disponible en https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf (traducción de las autoras).

falsas, con el propósito de modificar las decisiones del electorado, especialmente de aquellos que se perciben como vulnerables o inseguros.[87]

De esta forma, el indebido tratamiento de datos personales, más cuando se trata de datos personales sensibles, podría tener serias implicaciones para la democracia y el ejercicio libre e informado de los derechos políticos. Las prácticas atribuidas a Cambridge Analytica relativas a la publicidad electoral dirigida (y, en particular, aquella que pudiera considerarse falsa, subjetiva, dudosa y diseñada en atención a las debilidades de las personas concernidas) ponen en el centro del debate la importancia de supervisar el tratamiento de esta información a fin de evitar una reducción significativa de la libertad ciudadana. La deformación en la percepción del electorado a través de la recolección y procesamiento de su información personal implica una intrusión en la conformación de su autonomía y, por ende, en su proceso de toma de decisiones. Se trata de una forma velada de manipulación y desinformación a través de la tecnología y el uso de los grandes datos con repercusiones de carácter global.

Otra de las grandes preocupaciones que surgen a partir del tratamiento de datos personales de los electores por parte

[87] "5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día", *op. cit.*

de los partidos políticos para fines propagandísticos se relaciona con el riesgo que ello supone para la garantía de secrecía del voto. Como se ha mencionado anteriormente, la figura del voto secreto brinda la posibilidad de poder ejercer este derecho libre de cualquier coacción, amenaza o posible intento implícito o explícito de manipulación por parte de los partidos políticos. Sin embargo, por medio del tratamiento automatizado de los datos personales sensibles de los electores, los partidos políticos han adquirido también la posibilidad de identificar con un alto grado de asertividad la orientación política y la posible decisión de voto de las personas. De esta manera, "aunque los votantes siguen disfrutando de absoluta privacidad una vez que entran en la cabina de votación, los rasgos que predicen su votación y que son captados tanto de fuentes públicas como privadas lejos de las mesas electorales pueden vulnerar el derecho al voto secreto no sujeto a presiones ni a compras".[88]

Al respecto, se han abierto grandes cuestionamientos relacionados con el tipo de límites y controles que deben existir en cuanto al debido tratamiento de los datos personales para fines de mercadotecnia electoral y la diseminación de información a través de las

[88] Rosario García Mahamut, "Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español", en *Teoría y realidad constitucional,* núm. 35, Madrid, UNED, 2015, p. 335.

plataformas de internet. En este contexto, tanto el derecho a la vida privada como el derecho a la protección de datos personales, por lo que se refiere a la capacidad de autodeterminación informativa de las personas, cobran especial relevancia dado que permiten que sean ellas mismas quienes determinen no sólo qué tipo de información quieren recibir, sino también qué información personal puede ser utilizada para fines de propaganda electoral. Ello, a su vez, les permitiría elegir y modular el uso que los agentes económicos, los analistas de datos y los propios partidos políticos realicen respecto de sus datos personales.

Por supuesto, para que lo anterior sea viable es necesario previamente que los electores estén plenamente conscientes de las condiciones y particularidades del tratamiento que se realice de sus datos, lo cual requiere ciertamente el cumplimiento de los principios y deberes establecidos por la normatividad en la materia.[89] Como se observa en distintas actuaciones de las autoridades de protección de datos personales en el ámbito europeo,[90] la transparencia de quienes tratan datos personales con fines políticos

[89] En el caso particular de México el ordenamiento jurídico aplicable para los partidos políticos en el ámbito federal es la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación* el 26 de enero de 2017. Por lo que hace al ámbito estatal (o municipal) resultarían aplicables las diversas legislaciones especiales en la materia emitidas por cada entidad federativa.

[90] *Cfr.* ICO, *Democracy Disrupted? Personal information and political influence, op. cit.,* y ESDP, *op. cit.*

se constituye en uno de los pilares sobre los cuales debe construirse una práctica sana que permita conciliar los beneficios y los riesgos que suponen las nuevas tecnologías. Al respecto, la autoridad británica de protección de datos personales ha señalado que "es esencial que los partidos políticos y las campañas operen en un terreno de juego equilibrado al acceder al electorado, y que los votantes tengan acceso a toda la gama de mensajes e información política disponible, así como que comprendan quiénes son los autores de dicha información".[91]

Lo anterior supone que los actores políticos y quienes se benefician del ecosistema digital cumplan con los principios, deberes y obligaciones en materia de protección de datos personales. La transparencia en las políticas de privacidad, el consentimiento libre e informado para el tratamiento de datos personales y las finalidades legítimas del tratamiento de dicha información, entre otros principios, configuran los elementos esenciales que deben regir la comunicación política hacia la ciudadanía. Ello no implica que los partidos políticos no puedan hacer uso de la información personal de los electores, sino que dicho uso debe realizarse de manera lícita y diligente, especialmente tratándose de datos personales sensibles que se utilizan para el envío de propaganda o publicidad dirigida.

[91] ICO, *Investigation into the use of data analytics in political campaigns. A report to Parliament, op. cit.,* p. 11. Traducción de las autoras.

De esta forma, la democracia, la privacidad y la protección de datos personales adquieren un sentido y un valor comunes. Por una parte, brindan garantías que permiten la posibilidad de elegir y participar en la toma de decisiones políticas de manera libre e informada y, por la otra, repelen cualquier acto de coacción o intrusión ilegítima que reduzca injustificadamente el valor democrático de la libertad.

Reflexiones finales

El advenimiento de internet y el desarrollo trepidante de las tecnologías de la información y comunicación hacen necesario hoy más que nunca el entendimiento de la relación dialéctica entre la democracia, por una parte, y los derechos a la vida privada y a la protección de datos personales, por la otra.

Estas tecnologías constituyen un instrumento muy poderoso para dotar de efectividad los derechos tradicionalmente asociados a la participación directa e indirecta de la ciudadanía en el ejercicio democrático. La libertad de expresión y el derecho a la información son buena muestra de ello. Pero también su utilización y sus cada vez más sofisticadas capacidades y alcances imponen nuevos retos para la salvaguarda de verdaderos espacios de autonomía, que permitan la formación de personas capaces de discernir entre las opciones que les presentan y de elaborar sus propias opiniones y juicios.

Se trata, pues, de incorporar el valor democrático de la libertad al uso de la tecnología a través de la promoción, protección, respeto y garantía de los derechos a la vida privada y la protección de los datos personales, a fin de evitar su utilización para la realización de injerencias arbitrarias o abusivas, sea por parte del Estado o de terceros, que, incluso, puedan dar lugar a ciertas formas de manipulación política; a todo lo cual se añaden las obligaciones positivas del Estado para dotar a las personas de un cierto poder de control y disposición sobre la información que les concierne. La autodeterminación informativa en el entorno digital se constituye en el medio necesario para que la ciudadanía pueda tener una información completa sobre quién detenta su información personal, para qué fines concretos será utilizada y cómo será procesada. Sólo de esta forma es justificable el tratamiento de los datos personales con fines políticos mediante técnicas de *big data*, inteligencia artificial y *machine learning*.

Así, la prevalencia y la subsistencia de la democracia, tanto en su dimensión sustantiva como procedimental, suponen la efectividad de los derechos a la vida privada y a la protección de datos personales. Su propio diseño y funcionamiento dependen de ello. Pero también, en un sentido inverso, la tutela y la efectividad

de estos derechos sólo pueden darse en un entorno democrático. La prueba de esta relación intrínseca consiste, parafraseando a Bobbio,[92] en el hecho histórico de que "cuando caen, caen juntos".

[92] Norberto Bobbio, *op. cit.,* p. 16.

Fuentes consultadas

Bibliografía

Alexy, Robert, "Constitutional Rights and Proportionality", en *Revus, Journal for constitutional theory and philosophy of law*, núm. 22, Eslovenia, 2014.

Black, Edwin, *IBM and the Holocaust*, Estados Unidos de América, Crown Books, 2001.

Bobbio, Norberto, *El futuro de la democracia*, México, Fondo de Cultura Económica, 1986.

Botero, Catalina, *Libertad de expresión e internet. Relatoría Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos de la OEA*, *s.l.,* OEA/CIDH, 2013.

Cerdas, Rodolfo, "Democracia y Derechos Humanos", en *Estudios de Derechos Humanos*, tomo I, San José, Instituto Interamericano de Derechos Humanos, 1994.

De Hert, Paul y Serge Gutwirth, "Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action", en Gutwirth, Serge *et al*. (eds.), *Reinventing Data Protection?*, Utrecht, Springer, 2009.

Ferrajoli, Luigi, *Poderes salvajes. La crisis de la democracia constitucional*, prólogo y traducción de Perfecto Andrés Ibáñez, Madrid, Trotta, 2011.

Galindo, Fernando, "Democracia, internet y gobernanza: una concreción", en *Seqüência*, núm. 65, Brasil, 2012.

García Mahamut, Rosario, "Partidos políticos y derecho a la protección de datos en campaña electoral: tensiones y conflictos en el ordenamiento español", en *Teoría y realidad constitucional,* núm. 35, Madrid, UNED, 2015.

García Ricci, Diego, *Para entender el derecho a la privacidad,* México, Nostra, 2017.

Gavison, Ruth, "Privacy and the Limits of Law", en *The Yale Law Journal*, vol. 89, núm. 3, Massachusetts, enero de 1980.

Heredero Higueras, Manuel, "La Sentencia del Tribunal Constitucional de la República Federal Alemana relativa a la Ley del Censo de Población de 1983", en *Documentación*

administrativa DA, núm. 198, España, Instituto Nacional de Administración Pública, 1983.

Maqueo, María S. *et al*., "Protección de datos personales, privacidad y vida privada: la inquietante búsqueda de un equilibrio global necesario", en *Revista de Derecho (Valdivia)*, vol. XXX, núm. 1, Chile, junio 2017, disponible en https://scielo.conicyt.cl/scielo.php?script=sci_abstract&pid=S0718-09502017000100004&lng=es&nrm=iso

Mayer, Jonathan y Patrick Mutchler, "MetaPhone: The Sensitivity of Telephone Metadata", *s.d.,* 12 de marzo de 2014, disponible en http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/

Nollkaemper, André y Rosanne van Alebeek, "The Legal Status of Decisions by Human Rights Treaty Bodies in National Law", en H. Keller, y G. Ulfstein (eds.), *Human Rights Treaty Bodies*, Amsterdam, Cambridge University Press, 2011.

Piñar Mañas, José Luis, *¿Existe la privacidad?*, Madrid, CEU Ediciones, 2008.

Prosser, William, "Privacy", en *California Law Review*, vol. 48, núm. 3, California, 1960.

Rodotà, Steffano, "Democracia y protección de datos", en *Cuadernos de Derecho Público*, tr. revisada por José Luis Mañas, núms. 19-20, España, mayo a diciembre de 2013.

Roessler, Beate, "New Ways of Thinking about Privacy", en John Dryzek *et al.* (eds.), *Oxford Handbook of Political Theory*, 2009 (versión en línea).

Salazar, Luis y José Woldenberg, *Principios y valores de la democracia*, México, Instituto Nacional Electoral (Cuadernos de Divulgación de la Cultura Democrática, núm. 1), 2016, disponible en https://portalanterior.ine.mx/archivos2/portal/historico/contenido/recursos/IFE-v2/DECEYEC/DECEYEC-CuadernosdeDivulgacion/docs/01.pdf

Salazar, Pedro, *La democracia constitucional*, México, Fondo de Cultura Económica, 2006.

Warren, Adam *et al.,* "Sources of Literature on Data Protection and Human Rights", en *Journal of Information Law and Technology (JILT),* Inglaterra, 2 de julio de 2001, disponible en https://warwick.ac.uk/fac/soc/law/elj/jilt/2001_2/warren/

Warren, Samuel y Louis Brandeis, "The Right to Privacy", en *Harvard Law Review*, vol. IV, núm. 5, Cambridge, diciembre de 1890.

Westin, Alan, *Privacy and freedom,* Nueva York, Ig Publishing, 1967.

_____, "Social and Political Dimensions of Privacy", en *Journal of Social Issues*, núm. 2, Nueva Jersey, 2003.

Wring, Dominic, "Reconciling Marketing with Political Science: Theories of Political Marketing", en *Journal of Marketing Management*, Inglaterra, vol. 13, 1997.

Documentos

ACE Proyecto. Red de Conocimientos Electorales, Voz "Secrecía del Voto", Versión 2.0, s.d., disponible en: http://aceproject.org/main/espanol/ei/eie12a.htm

Asamblea General de las Naciones Unidas, Resolución 68/167 "El derecho a la privacidad en la era digital", *s.l.,* aprobada el 18 de diciembre de 2013.

_____, Resolución 69/166 "El derecho a la privacidad en la era digital", *s.l.,* aprobada el 18 de diciembre de 2014.

Carta Africana de Derechos Humanos y de los Pueblos, aprobada durante la XVIII Asamblea de la Organización de la Unión Africana, Nairobi, Kenia, 27 de julio de 1981.

Carta de los Derechos Fundamentales de la Unión Europea, publicada en el *Diario Oficial de las Comunidades Europeas*, Estrasburgo, 18 de diciembre de 2000.

Comisión Europea, *Comunicación de la Comisión al Parlamento Europeo y al Consejo*, Bruselas, 2013.

Comité de Derechos Humanos de la Organización de las Naciones Unidas, Communication No. 488/1992, Toonen v. Australia, ONU, Doc. CCPR/C/50/D/488/1992, 31 de marzo de 1994.

_____, Observación general No. 16, adoptada en el 32º periodo de sesiones, 1988.

_____, Observación general No. 35, adoptada en el 112º periodo de sesiones, 2014.

Conferencia Internacional de Autoridades de Protección de Datos Personales y Privacidad, "Resolución sobre el Uso de Datos Personales para la Comunicación Política", adoptada en Montreaux, Suiza, del 14 a 16 de septiembre de 2005.

Convención Americana de Derechos Humanos, San José, Costa Rica, 22 de noviembre de 1969.

Convención de la Unión Africana sobre Ciberseguridad y la Protección de Datos Personales, adoptada en la XXIII Sesión Ordinaria de la Asamblea de la Organización de la Unión Africana, Malabo, Guinea Ecuatorial, 27 de junio de 2014.

Convención de Viena sobre el Derecho de los Tratados, Comisión de Derecho Internacional de las Naciones Unidas, Viena, entrada en vigor el 27 de enero de 1980.

Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares, adoptada por la Asamblea General de las Naciones Unidas en su Resolución 45/158, de 18 de diciembre de 1990.

Convención sobre los Derechos del Niño, adoptada y abierta a la firma y ratificación por la Asamblea General de las Naciones Unidas en su Resolución 44/25 de 20 de noviembre de 1989, en vigor el 2 de septiembre de 1990.

Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales (Convenio Europeo de Derechos Humanos), Roma, Italia, 4 de noviembre de 1950.

Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, Estrasburgo, Francia, 28 de enero de 1981.

Corte Interamericana de Derechos Humanos, *Caso Artavia Murillo y otros ("Fecundación in vitro") vs. Costa Rica*, Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 28 de noviembre de 2012.

_____, *Caso Atala Riffo y niñas vs. Chile,* Fondo, Reparaciones y Costas, Sentencia de 24 de febrero de 2012.

_____, *Caso Escher y otros vs. Brasil*, Excepciones Preliminares, Fondo, Reparaciones y Costas, Sentencia de 6 de julio de 2009.

_____, *Caso Fontevecchia y D´Amico vs. Argentina*, Fondo, Reparaciones y Costas, Sentencia de 29 de noviembre de 2011.

_____, *Caso Tristán Donoso vs. Panamá,* Excepción Preliminar, Fondo, Reparaciones y Costas, Sentencia de 27 de enero de 2009.

Declaración conjunta sobre Universalidad y el Derecho a la Libertad de Expresión, ONU/OSCE/OEA/CADHP, París, mayo de 2014.

Declaración Universal de Derechos Humanos, adoptada por la Asamblea General de las Naciones Unidas en su Resolución 217 A (III), París, Francia, 10 de diciembre de 1948.

European Data Protection Supervisor (EDPS), *Opinion on online manipulation and personal data*, Opinión 3/2018, Bruselas, EDPS, 19 de marzo de 2018.

Information Commissioner´s Officer (ICO), *Big data, artificial intelligence, machine learning and data protection*, Versión 2.2, Londres, Inglaterra, ICO, 4 de septiembre de 2017, disponible en https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf

_____, *Democracy Disrupted? Personal information and political influence*, Londres, Inglaterra, 11 de julio de 2018, disponible en https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf

_____, *Investigation into the use of data analytics in political campaigns. A report to Parliament*, Londres, Inglaterra, 6 de noviembre de 2018, disponible en https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf

La Rue, Frank, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/HRC/23/40, 17 de abril de 2013.

Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, publicada en el *Diario Oficial de la Federación*, México, 26 de enero de 2017.

Organización de los Estados Americanos (OEA), *Carta Democrática Interamericana*, Vigésimo Octavo Período Extraordinario de Sesiones, Lima, Perú, 11 de septiembre de 2001.

Pacto Internacional de Derechos Civiles y Políticos, adoptado y abierto a la firma, ratificación y adhesión por la Asamblea General de la Organización de las Naciones Unidas en su resolución 2200 A (XXI), *s.l.,* adoptado el 16 de diciembre de 1966 y en vigor el 32 de marzo de 1976.

Senado de la República, "Dictamen de las Comisiones Unidas de Relaciones Exteriores, Europa; de Relaciones Exteriores; y de Anticorrupción y Participación Ciudadana, con proyecto de decreto por el que se aprueba la adhesión de México al Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal y a su Protocolo Adicional relativo a las Autoridades de Control y a los Flujos Transfronterizos de Datos Personales, hechos el veintiocho de enero de mil novecientos ochenta y uno y el ocho de noviembre de dos mil uno, respectivamente", México, 18 de abril de 2018.

Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, "Acuerdo mediante el cual se aprueban las disposiciones administrativas de carácter general para la elaboración, presentación y valoración de evaluaciones de impacto a la protección de datos personales", publicado en el *Diario Oficial de la Federación,* México, 23 de enero de 2018.

Suprema Corte de Justicia de la Nación, Amparo en Revisión 237/2014, México, Primera Sala, ministro Arturo Zaldívar Lelo de Larrea.

_____, Contradicción de tesis 293/2011, México, Pleno.

Tribunal Europeo de Derechos Humanos, *Association for European Integration and Human Rights and Ekimdzhiev*, Sentencia de 28 de junio de 2007.

_____, *Barbulescu v. Rumania*, Sentencia de 12 de enero de 2016 [Voto disidente del Juez Pinto de Albuquerque].

_____, *Big Brother Watch and Others v. The United Kingdom*, Sentencia de 13 de septiembre de 2018.

_____, *Case of Z v. Finland*, Sentencia de 25 de febrero de 1997.

_____, *Kruslin v. France*, Sentencia de 24 de abril de 1990.

_____, *Malone v. The United Kingdom,* Sentencia de 2 de agosto de 1984.

_____, *Niemietz v. Germany*, Sentencia de 16 de diciembre de 1992.

_____, *Roman Zakharov v. Russia*, Sentencia de 4 de diciembre de 2015.

_____, *Valenzuela Contreras v. España*, Sentencia de 30 de julio de 1998.

_____, *Weber and Saravia v. Germany*, Sentencia de 29 de junio de 2006.

Artículos

"5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día", en *BBC News*, 21 de marzo de 2018, disponible en https://www.bbc.com/mundo/noticias-43472797

Mac Askill, Ewen y Alex Hern "Edward Snowden: 'The people are still powerless, but now they're aware'", en *The Guardian*, 4 de junio de 2018, disponible en https://www.theguardian.

com/us-news/2018/jun/04/edward-snowden-people-still-powerless-but-aware

Woollacott, Emma, "UK Mass Survaillance Ruled Unlawful", en *Forbes*, 13 de septiembre de 2018, disponible en https://www.forbes.com/sites/emmawoollacott/2018/09/13/uk-mass-surveillance-ruled-illegal/#2b94584863

Sobre las autoras

María Solange Maqueo Ramírez es directora y profesora-investigadora de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas (CIDE); doctora *Summa Cum Laude* en el programa Estado de Derecho y Políticas Públicas, por la Universidad de Salamanca, España. Miembro del Sistema Nacional de Investigadores, nivel I; presidenta del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales; líder del Grupo de Derechos Digitales del Centro de Política Digital para América Latina del CIDE; y coordinadora académica del Diplomado en Privacidad, Regulación y Gobernanza de Datos.

Alessandra Barzizza Vignau es egresada de la Licenciatura en Derecho por el CIDE, y actualmente se desempeña como abogada en el área de Asesoría Jurídica de Altán Redes. Cuenta con un diplomado en Privacidad,

Regulación y Gobernanza de Datos por el CIDE y un curso de Derecho Internacional Público impartido en la Academia de Derecho Internacional de La Haya. En 2018 asistió a la Escuela del Sur de Gobernanza de Internet, impartida por la Organización de los Estados Americanos. Durante sus estudios de licenciatura fue campeona nacional del Concurso Nacional de Derecho Constitucional en 2017 y dos veces participante en el concurso Phillip C. Jessup International Law Moot Court Competition, donde obtuvo el premio de mejor orador a nivel nacional.

41

Democracia, privacidad y protección de datos personales

se terminó de imprimir en noviembre de 2020 en Litográfica Ingramex, S.A. de C.V., Centeno 195, col. Valle del Sur, Alcaldía Iztapalapa, C.P. 09819, Ciudad de México.

Se utilizaron las familias tipográficas Acumin Pro y Slate Pro; papel Bond ahuesado cultural de 90 gramos y forros en cartulina Bristol de 240 gramos.

La edición consta de 1,000 ejemplares y estuvo al cuidado de la Dirección Ejecutiva de Capacitación Electoral y Educación Cívica del Instituto Nacional Electoral.

Consulta las bases de datos del INE

CUADERNOS DE DIVULGACIÓN DE LA CULTURA DEMOCRÁTICA
(TÍTULOS PUBLICADOS)

1. **Principios y valores de la democracia,** Luis Salazar y José Woldenberg, 1993
2. **La cultura política democrática,** Jacqueline Peschard, 1994
3. **La democracia como forma de gobierno,** José F. Fernández Santillán, 1995
4. **La participación ciudadana en la democracia,** Mauricio Merino, 1995
5. **Elecciones y democracia,** José Antonio Crespo, 1995
6. **Gobernabilidad y democracia,** Antonio Camou, 1995
7. **Sistemas electorales y de partidos,** Leonardo Valdés, 1995
8. **Partidos políticos y democracia,** Jaime F. Cárdenas Gracia, 1996
9. **Esferas de la democracia,** Jesús J. Silva-Herzog Márquez, 1996
10. **Tolerancia y democracia,** Isidro H. Cisneros, 1996
11. **Oposición y democracia,** Soledad Loaeza, 1996
12. **Estado de derecho y democracia,** Jesús Rodríguez Zepeda, 1996
13. **Diálogo y democracia,** Laura Baca Olamendi, 1996
14. **Democratización y liberalización,** César Cansino, 1997
15. **Consulta popular y democracia directa,** Jean-François Prud'homme, 1997
16. **Democracia y educación,** Gilberto Guevara Niebla, 1998
17. **Federalismo, gobiernos locales y democracia,** Tonatiuh Guillén López, 1999
18. **Libertad y democracia,** Víctor Alarcón Olguín, 1999
19. **Gobiernos y democracia,** Javier Hurtado, 1999
20. **Sistemas parlamentario, presidencial y semipresidencial,** Ricardo Espinoza Toledo, 1999
21. **Rendición de cuentas y democracia. El caso de México,** Luis Carlos Ugalde, 2002
22. **Concepciones de la democracia y justicia electoral,** José Ramón Cossío D., 2002

23. **Género y democracia,** Estela Serret, 2004
24. **Comunicación y democracia,** Enrique E. Sánchez Ruiz, 2004
25. **Democracia y (cultura de la) legalidad,** Pedro Salazar Ugarte, 2006
26. **Multiculturalismo y democracia,** Lourdes Morales Canales, 2008
27. **Ciudadanía y democracia,** Alberto J. Olvera, 2008
28. **Democracia y formación ciudadana,** Teresa González Luna Corvera, 2010
29. **Sufragio extraterritorial y democracia,** Víctor Alejandro Espinoza Valle, 2011
30. **Políticas públicas y democracia,** David Arellano Gault y Felipe Blanco, 2013
31. **Derechos fundamentales y democracia,** Miguel Carbonell, 2013
32. **Formación ciudadana en México,** Silvia L. Conde, 2014
33. **Democracia y organismos internacionales,** Alejandra Nuño, 2016
34. **Democracia y medios en México: el papel del periodismo,** Manuel Alejandro Guerrero, 2016
35. **Democracia y burocracia,** Guillermo M. Cejudo, 2016
36. **Democracia, populismo y elitismo,** Luis Daniel Vázquez Valencia, 2016
37. **Los derechos humanos y la democracia en el sistema interamericano,** Natalia Saltalamacchia y María José Urzúa, 2016
38. **Mujeres y derechos políticos en México: una introducción conceptual,** Ricardo Ruiz Carbonell, 2017
39. **Democracia y gobiernos municipales en México: de la política a las políticas,** Oliver D. Meza, 2017
40. **Democracia y género. Historia del debate público en torno al sufragio femenino en México,** Gabriela Cano, 2018
41. **Democracia, privacidad y protección de datos personales,** María Solange Maqueo Ramírez y Alessandra Barzizza Vignau, 2019

41

CUADERNOS DE
DIVULGACIÓN DE LA
CULTURA DEMOCRÁTICA

Consulta el catálogo
de publicaciones del INE

INE
Instituto Nacional Electoral