

Revista

ESTUDIOS EN
DERECHO
A LA INFORMACIÓN



Universidad Nacional Autónoma de México
Instituto de Investigaciones Jurídicas
Facultad de Ciencias Políticas y Sociales
Instituto Nacional de Transparencia, Acceso
a la Información y Protección de Datos Personales
Centro de Investigación y Docencia Económicas

INSTITUTO DE INVESTIGACIONES JURÍDICAS

Director

Dr. Pedro Salazar

Secretaria académica

Dra. Issa Luna Pla

Secretario técnico

Lic. Raúl Márquez Romero

Jefa del Departamento de Publicaciones

Mtra. Wendy Vanesa Rocha Cacho

Revista Estudios en Derecho a la Información, núm. 8, julio-diciembre de 2019, es una publicación semestral editada por la Universidad Nacional Autónoma de México, Ciudad Universitaria, Coyoacán, 04510 Ciudad de México, a través del Instituto de Investigaciones Jurídicas, Circuito Maestro Mario de la Cueva s/n, Ciudad de la Investigación en Humanidades, Ciudad Universitaria, 04510 Ciudad de México, teléfono 5622 7474, correo electrónico: *autoresredi@gmail.com*. Editor responsable: Daniel Vázquez. Certificado de Reserva de Derechos al Uso Exclusivo del Título: 04-2016-021916284300-102. Certificado de Licitud de Título y Contenido: 17309. ISSN (versión electrónica): 2594-0082.

Miguel López Ruiz

Cuidado de la edición

José Antonio Bautista Sánchez

Formación en computadora

Ana Julieta García Vega

Diseño de interiores

ESTUDIOS EN DERECHO A LA INFORMACIÓN

Revista

Dr. Daniel Vázquez
Dr. Khemvirg Puente M.
Directores

Lic. Raúl Márquez Romero
Mtra. Wendy Vanesa Rocha Cacho
Coordinación Editorial

CONSEJO EDITORIAL



Pedro Salazar Ugarte (México, UNAM-IIJ); Fernando Castañeda Sabido (México, UNAM-FCPyS); Patricia Kurczyn Villalobos (México, INAI); Sergio López Ayllón (México, CIDE); Miguel Carbonell Sánchez (México, UNAM-IIJ); Ana Elena Fierro Ferráez (México, CIDE); Julio Alejandro Téllez Valdés (México, UNAM-IIJ); Diego Valadés Ríos (México, UNAM-IIJ); María Solange Maqueo Ramírez (México, CIDE); Roberto Saba (Argentina, Universidad de Palermo); Jacqueline Peschard Mariscal (México, UNAM-FCPyS); Alonso Gómez Robledo Verduzco (México, UNAM-IIJ); Mercedes de Vega Armijo (México, Archivo General de la Nación); Francisco Javier Acuña Llamas (México, INAI); Carlos Humberto Reyes Díaz (México, UNAM, Coordinación de Posgrado en Derecho); Ana Azurmendi (España, Universidad de Navarra); William Guilles (Francia, Chaire des Amériques de l'Université Paris 1 Panthéon Sorbonne); Iréne Bouhadana (Francia, Chaire des Amériques de l'Université Paris 1 Panthéon Sorbonne); Angélica Cuéllar Vázquez (México, UNAM-FCPyS); Arturo Chávez López (México, UNAM-FCPyS); Areli Cano Guadiana (México, Auditoría Superior de la Federación).



COMITÉ EDITORIAL

Guillermo M. Cejudo (México, CIDE); Blanca Lilia Ibarra (México, Instituto Nacional de Acceso a la Información); María Marván Laborde (México, UNAM-IIJ); Laura Beatriz Montes de Oca Barrera (México, UNAM-IIS); Alejandra Ríos Cazares (México, CIDE); José Roldán Xopa (México, CIDE); Egbert Sánchez Vanderkast (México, UNAM-IIBI).

Nidia Andrade Cárdenas
Asistente editorial

“Las opiniones expresadas por los autores no necesariamente reflejan la postura del editor de la publicación. Se autoriza la reproducción total o parcial de los textos aquí publicados, siempre y cuando se cite la fuente completa y/o la dirección electrónica de la publicación”.

<http://revistas.juridicas.unam.mx/index.php/derecho-informacion/index>



Primera edición: 31 de julio de 2019

DR © 2019. Universidad Nacional Autónoma de México

INSTITUTO DE INVESTIGACIONES JURÍDICAS

Circuito Maestro Mario de la Cueva s/n
Ciudad de la Investigación en Humanidades
Ciudad Universitaria, 04510 Ciudad de México

Impreso y hecho en México

ISSN (versión electrónica): 2594-0082

CONTENIDO

ARTÍCULOS

Nuevos desafíos para la protección de datos personales en México. La regulación de la tecnología <i>blockchain</i>	3
Manuel Gustavo OCAMPO MUÑOA	
<i>Big data, big data analytics</i> y datos personales en los tiempos del Internet: de la autorregulación estadounidense al Reglamento General de Protección de Datos de la Unión Europea	21
Mauricio Augusto CALCANELO MONTS	
Gobierno cercano y moderno: una mirada desde los estándares internacionales del acceso a la información pública	45
Arturo Miguel CHIPULI CASTILLO	
El efecto transformador de la tensión entre democracia, libertad de expresión e información y dignidad individual durante el correato	69
María Fernanda COBO MANTILLA	

COMENTARIOS JURÍDICOS

Comentario jurídico a la Recomendación General 29 “Sobre el expediente clínico como parte del derecho a la información en materia de salud” emitida por la CNDH	95
Alejandro DÍAZ PÉREZ	
Rita Astrid MUCIÑO CORRO	

CONTENIDO

RESEÑAS BIBLIOGRÁFICAS

Los límites de la privacidad	111
Óscar ZAVALA GAMBOA	

VI

-
-
-

ARTÍCULOS



NUEVOS DESAFÍOS PARA LA PROTECCIÓN DE DATOS
PERSONALES EN MÉXICO. LA REGULACIÓN
DE LA TECNOLOGÍA BLOCKCHAIN
NEW CHALLENGES FOR THE PROTECTION
OF PERSONAL DATA IN MEXICO. THE REGULATION
OF BLOCKCHAIN TECHNOLOGY

● ○ ●

*Manuel Gustavo OCAMPO MUÑOA**

RESUMEN: En este documento se pretende verificar la importancia de contar con un marco regulatorio adecuado para el uso de la tecnología *blockchain* en México en lo relativo a la protección de los datos personales en posesión de los particulares, para lo cual se estudian brevemente la trascendencia jurídica de la utilización de la cadena de bloques en diferentes actividades y algunos temas específicos que lo entrelazan con ese derecho fundamental, así como sus beneficios y los retos de su implementación en el ámbito público.

PALABRAS CLAVE: *blockchain*, protección de datos personales, *bitcoin*.

ABSTRACT: *This document aims to verify the importance of having an adequate regulatory framework for the use of Blockchain*

* Maestro en derecho por el Instituto de Investigaciones Jurídicas de la Universidad Autónoma de Chiapas (IJJ-UACH). Cuenta con un diplomado en protección de datos personales por la Universidad de Guadalajara, y es licenciado en derecho por la UACH. Actualmente es candidato a doctor en derecho por el IJJ-UNACH, y miembro del Sistema Estatal de Investigadores del Consejo de Ciencia y Tecnología del Estado de Chiapas, nivel II. Correo: manuel.ocampo@ijj-unach.mx.

Fecha de recepción: 18 de diciembre de 2018.

Fecha de dictamen: 25 de marzo de 2019.

MANUEL GUSTAVO OCAMPO MUÑOZA

Technology in Mexico in relation to the protection of personal data held by individuals, for which the transcendence of the use of the blockchain in different activities and some specific issues that intertwine it with that fundamental right are briefly studied, as well as its benefits and the challenges of its implementation in the public sphere.

4

KEY WORDS: *blockchain, protection of personal data, bitcoin.*

I. INTRODUCCIÓN

La utilización de las criptomonedas genera un nuevo desafío para la ciencia jurídica en general, y en lo particular en la regulación del derecho a la protección de datos personales. El rápido desarrollo de las unidades de moneda ha generado otras tecnologías que la complementan, como es el caso de las denominadas cadenas de bloques o *blockchain*, cuya utilidad va más allá de transferir valor a esas monedas, sino que involucran precisamente el manejo de información personal, lo que despierta especial interés en los sistemas jurídicos, pues afecta el derecho humano a la protección de datos.

Es por ello que el objetivo de este trabajo es verificar la importancia de establecer un marco regulatorio adecuado a la tecnología *blockchain* en México, con énfasis en la protección de datos personales en posesión de los particulares.

El trabajo se ha dividido, para efectos didácticos, en siete apartados. El primero corresponde a esta introducción, y los restantes, al desarrollo de diferentes temas relacionados con la *blockchain*, sus aplicaciones, sus beneficios y los retos de su implementación en el ámbito público.

En el apartado denominado “La inclusión de la *blockchain* en lo jurídico”, se describe la trascendencia de la cadena de bloques en el campo del derecho, así como algunos de los retos y la importancia del diseño de un adecuado marco regulatorio.

En el tercer apartado se establece el marco teórico. Se definen los componentes de la *blockchain* y el contenido del derecho a la protección de datos personales, con la finalidad de entender el objetivo, el planteamiento del problema, la propuesta de solución, la metodología y el resultado esperado en este trabajo.

En los apartados cuarto y quinto se aborda la trascendencia jurídica de la *blockchain* en México; además, se pretende relacionar sus diferentes

usos con lo jurídico para justificar la necesidad de un marco regulatorio amplio; asimismo, se señalan los temas específicos del derecho a la protección de datos personales en posesión de los particulares que se relacionan con el uso de la *blockchain*. Se busca precisar los aspectos que entrelazan ambos temas en nuestro país.

En las reflexiones finales, a manera de conclusión, se realizan algunos apuntes respecto a la manera en como la sociedad mexicana asimila esta tecnología y los posibles campos que deben regularse; por último, se enlistan las fuentes utilizadas en la elaboración de este documento.

5

II. LA INCLUSIÓN DE LA *BLOCKCHAIN* EN LO JURÍDICO

La tecnología *blockchain* tiene diferentes usos y ventajas; por ejemplo, ofrece la oportunidad a la administración pública, de ser más eficiente. Su relevancia jurídica salta a la vista al ser parte del mundo del *big data* y por tener una creciente demanda en las organizaciones.

El uso de las monedas y pagos digitales; los sistemas registrales, como el de propiedad; los sistemas electorales, en específico en el tema del sufragio el día de la elección; la gestión de identidad; el diseño de cadenas de suministro; el cuidado de la salud; los registros corporativos; los sistemas de fiscalización y la gestión de derechos, son algunos de los temas que entrelazan esta nueva tecnología con el campo del derecho, mismos que se describirán de manera breve para ilustrar la vinculación entre la tecnología y el derecho.

El efectuar pagos utilizando dispositivos móviles¹ genera que el dinero físico tenga menos uso, lo cual puede traer beneficios en la economía al disminuir el dinero circulante; sin embargo, en sociedades como la mexicana existen barreras políticas, culturales y económicas que lo impiden, por considerarlo inseguro.

En los sistemas electorales, la innovación ha impactado en su elemento fundamental como mecanismo de expresión de la voluntad ciudadana: el voto electrónico. Realizar elecciones en México utilizando la cadena de bloques como herramienta por parte del Instituto Nacional Electoral quizá reduciría los costos del proceso electoral; no obstante, no se ha logrado tener una legislación en materia de voto electrónico por razones de presupuesto y privacidad. La principal causa demostrada hasta ahora es la des-

¹ Tal es el caso de Dinamarca, país donde su Banco Central dejó de fabricar billetes y monedas desde 2013 para invertir en sistemas electrónicos.

MANUEL GUSTAVO OCAMPO MUÑOZA

confianza del electorado, el temor que provocan los medios electrónicos, y la distancia del soporte físico.

En cuanto a la gestión de identidad, ésta es una amplia área administrativa que se ocupa de la identificación de individuos en un sistema, así como de controlar su acceso a los recursos dentro de ese sistema mediante la asociación de derechos de usuario y restricciones conforme a la identidad establecida. En un entorno empresarial, la gestión de identidades se utiliza para aumentar la seguridad y la productividad, mientras que se disminuyen costos y el esfuerzo redundante. En tanto que se trata de un sistema de control, el desafío es establecer el tipo de contratación que se debe implementar para el personal y el nivel de responsabilidad que debe concederse a quienes lo manejen.

En las cadenas de suministro, la utilización de la *blockchain* en su diseño permite organizar mejor el conjunto de actividades, instalaciones y medios de distribución necesarios para llevar a cabo el proceso de venta de un producto en su totalidad. Lo anterior es un beneficio para el consumidor, pero trae consigo la falta de certeza en el acto jurídico que se realice; es decir, nuestro sistema jurídico no contempla categóricamente los contratos de compraventa que se realicen desde plataformas o sitios web.

Algo similar sucede en el área de la salud, en la que, gracias a los desarrollos tecnológicos, es posible olvidarse de las visitas médicas de rutina al contratar los servicios de un proveedor de cuidados de la salud. El médico o enfermera pueden proporcionar información importante, y así ayudar a prevenir enfermedades, así como proveer tratamientos para cualquier problema que una persona pueda experimentar desde cualquier parte del mundo utilizando una aplicación; sin embargo, aún no existe claridad en cuanto al acto jurídico que se celebra o la modalidad de éste, o incluso la legislación aplicable.

En lo que respecta a los registros corporativos como medios de control de las empresas, estos libros sociales tienen como objetivo asentar actos importantes de la sociedad: la distribución de los socios, si aumentó su capital, si compraron algún activo o si los accionistas tomaron cualquier acuerdo. En esos libros se encuentran la historia y las acciones que la sociedad ha llevado a cabo durante su vida. Hoy día es posible sustituirlos por una base de datos protegida por una cadena de bloques. No obstante lo anterior, el principal problema jurídico resulta ser la tradición de derecho escrito de México.

En cuanto a los sistemas de fiscalización, en nuestro país existe el Sistema Nacional de Fiscalización (SNF), que se define como

El conjunto de mecanismos interinstitucionales de coordinación entre los órganos responsables de las tareas de auditoría gubernamental en los distintos órdenes de gobierno, con el objetivo de maximizar la cobertura y el impacto de la fiscalización en todo el país, con base en una visión estratégica, la aplicación de estándares profesionales similares, la creación de capacidades y el intercambio efectivo de información, sin incurrir en duplicidades u omisiones (LGSNA, artículo 3).

7

En México existe un amplio andamiaje de control y supervisión, tanto al interior como al exterior de los distintos órganos que desempeñan funciones de gobierno. La Auditoría Superior de la Federación, la Secretaría de la Función Pública, las contralorías de las entidades federativas, las entidades de fiscalización superiores locales, las contralorías municipales y las contralorías internas de los órganos constitucionalmente autónomos deben tener la capacidad de mantener una vigilancia permanente sobre el desempeño de los entes públicos.²

En ese sentido, sería pertinente la implementación de la tecnología *blockchain*; sin embargo, dado el carácter confidencial de la información que se maneja, el nivel de protección requiere de la autorización del Congreso de la Unión, y, por ende, de la socialización de la idea con los diferentes grupos parlamentarios.

Por último, con la irrupción de los contenidos digitales y la gran facilidad para difundirlos gracias a Internet se hizo necesaria una nueva forma de proteger los derechos de sus autores y editores. Fue así como nació la expresión y gestión de derechos digitales. También conocidas como “programas anticopias”, son tecnologías de control de acceso usadas por editoriales y titulares de derechos de autor para limitar el uso de medios o dispositivos digitales a personas o equipo no autorizado. También se utiliza para referir a las restricciones asociadas a instancias específicas de obras digitales o dispositivos.

Tal como se advierte de lo anterior, la *blockchain* cada día adquiere más importancia; su presencia en la vida cotidiana es más usual de lo se puede pensar, al grado que, quizá sin saberlo ni tener idea de sus alcances, ya la hemos utilizado. La problemática central que se advierte en su utilización es el tipo de datos que requiere aquélla para ser eficiente, los que sin duda son de carácter personal, e inclusive algunos de ellos, de los considerados sensibles.

² Para mayor información se le invita a consultar la página del Sistema Nacional de Fiscalización en la liga www.snf.org.mx.

MANUEL GUSTAVO OCAMPO MUÑOZA

Lo anterior lleva a plantear algunos cuestionamientos con relación a la *blockchain* y los nuevos desafíos que genera a la protección de datos personales en México, entre otros: ¿cuál es el marco regulatorio adecuado?; ¿cómo se garantiza en ella la protección de datos personales?; ¿qué beneficios proporciona a la sociedad su uso?, y ¿qué sectores o instituciones requieren de su utilización?

8

III. CONCEPTOS BÁSICOS

- Al relacionarse el tema del presente ensayo con la tecnología *blockchain* y la protección de datos personales en México, se requiere establecer algunos conceptos que permitan entender el objetivo, el planteamiento del problema, la propuesta de solución, la metodología y el resultado esperado en este trabajo.

La cadena de bloques es una tecnología que permite la realización confiable y segura de cualquier tipo de transacción entre dos o más personas sin la necesidad de intermediarios, a través de Internet (Criptonoticias, 2017: 5).

Su introducción al mundo se dio a través de la criptomoneda *bitcoin*, que se basó para su implementación en un círculo de socios confiables que hacen negocios regularmente y ya han sido aprobados en cuestiones de seguridad (Velázquez, 2018). Las conversiones de *bitcoin* incluso pueden hacerse en algunas tiendas de conveniencia (Corona, 2018).

La creación de la primera plataforma de esta tecnología se adjudica al mismo creador de la citada moneda digital, Satoshi Nakamoto, quien publicó un artículo sobre su invención y luego desapareció (*La Nación*, 2017).

Hoy, su núcleo es parte del dominio público, y sólo las adiciones y variaciones importantes se pueden patentar. Además, es el proveedor de carteras *bitcoin* más usado, al contar con más de siete millones de clientes y ofrecer todo tipo de datos y gráficos que ayudan a los usuarios y empresas a conocer mejor el mundo de las criptomonedas (Díaz Ruiz, 2017).

Es una tecnología que en su conjunto se explica como un almacén de datos que permite, además de guardar gran cantidad de información, organizarla en bloques, cifrarlos y distribuirlos entre muchos usuarios. Recibe otras denominaciones, como “tecnología *blockchain*”, “tecnología de contabilidad distribuida” o “tecnología *bitcoin*”.

La expresión “tecnología *blockchain*” suele usarse en las cadenas públicas y por todos los desarrolladores y usuarios; la denominación “tecnolo-

gía de contabilidad distribuida” o DLT (*Distributed Ledger Technology*, por sus siglas en inglés) se utiliza en el ámbito del desarrollo privado, y está más bien alejada de *bitcoin* como criptomoneda; mientras que “tecnología *bitcoin*” es el término más ambiguo, y refiere a tres conceptos: la tecnología de contabilidad distribuida en su conjunto, la *blockchain* de *bitcoin* en particular, e incluso los protocolos que han permitido el desarrollo de todas las criptomonedas.

La cadena de bloques es una articulación de tecnologías estructuradas en un sistema naturalmente encriptado, lo que proporciona a los usuarios involucrados, protección de sus identidades y de los datos de sus transacciones. Dicho sistema se encuentra integrado por un libro de contabilidad digital, carteras digitales, mineros y nodos.

En consideración al acceso a los datos almacenados, la cadena de bloques puede clasificarse en pública o privada. En la primera no hay ninguna restricción para la lectura de datos ni para la realización de las operaciones por parte de los usuarios; en cambio, en la segunda, tanto la lectura como las operaciones se limitan a participantes determinados.

En cuanto a la capacidad para generar bloques, se dividen en aquellas sin permisos y con permisos. En la primera no hay restricciones para poder realizar transacciones y crear nuevos bloques, de modo que se ofrecen monedas o activos digitales nativos de la red como recompensa a los usuarios que quieran mantener la red; son descentralizadas, como *bitcoin*. Las segundas son desarrolladas por entidades generalmente privadas, en muchos casos para uso interno, y los usuarios de éstas necesitan permisos por parte de los administradores de la red para interactuar con el protocolo; son centralizadas, es decir, controladas por la entidad, y no por los usuarios.

Ahora bien, con relación al derecho a la protección de datos personales, el punto de partida es el concepto de dato personal. Éste ha sido definido como cualquier información que permita identificar o hacer identificable al individuo (AEPD, 2015: 12-16).

Desde la perspectiva de los derechos fundamentales es el reconocimiento al ciudadano de la facultad de controlar sus datos personales y la capacidad para disponer y decidir sobre ellos. En consecuencia, se trata de un concepto bastante amplio, puesto que puede atribuirse la naturaleza de dato personal a una imagen, a un sonido, a un número de teléfono o a una dirección IP o de correo electrónico (Martínez, 2007: 47-62).

En ese sentido, el derecho a la protección de datos está en constante crecimiento, y, jurídicamente hablando, es probable que esto genere inva-



MANUEL GUSTAVO OCAMPO MUÑOZA

dir otros ámbitos, como el del secreto de las comunicaciones, el derecho a la propia imagen y el de la inviolabilidad del domicilio.³

En el artículo 8 del Convenio para la Protección de los Derechos y las Libertades Fundamentales de 1950 se reconoce por primera vez el derecho de la persona al respeto de su vida privada y familiar, su domicilio y su correspondencia; se encuentra eco de ese derecho en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos de 1966 y en el artículo 11 de la Convención Americana sobre Derechos Humanos de 1969, que prohíben injerencias arbitrarias o ilegales en la vida privada, la familia, el domicilio o la correspondencia, así como los ataques ilegales a la honra y a la reputación. Se considera a la Resolución 509 de la Asamblea del Consejo de Europa de 1968, sobre los derechos humanos y nuevos logros científicos y técnicos, como la generadora de que en diversas leyes en países europeos se abordara el tema, siendo Suecia el primer Estado soberano en promulgar una ley de protección de datos personales en 1973 (Millán Gómez, 2011: 19-48).

Con relación al desarrollo de este derecho fundamental en América, Stewart señala que la Organización de Estados Americanos toma como referencia los logros europeos en la materia, teniendo en cuenta al mismo tiempo los sucesos del propio continente, para de esta manera redactar leyes o disposiciones en códigos debidamente contextualizados por medio de comités, en los que interactúen los Estados miembros (2014: 450).

Esa idea de cooperación interestatal en la protección de datos es necesaria, pues este derecho requiere de una doble naturaleza. Una interna, que disminuya las diferencias entre legislaciones nacionales europeas al mínimo, con el debido respeto a las particularidades de la legislación y cultura nacionales, y asegure que las normas se cumplen y se hagan cumplir con igual rigor en toda la Unión Europea; y la otra externa, que busque la convergencia con otros modelos e intente que otras regiones del planeta se unan a nuestros esfuerzos por la defensa de un derecho fundamental del individuo (Cervera Navas, 2003: 131-143).

Con el objetivo de garantizar estándares de protección de datos elevados y adaptados a la realidad digital del mundo actual, la Unión Europea (UE) presentó el Reglamento General de Protección de Datos (RGPD). Este Reglamento, que deroga la Directiva 95/46/CE, fue aprobado por el Parlamento Europeo en abril de 2016, y entró en vigor veinte días después

³ Al respecto, el artículo 12 de la Declaración Universal de los Derechos Humanos enfatiza la necesidad de garantizar la protección de los datos personales para evitar injerencias o ataques a la vida privada, a la familia y a la reputación.

de su publicación en el *Diario Oficial de la Unión Europea* el 4 de mayo de 2016. Su ámbito de aplicación se extiende a todos los países miembros de la UE y se aplica directamente en todos ellos a partir del 25 de mayo de 2018.

El reglamento devuelve a los ciudadanos el control de sus datos personales y garantiza en toda la UE estándares de protección elevados y adaptados al entorno digital. También incluye nuevas normas mínimas sobre el uso de datos para fines judiciales y policiales. Con este reglamento de protección de datos se consigue un nivel uniforme de protección en toda la UE. Asimismo, ofrece claridad a las empresas con una norma única para toda la UE, que refuerza la confianza y la seguridad jurídica e impulsa la competencia justa (PE, 2016).

Entre otras disposiciones, las nuevas reglas incluyen el derecho al olvido, mediante la rectificación o supresión de datos personales; la necesidad de consentimiento claro y afirmativo de la persona concernida al tratamiento de sus datos personales; la portabilidad o el derecho a trasladar los datos a otro proveedor de servicios; el derecho a ser informado si los datos personales han sido pirateados; lenguaje claro y comprensible sobre las cláusulas de privacidad, y multas de hasta el 4% de la facturación global de las empresas en caso de infracción.

El nuevo paquete de protección de datos también incluye una directiva sobre transmisión de datos para cuestiones judiciales y policiales. La intención es proteger a las personas implicadas en investigaciones policiales o procesos judiciales (sea como víctimas, acusados o testigos) mediante la clarificación de sus derechos y el establecimiento de límites en la transmisión de datos para prevención, investigación, detección y enjuiciamiento de delitos o la imposición de penas. Se han incluido salvaguardas para evitar riesgos para la seguridad pública, al tiempo que se facilita una cooperación más rápida y efectiva entre las autoridades policiales y judiciales.

Al fijar estándares europeos para el intercambio de información, esta norma se convertirá en una herramienta útil para ayudar a las autoridades a trasladar datos personales de manera sencilla y efectiva, asegurando el respeto al derecho fundamental a la privacidad (PE, 2016).

En el caso de México, si bien es cierto que el tema de los datos personales y la protección que merecen ya estaban legalmente contemplados en el ámbito federal desde 2002 a través de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental, éste se encontraba limitado, y no fue hasta la reforma al artículo 60. de la Constitución general de la República (publicada en el *Diario Oficial de la Federación* del 20 de julio de 2007) cuando se incluyó por vez primera el derecho a la privacidad y a la intimidad (Castillo y Monterrey, 2011: 179-216).



MANUEL GUSTAVO OCAMPO MUÑOA

12 Es preciso apuntar que hasta antes de 2010 no se contaba con un instrumento legal que exigiera a los particulares que manejaban datos personales contar mínimamente con un aviso de privacidad ni existían reglas específicas con relación al tiempo en que los podían guardar o qué mecanismos utilizar para depurarlos. Es así que surge la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), publicada el 5 de julio de ese año, con la intención de solventar esas lagunas legales, al establecer las reglas mediante las cuales la ciudadanía podría conocer y en su caso ejercitar y exigir el derecho a la protección de sus datos personales a los particulares, quedando éstos obligados a contar con mecanismos para salvaguardarlos, bajo la supervisión de las autoridades.

IV. TRASCENDENCIA JURÍDICA DE LA *BLOCKCHAIN*

Quizá el más grande desafío que enfrenta el derecho es el relacionado con las tecnologías de la información, pues el ser humano a lo largo de su vida va dejando un cúmulo de datos que se encuentran dispersos, pero que con los actuales desarrollos tecnológicos resulta posible agrupar e interpretar. Esto permite crear un perfil determinado del individuo, y por ende, aumentar sensiblemente la posibilidad de ser objeto de manipulaciones; entonces se presenta la necesidad de que el derecho fundamental a la protección de datos de carácter personal contenga una doble protección: por un lado, el derecho del ciudadano a preservar el control sobre éstos, y por otro, la aplicación de las nuevas tecnologías de la información (García González, 2007: 743-778).

El uso y la diversificación de las tareas que se vinculan con la *blockchain* es cada vez mayor. Esta situación dificulta establecer estándares para la protección de los datos personales que se manejan en ella. Algunos ejemplos de actividades que puede realizar son las siguientes:

En las criptomonedas, su función principal es transferir valor, evitando que una unidad de moneda digital se pueda gastar dos veces; lo hace registrando cada transacción una única vez y de forma inalterable. Muchas criptomonedas han desarrollado su propia *blockchain*, como *SolarCoin* y *Zcash*, pero otras prefieren confiar en la ya madura estructura de *bitcoin*, y se construyen con base en su plataforma, tal como los activos digitales de *Counterpart*.

En el caso de las transacciones y sistemas de pago, muchas empresas (en su mayoría bancos e instituciones financieras), dadas sus cualidades, como la velocidad, la seguridad y la privacidad, las han adoptado para construir sus propias plataformas que permitan reducir los costos de los pagos internacionales e interbancarios y ser más veloces.

En el registro de documentos, la *blockchain* permite que muchas partes puedan acceder desde cualquier lugar del mundo. Está siendo usada para registrar y verificar la autenticidad de toda clase de documentos: desde títulos universitarios y actas matrimoniales, hasta historiales médicos, área que por cierto ha tenido mucha atención, pues permitiría unir en una sola plataforma a hospitales, aseguradoras y prestamistas.

En la cadena de suministro resuelve la problemática de saber exactamente de dónde provienen las cosas, dado que con esta tecnología es posible marcar casi cualquier objeto con una huella digital única que seguirá todo su ciclo de vida desde el principio.

En lo relativo a los contratos inteligentes y aplicaciones descentralizadas, es capaz de crear la infraestructura adecuada para crear esos acuerdos digitales automatizados en los que se elimina la necesidad de confiar en terceras partes para su cumplimiento.

Se utiliza también en el mundo del entretenimiento, en el que varios videojuegos y juegos de azar se han construido sobre una cadena de bloques, o bien apoyándose en algún activo digital propio de ella.

Ahora bien, tomando en consideración las mencionadas tareas que pueden encomendarse a la *blockchain*, es indudable la pertinencia de diseñar un adecuado marco regulatorio de esta nueva tecnología en México. En ese sentido, y para enfatizar la importancia de una regulación efectiva, se remitirá a tres ejemplos que entrelazan figuras jurídicas del derecho civil, del derecho electoral, de la propiedad industrial y de la protección de datos personales en Europa, Asia y África.

El primero alude a una buena práctica de la Unión Europea, que consiste en promover iniciativas y foros institucionales en los que se difunde de manera constante la trascendencia social y jurídica de dicha tecnología. Lo anterior, debido al interés que despierta la digitalización del mercado único europeo, y con ello la posibilidad del uso de las criptomonedas y de herramientas (como el cómputo en la nube o el Internet de las cosas) en transacciones que generarán actos de comercio que tendrán que regularse de alguna manera.

Para el Parlamento Europeo, la cadena de bloques no es solamente una tecnología, sino también una infraestructura adecuada para simplificar



MANUEL GUSTAVO OCAMPO MUÑOA

las complejas transacciones financieras y comerciales, para el desarrollo de monedas virtuales que permiten la transferencia de valor (*Blockchain* 1.0) y también el marco ideal para el desarrollo de contratos inteligentes (*Blockchain* 2.0), que abren un amplio rango de posibilidades necesarias para la expansión del sector financiero, tanto respecto de la parte oferente como de la aceptante en las transacciones de ese tipo.

14 Es una tecnología de contabilidad distribuida que supone un cambio en las relaciones financieras, no sólo por las criptomonedas que la utilizan como base, sino por otros sectores relacionados con las finanzas, como el de los seguros, el legal, el de la propiedad y el de los contratos inteligentes, aunado a que todos en *blockchain* pueden ver y validar transacciones creando transparencia y confianza (Tolentino Morales, 2018).

El segundo ejemplo emerge de su creciente utilización en el área de la propiedad intelectual. La empresa china de telecomunicaciones y fabricación de teléfonos inteligentes *Huawei* pretende utilizar la tecnología *blockchain* para proteger esos derechos. En octubre de 2016 se asoció al consorcio de *Hyperledger*. Para enero de 2018, fue de las primeras en adoptar el *software Sawtooth*, que se encarga de crear productos para el análisis conjunto tradicional, así como para el análisis de elección discreta y otras formas de conjunto. Al implementarlo, busca que cuando las partes inicien solicitudes de descarga a través de la red de igual a igual, el sistema compare sus claves privadas o licencias para acceder al contenido con la información de verificación, y una vez que se llegue a un consenso, la cadena de bloques permitirá la descarga (Herrera, 2018).

Por último, un uso innovador es el que se le ha dado en materia electoral en Sierra Leona, en donde el 7 de marzo de 2018 se utilizó por primera vez en el mundo la *blockchain* para registrar el 70% del conteo de sus elecciones presidenciales. La empresa que ha desarrollado la tecnología se denomina *Agora*, y tiene su sede en Suiza; busca fundamentalmente reducir los costos de una votación recortando boletas de papel, así como reducir la corrupción en los comicios. Su sistema de votación digital usa una cadena de bloques privada para supervisar los resultados en tiempo real. Por ello, pudo publicar dos horas antes que la Comisión Nacional Electoral de la mencionada nación africana un recuento del 86% del total de la votación (Beamonte, 2018).

La tecnología *blockchain* permitió, entre otras cosas, recortar los costos de las boletas de papel, reducir la corrupción en el proceso de elección y obtener los resultados en tiempo real.

V. TEMAS ESPECÍFICOS DEL DERECHO A LA PROTECCIÓN DE DATOS
PERSONALES EN POSESIÓN DE LOS PARTICULARES QUE SE RELACIONAN
CON EL USO DE LA *BLOCKCHAIN*

El derecho a la protección de datos personales en posesión de los particulares incluye una temática que entrelaza lo jurídico con otras esferas del conocimiento relacionadas con el acceso a la información y las bases de datos. A continuación, de manera enunciativa, se describen algunos de los tópicos que la relacionan con la *blockchain*.

15

El primero, sin duda, son los denominados derechos ARCO. Se definen como el conjunto de acciones a través de las cuales una persona física puede ejercer el control sobre sus datos personales: acceso, rectificación, cancelación y oposición. Sólo pueden ser ejercidos por el titular de los datos, por su representante legal o por un representante acreditado. Se considera que el ejercicio de estos derechos se debe llevar a cabo mediante pasos medios sencillos y gratuitos puestos a disposición por el responsable del fichero y que están sujetos a plazo, por lo que resulta necesario establecer procedimientos adecuados para su satisfacción.

El derecho de acceso es el derecho del titular de los datos a obtener información sobre si sus propios datos están siendo objeto de tratamiento, la finalidad del tratamiento que (de ser el caso) se esté realizando, así como la información disponible sobre el origen de dichos datos y las comunicaciones realizadas o previstas de estos últimos.

El derecho de rectificación es el derecho del titular de los datos a que se modifiquen aquellos que resulten ser inexactos o incompletos. El derecho de cancelación es el derecho del titular a que se supriman esos datos que resulten ser inadecuados o excesivos (de aquí surge el llamado “derecho al olvido”). El derecho de oposición es el derecho del titular a que no se lleve a cabo el tratamiento de aquellos datos de carácter personal o se cese en el mismo en los supuestos en que no sea necesario su consentimiento para el tratamiento, que se trate de ficheros de prospección comerciales o que tengan la finalidad de adoptar decisiones referidas al interesado y basadas únicamente en el tratamiento automatizado de sus datos.

El segundo tema de interés son los principios y deberes de la protección de datos personales. Recio Gayo (2015: 5-65) considera que en materia de protección de datos personales, éstos cumplen con la labor de legitimar el tratamiento de los datos, y deben asegurarse a lo largo de su ciclo de vida, en todas y cada una de las fases de su tratamiento; es decir, desde que se obtienen o recaban (ya sea del propio interesado o no) hasta

MANUEL GUSTAVO OCAMPO MUÑOZA

que finalmente son destruidos, eliminados o borrados. De acuerdo con la LFPDPPP, son considerados como principios la licitud, el consentimiento, la información, la calidad, la finalidad, la lealtad, la proporcionalidad, y la responsabilidad; mientras que son considerados deberes la confidencialidad y la seguridad.

16 Otro concepto que vincula es el denominado “aviso de privacidad”, que es un documento generado por la persona física responsable de la recopilación y tratamiento adecuado de datos personales, y debe ser puesto a disposición del titular de los datos. Es el primer paso para cumplir con las obligaciones exigidas por la ley, y puede realizarse de forma electrónica. Debe ser formulado de manera sencilla, ser de fácil comprensión y debe incluir información clara y específica sobre los siguientes aspectos: ¿quién recopila los datos?; ¿qué datos recopila?; ¿con qué finalidad los recopila?; ¿cómo limitar su uso o divulgación?; ¿cómo revocar su uso?; ¿cuál es el procedimiento que tiene el titular para ejercer sus derechos de acceso, rectificación, corrección y oposición?; ¿en qué forma se comunican cambios al aviso de privacidad?; ¿en qué forma se comunican la aceptación o negativa para autorizar la transferencia de datos a terceros?, entre otros.

Las medidas compensatorias, entendidas como los mecanismos alternos para dar a conocer el aviso de privacidad a los titulares de los datos a través de medios de comunicación, constituyen otro elemento de estudio que une la *blockchain* con la protección de datos personales.

Su implementación es de manera excepcional cuando al responsable le resulta imposible poner a disposición de cada titular, de manera directa o personal, el aviso de privacidad, o ello exige esfuerzos desproporcionados. El aviso de privacidad divulgado a través de la medida compensatoria deberá contener, al menos, la identidad y el domicilio del responsable, las finalidades del tratamiento y los mecanismos que el responsable ofrece al titular para conocer el aviso de privacidad completo, de conformidad con lo dispuesto por la ley y su reglamento.

El responsable podrá publicar el citado aviso a través de diarios de circulación nacional, locales, o en revistas especializadas; página de Internet del responsable; hiperenlaces o hipervínculos situados en una página de Internet del Instituto Nacional de Acceso a la Información (INAI); carteles informativos; cápsulas informativas radiofónicas y otros medios alternos de comunicación masiva.

Finalmente, el tema de la autorregulación o autorreglamentación, que se refiere a la capacidad que tiene un sujeto, una institución, una organización o una asociación de regularse a sí misma bajo controles voluntarios, es uno de los más importantes para el desarrollo de la tecnología *blockchain*.

En los distintos ámbitos privados, la autorregulación se constituye como la potestad de establecer reglas por parte del cada sujeto dentro de su esfera de acción, estableciendo de manera voluntaria, normas deontológicas y códigos de autocontrol. En el sistema jurídico mexicano es una noción muy amplia, pues abarca, por ejemplo, ámbitos como el bursátil, el bancario, el profesional, el publicitario, el de la radiodifusión, el político, el económico, el tecnológico, entre otros (SE, 2015: 35-37).

17

VI. REFLEXIONES FINALES

El uso de las criptomonedas en México ha sido el primer contacto con la *blockchain* y los datos personales; actualmente se puede comprar en algunas tiendas con monedas virtuales; tal es el caso de locales de venta de pizzas, consultorios dentales y tiendas de conveniencia.

El 9 de marzo de 2018 se publicó en el *Diario Oficial de la Federación* la Ley para Regular las Instituciones de Tecnología Financiera. Dicho ordenamiento busca principalmente la supervisión de las criptomonedas para evitar el lavado de dinero o los fraudes. A partir de entonces se regulan los servicios financieros que prestan las referidas instituciones, así como su organización, operación y funcionamiento. Además, se pone especial énfasis en verificar los servicios financieros sujetos a alguna normatividad especial que sean ofrecidos o realizados por medios innovadores.

Al autorizarse la utilización de tecnología financiera, la responsabilidad central recae en el Banco de México, pues es la institución que vigila y autoriza los activos virtuales que pueden funcionar en el país, y por su parte los usuarios estarían obligados a comprobar que el dinero que se traslade a criptomoneda no tenga una procedencia ilícita.

Cabe aclarar que lo anterior no interfiere con la operación de la moneda, ya que el banco central no reconoce a los activos virtuales como monedas en curso legal, y tampoco respalda su valor, como sí lo hace con el peso. Sin embargo, el Estado se reserva el derecho de autorizar el uso de cualquiera de ellas y a clasificar las operaciones que se hacen como legales o ilegales.

Los usuarios, según la legislación, deben recibir información por parte de las empresas sobre la volatilidad de las criptomonedas, la irreversibilidad de las operaciones, los riesgos tecnológicos y cibernéticos, así como la posibilidad de la existencia de un fraude.

Ahora bien, dado que la tecnología de *blockchain* es una base de datos descentralizada sobre la que cualquier persona puede escribir y consultar

MANUEL GUSTAVO OCAMPO MUÑOZA

títulos, registros, certificaciones o archivos de una forma digital, pero que no se puede modificar ni falsificar, pretende eliminar la necesidad de instituciones y bases de datos centralizadas. Esto último puede abonar en el caso de México al tema del gobierno abierto.

18 En el caso de los contratos inteligentes, se generan nuevas formas y enfoques legales, como el arbitraje en caso de defectos de codificación, la responsabilidad legal de los programadores de dichos contratos o la necesidad de garantizar la validez y ejecutividad legal dentro de los sistemas nacionales, así como el cumplimiento de requisitos inexcusables, como los fiscales.

● Se deben establecer reglas claras para los denominados “contratos inteligentes”, pues no sólo se refieren a los típicos acuerdos comerciales entre partes y a las clásicas figuras, como el préstamo o los seguros, sino que también menciona la automatización de la sucesión y de la herencia, especialmente de la herencia digital.

● Crear una cadena de bloques accesible al público puede generar grandes beneficios para la administración pública. Los usuarios de diversos servicios, como los registros de la propiedad, licencias comerciales o certificados de nacimiento, tendrían una menor dependencia de abogados, notarios, funcionarios públicos o terceros.

● Deben diseñarse *blockchains* abiertos para temas de interés público (como los relacionados con la administración de las finanzas públicas, licitaciones o gestión de votos y los de carácter electoral) con distintos tipos de acceso; por ejemplo: uno para el gobierno federal, para los gobiernos estatales, locales, e incluso para vincularlos a los tres.

Un adecuado marco regulatorio de la cadena de bloques debe incluir exigencias relacionadas con la utilización de mecanismos de protección de datos personales de última generación en el caso de los particulares que los manejan; es decir, ciberseguridad para mantener registros automatizados, eficientes y sin fraudes, así como instrumentar políticas de autorregulación.

VII. FUENTES

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS, 2015, *Código de buenas prácticas en protección de datos para proyectos big data*, Madrid, AEPD.

BEAMONTE, Paloma, 2018, “Sierra Leona es el primer país que usa *blockchain* en unas elecciones”, *Hipertextual*, México, 15 de marzo, disponible en: <https://hipertextual.com/2018/03/sierra-leona-blockchain-elecciones> (fecha de consulta: 14 de diciembre de 2018).

Criptonoticias, 2017, “¿Qué es la tecnología de contabilidad distribuida o *blockchain*?”, *Criptonoticias.com*, México, disponible en: <https://www.criptonoticias.com/informacion/que-es-tecnologia-contabilidad-distribuida-blockchain/> (fecha de consulta: 14 de diciembre de 2018).

CASTILLO PORRAS, Gregorio y MONTERREY CHEPOV, Eugenio, 2011, *La protección de los datos personales. Retos de la protección de datos personales en el sector público*, México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del DF.

CERVERA NAVAS, Leonardo, 2003, *El modelo europeo de protección de datos de carácter personal*, Madrid, Cuadernos de Derecho Público.

CORONA, Sonia, 2018, “La fiebre del *bitcoin* aterriza en México”, *El País*, México, 29 de enero, disponible en: https://elpais.com/tecnologia/2018/01/27/actualidad/1517018747_329248.html (fecha de consulta: 14 de diciembre de 2018).

DÍAZ RUIZ, Jesús, 2017, “Encuesta sobre el uso de *blockchain* por parte de empresas y *startups*”, *Cloud Computing*, España, disponible en: <https://www.revistacloudcomputing.com/2017/11/sngular-da-a-conocer-los-resultados-de-su-observatorio-de-blockchain/> (fecha de consulta: 14 de diciembre de 2018).

GARCÍA GONZÁLEZ, Aristeo, 2007, “La protección de datos personales: derecho fundamental del siglo XXI. Un estudio comparado”, *Boletín Mexicano de Derecho Comparado*, México, núm. 120.

HERRERA, Carlos, 2018, “Huawei solicita patente de *blockchain* para manejar derechos de propiedad intelectual”, *Coincrispy*, México, disponible en: <https://www.coincrispy.com/2018/03/07/huawei-solicita-patente-blockchain/> (fecha de consulta: 14 de diciembre de 2018).

LA NACIÓN, 2017, “¿Quién es el dueño del *blockchain*?”, *Economist Newspaper Ltd.*, México, disponible en: <https://www.lanacion.com.py/2017/01/15/quien-dueno-del-blockchain/> (fecha de consulta: 14 de diciembre de 2018).

MARTÍNEZ, Ricardo, 2007, “El derecho fundamental a la protección de datos. Perspectivas”, *Revista de los Estudios de Derecho y Ciencia Política de la UOC, Monográfico III congreso internet, derecho y política (IDP). Nuevas perspectivas*, Barcelona, núm. 5.

MILLÁN GÓMEZ, Agustín, 2011, “Reconocimiento normativo del derecho a la protección de datos personales en el ámbito internacional”, *Retos de la protección de datos personales en el sector público*, México, Instituto de Acceso a la Información Pública y Protección de Datos Personales del D. F.



MANUEL GUSTAVO OCAMPO MUÑOZA

- PARLAMENTO EUROPEO, 2016, *Noticias del Parlamento Europeo*, 14 de abril, disponible en: <http://www.europarl.europa.eu/news/es/press-room/20160407IPR21776/reforma-de-la-proteccion-de-datos-nuevas-reglas-adaptadas-a-la-era-digital>.
- RECIO GAYO, Miguel, 2015, *Principios y deberes en materia de protección de datos personales*, México, INAI.
- 20 SECRETARÍA DE ECONOMÍA, 2015, *Prosof 2.0. Estudio de autorregulación en materia de privacidad y protección de datos personales en el ámbito de las TI. 5a. Entrega: versión final*, México, SE.
- STEWART, David P., 2014, “Privacidad y protección de datos”, 84o. *Periodo Ordinario de Sesiones OEA*, Río de Janeiro, OEA.
 -
 -
- TOLENTINO MORALES, Juan, 2018, “¿Una nación *blockchain*? Esto es lo que el gobierno mexicano tiene entre manos”, *The Huffington Post México*, México, disponible en: https://www.huffingtonpost.com.mx/2018/01/11/una-nacion-blockchain-esto-es-lo-que-el-gobierno-mexicano-tiene-entre-manos_a_23330182/ (fecha de consulta: 14 de diciembre de 2018).
- VELÁZQUEZ, Karina, 2018, “*Blockchain* y su futuro en las empresas en 2018”, *M4rketiing Ecommerce*, México, disponible en: <https://marketing4ecommerce.mx/blockchain-y-su-futuro-en-las-empresas-en-2018/> (fecha de consulta: 14 de diciembre de 2018).

Marco jurídico

- Declaración Universal de los Derechos Humanos, disponible en: <https://www.un.org/es/universal-declaration-human-rights/>.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.
- Ley General del Sistema Nacional Anticorrupción (LGSNA), disponible en: <http://www.diputados.gob.mx/LeyesBiblio/pdf/LGSNA.pdf>.

**BIG DATA, BIG DATA ANALYTICS Y DATOS
PERSONALES EN LOS TIEMPOS DEL INTERNET:
DE LA AUTORREGULACIÓN ESTADOUNIDENSE
AL REGLAMENTO GENERAL DE PROTECCIÓN
DE DATOS DE LA UNIÓN EUROPEA**

*BIG DATA, BIG DATA ANALYTICS AND PERSONAL
DATA IN THE INTERNET ERA: FROM THE AMERICAN
AUTOREGULATION TO THE EUROPEAN UNION GENERAL
REGULATION OF DATA PROTECTION*



*Mauricio Augusto CALCANEÓ MONTS**

RESUMEN: El artículo expone y explica las implicaciones derivadas del surgimiento y uso cada vez más extendido del internet, en términos de los datos personales de sus usuarios. En particular, se aborda lo relativo al impacto que tiene el *big data* o la existencia de grandes volúmenes de datos personales obtenidos a partir de los registros electrónicos, así como el procesamiento y análisis de dichos datos mediante el *big data analytics*. Para ello, se analizan los modelos regulatorios que existen sobre la materia en Estados Unidos y la Unión Europea, concluyéndose sobre la inviabilidad de la autorregulación norteamericana y la necesidad de enfoques más amplios, como el europeo.

PALABRAS CLAVE: Internet, *big data*, *big data analytics*, datos personales, regulación.

* Licenciado en derecho por la UNAM, licenciado en economía por la UAM-Xochimilco, maestro en derecho administrativo y regulación por el ITAM, y candidato a doctor por el Posgrado en Ciencias Políticas y Sociales de la UNAM. Correo: calcaneomonts@yahoo.com.

Fecha de recepción: 6 de junio de 2018.

Fecha de dictamen: 16 de marzo de 2019.

MAURICIO AUGUSTO CALCANELO MONTS

22

ABSTRACT: The article exposes and explains the implications derived from the rise and increasingly widespread use of the internet, in terms of the personal data of its users. In particular, it deals with regard with the impact that big data has or the existence of large volumes of personal data obtained from electronic records, as well as the processing and analysis of such personal data through the big data analytics. In this regard, the regulatory models that exist in United States and in the European Union on the matter are analyzed, concluding on the unfeasibility of the American auto-regulation and the need for broader approaches as the European one.



KEY WORDS: Internet, big data, big data analytics, personal data, regulation.

I. INTRODUCCIÓN

El Internet conecta a miles de millones de seres humanos prácticamente a todo lo largo y ancho del orbe, eliminando así las barreras espaciales y temporales existentes con antelación. Es, sin duda alguna, un cambio de gran calado en el ámbito tecnológico y de las comunicaciones, con hondas repercusiones sobre la forma en que los seres humanos interactúan y se comunican.

El éxito del Internet está sustentado en el tipo de comunicación que alberga, que es llevada a cabo en forma instantánea y de manera impersonal o indirecta a través de dispositivos electrónicos. Es gracias a esta mediación electrónica que se cuenta con registros en tiempo real de prácticamente la totalidad de las actividades efectuadas por los usuarios del Internet (Varian, 2010).

Es una cantidad ingente de información sobre los más diversos movimientos de todos y cada uno de los usuarios del Internet (*big data*), que ha sido posibilitada por el desarrollo acelerado y el consiguiente abatimiento de los costos de las tecnologías y técnicas atinentes a la recolección, almacenamiento y procesamiento de dicha información, lo que se ha visto acompañado por importantes progresos en las capacidades tecnológicas, técnicas y humanas para el análisis de la información (*big data analytics*) (Cate, 2014; Einav y Levin, 2013; White House, 2014a y 2014b; Federal Trade Commission, 2014).

Es decir, si bien el Internet ha hecho realidad una mayor y mejor comunicación entre individuos, al mismo tiempo, por su propia naturaleza

electrónica, ha permitido, por vez primera en la historia de la humanidad, la existencia de enormes volúmenes de información a un nivel de detalle sin precedentes sobre las actividades de sus usuarios, lo que, desde luego, no ha estado exento de una serie de cuestionamientos relacionados con la cantidad de información extraída, su contenido, la privacidad, y el uso que se está haciendo de esta información con propósitos analíticos y predictivos en los más distintos ámbitos de la actividad social (Kosinski y Behrend, 2017; Tucker *et al.*, 2017; Altman *et al.*, 2018; Tucker *et al.*, 2018).

23

Son dos los modelos regulatorios diametralmente opuestos en el ámbito de las democracias occidentales sobre los datos personales en el Internet: uno, el norteamericano, que es el más ampliamente extendido hasta ahora, y que se sustenta en la autorregulación de las empresas; el otro, el europeo, que reconoce una serie de derechos que protegen ampliamente los datos personales de los usuarios europeos del Internet, y que pone límites claros al actuar de las empresas (Wheeler, 2018), que pueden ser explicados con base en las diferencias culturales, políticas y jurídicas de ambos lados del Atlántico; la europea, más proclive a la intervención estatal, y la norteamericana, más cimentada en la libertad individual (Fukuyama, 2018).

El texto tiene como objetivo exponer y explicar la situación de los datos personales en los tiempos del Internet, los desafíos que esto implica y las medidas que en materia regulatoria se han tomado tanto en Estados Unidos como en Europa. En primer término, se aborda lo relacionado con el cúmulo de información disponible a partir del surgimiento y uso cada vez más extendido del Internet (*big data*), para después entrar al detalle de los avances técnicos y tecnológicos para el análisis de tales datos y su aplicación con fines explicativos, predictivos, e inclusive de manipulación (*big data analytics*). En segundo lugar, se revisan a la luz del marco analítico que proporcionan el *big data* y el *big data analytics*, los marcos regulatorios de los Estados Unidos y la Unión Europea relacionados con los datos personales en el Internet. El contraste es muy marcado, pues mientras en el primer caso, Estados Unidos, prevalece un esquema de autorregulación empresarial, en Europa, por el contrario, hay un reconocimiento de los derechos de los titulares de los datos personales y una fuerte regulación estatal sobre qué se puede recolectar, y sobre todo, qué se puede hacer con ellos. Se concluye que la regulación europea es, desde esta perspectiva, la respuesta más acorde a los desafíos que implican el *big data*, el *big data analytics* y los datos personales en los tiempos del Internet.

MAURICIO AUGUSTO CALCANELO MONTS

II. *BIG DATA*, *BIG DATA ANALYTICS* Y DATOS PERSONALES

24 Conceptualmente, el *big data* se refiere a la existencia de una ingente cantidad de datos asociados al uso cada vez más extendido del Internet y los dispositivos electrónicos vinculados a éste, tales como las computadoras, los teléfonos celulares, las aplicaciones para dispositivos móviles, los geolocalizadores, los sensores, y otros (Cate, 2014).

● Sobre la ingente cantidad de datos disponibles, baste destacar que
○ para 1999 se hablaba de una producción anual de nueva información de
● aproximadamente dos exabytes;¹ para 2002, dicha cantidad se había incrementado a cinco exabytes anuales correspondientes una tasa de crecimiento anual del 30% (Lyman y Varian, 2003), mientras que para 2013 se calculaba que se generaban los mismos cinco exabytes de información, pero cada dieciocho días (Einav y Levin, 2013). De forma que en 2013 se estimaba en cuatro zettabytes² el tamaño de la información generada.

No sólo es un enorme volumen de información disponible, sin parangón en la historia de la humanidad, sino que además se caracteriza por la velocidad en que puede ser obtenida, alcanzando incluso el tiempo real, por no hablar de su gran variedad al abarcar los más distintos aspectos de la actividad humana y a niveles de detalle nunca antes vistos. Como afirman Einav y Levin (2013: 2 y 3):

Prácticamente en internet todo es registrado. Cuando haces una búsqueda en Google o Bing, tus preguntas y subsecuentes acciones son registradas. Cuando compras en Amazon o eBay, no sólo cada compra, sino tus siguientes acciones son capturadas y registradas. Cuando lees un periódico en línea, ves videos, o revisas tus finanzas personales, todo tu comportamiento es registrado. El registro del comportamiento individual no se limita al internet: los mensajes de texto, los teléfonos celulares y la geo-localización, los datos escaneados, los datos laborales, y los datos electrónicos de salud, todos son parte de una huella de datos que vamos dejando.

La Comisión Federal de Comercio de los Estados Unidos, por ejemplo, investigó el actuar de los llamados *data brokers*, o las “empresas que recolectan información personal de los consumidores y la revenden o comparten con otras compañías” (Federal Trade Commission, 2014). Los ha-

¹ Un exabyte (EB) es equivalente a 1,000,000,000,000,000,000 bytes o 1018 bytes. Un byte es igual a un carácter de texto.

² Un zettabyte es igual a 1,000,000,000,000,000,000,000 bytes o 1021 bytes.

llazgos son reveladores con relación al tipo de información que se extrae, la forma en que se consigue y los usos que se le dan:

1) La información es obtenida vía internet y medios electrónicos asociados a éste, sin que los consumidores conozcan lo más mínimo sobre la existencia y operación de estas empresas, qué información recolectan ni cómo la procesan y usan.

2) La información de los consumidores con la que cuentan los *data brokers*, incluso indefinidamente, incluye nombres, direcciones, edad y registros de transacciones.

3) Los *data brokers* combinan estos datos para efectos de análisis y la realización de una serie de inferencias sobre los hábitos, gustos y demás aspectos relativos a los consumidores.

4) La información personal sobre los consumidores permite dar seguimiento puntual a cada uno de los mismos y es usada en una amplia variedad de industrias con tres fines principales: la publicidad personalizada en línea, la mitigación de riesgos y la búsqueda de productos.

25



Es un conjunto de información personal, profunda y vasta sobre quienes usan el Internet, que es obtenida y almacenada a partir de las posibilidades que brindan los desarrollos tecnológicos-computacionales, que han abatido los costos asociados a estas operaciones; que están en posesión de entes tales como los proveedores de servicios de telecomunicaciones, las redes sociales, las tiendas en línea, las empresas de telefonía celular, los bancos, los *data brokers*, los navegadores de Internet, los buscadores de información en Internet, y otros; y de la que se desconoce, en la gran mayoría de los casos, inclusive su propia existencia, por no hablar de su contenido preciso por parte de quienes son sus legítimos titulares (White House, 2014a y 2014b). Todo lo cual conlleva serias interrogantes en términos de la privacidad de los individuos y los datos personales de los usuarios del Internet.

La situación se torna todavía más crítica cuando se abordan los usos que se dan a esta información vía el *big data analytics* o, lo que es lo mismo, mediante el procesamiento y análisis del gran cúmulo de información disponible por medios electrónicos.

Si el *big data* se refiere a la gran cantidad de información de los individuos que se recopila, almacena y procesa a partir de la actividad de aquellos en el Internet, el *big data analytics* trata del análisis de tal información para detectar patrones de comportamiento, los que son utilizados con fines predictivos, e incluso de modificación de los mismos (White House, 2014b).

MAURICIO AUGUSTO CALCANELO MONTS

El *big data analytics* implica un gran salto cualitativo en términos de las capacidades tecnológicas, técnicas y humanas para trabajar y manipular ese enorme cúmulo de información conseguida a través de Internet, con el fin de obtener un orden, encontrar variables, patrones y relaciones, y no sólo eso, sino también poder anticipar comportamientos, e inclusive influir y moldear éstos en las más distintas esferas de la actividad humana (desde el simple acto de comprar un producto en Internet hasta hechos relacionados con elecciones de tipo político).

26

A través del *big data analytics* se crean modelos de comportamiento de los individuos, se realizan experimentos en tiempo real y se personaliza lo que ven y hacen en el Internet con base en su comportamiento previo (Varian, 2010).

La evidencia empírica sobre el *big data analytics* ha confirmado plenamente las múltiples posibilidades de su aplicación. Por ejemplo, en el contexto político se ha comprobado su utilidad lo mismo para movilizar votantes que para extraer información sobre las cualidades personales de los usuarios de Internet.

En un experimento realizado con motivo de las elecciones legislativas norteamericanas del 2 de noviembre de 2010, se incluyeron una serie de mensajes en Facebook para analizar si afectaban la autoexpresión política, la búsqueda de información y la emisión del voto. Los resultados son positivos para los tres efectos buscados; la movilización política en línea sí funciona para la inducción de estos tres tipos de conductas. Más importante todavía, la publicidad en Internet tiene influencia en los comportamientos de los individuos en la vida real (Bond *et al.*, 2012).

De igual manera, se comprobó que los “me gusta” en Facebook pueden servir para predecir con gran exactitud una serie de atributos personales de sus usuarios, como son las preferencias sexuales, el grupo étnico, la religión que se practica, los rasgos personales, la inteligencia, la felicidad, el uso de sustancias adictivas, la edad, el género, la separación de los papás y las preferencias políticas (Kosinski *et al.*, 2013).

La situación resultante es clara: un contado número de personas, empresas y gobiernos detentan la información y los conocimientos atinentes para acceder a profundidad, en forma detallada y en tiempo real, a las más variadas actividades de los individuos, para a través de esto predecir sus comportamientos, y, sobre todo, estar en aptitud de ejercer sobre ellos cierto tipo de influencia (White House, 2014). Es un poder sinigual en la historia del hombre, que se puede prestar a usos socialmente incorrectos, como lo es la manipulación de todo tipo, y que está cimentado en los datos personales de sujetos que en su mayoría desconocen dichos procesos.

La experiencia de la elección presidencial norteamericana de 2016 es reveladora a este respecto:

Está ampliamente documentada y probada la intervención de Rusia en las elecciones presidenciales norteamericanas por conducto de las redes sociales, utilizando publicidad pagada, con alto contenido ideológico y cultural, y dirigida a sujetos con ciertas características particulares, que los hacían propensos a estos temas divisivos (Freedom House, 2017; Persily, 2017; Tucker *et al.*, 2017).

27

Los gigantes del Internet, como Facebook, Google y Twitter, han rendido testimonio sobre el tema ante los comités de las cámaras de senadores y de representantes de los Estados Unidos, e incluso ante los parlamentos europeo y británico. Facebook, por ejemplo, aceptó que más de 126 millones de personas fueron alcanzadas por la publicidad contratada por la denominada Agencia de Investigación de Internet, de origen ruso. Twitter informó que identificaron 3,814 cuentas vinculadas con la misma agencia, las que emitieron 175 mil “tuits”, que significaron el 8.4% de los mensajes relacionados con la campaña presidencial norteamericana. La investigación periodística “Expedientes de *Cambridge Analytica*” documentó la sustracción, por parte de la empresa SCL Group/SCLElections/Cambridge Analytica, de los datos personales de las cuentas de Facebook de 87 millones de usuarios, en su mayoría estadounidenses, con el fin de crear perfiles psicológicos y políticos de los 230 millones de norteamericanos para su uso en la campaña presidencial de 2016, mediante diversas operaciones, que incluyeron rumores, desinformación y noticias falsas. Como consecuencia, el Departamento de Justicia estadounidense acusó formalmente a trece personas y tres compañías por el diseño de una red para subvertir las elecciones presidenciales de 2016, promover la discordia, socavar el respaldo público a la democracia y apoyar al ahora presidente de Estados Unidos.

Las redes sociales han ocupado un lugar privilegiado en la diseminación de información falsa, discursos de odio, interferencia electoral, propaganda extremista y con alto contenido conspirativo, que tiende a la polarización, entre otros. Como afirma Larry Diamond (2019), en un muy corto periodo de tiempo se pasó de una visión optimista de las redes sociales, como herramientas de la libertad de expresión y para el combate contra los gobiernos autoritarios, a otra francamente pesimista, por los efectos adversos que tiene en el funcionamiento de la democracia.

Frente a esta situación, son múltiples los llamados en Estados Unidos y alrededor del mundo para revisar y modificar el modelo de regulación imperante en materia de datos personales obtenidos en el Internet (Goldfarb y Tucker, 2011; Kosinski y Behrend, 2017; Altman *et al.*, 2018). Inclusive

MAURICIO AUGUSTO CALCANELO MONTS

Mark Zuckerberg, fundador y director ejecutivo de Facebook, se ha pronunciado recientemente en favor de cambiar la regulación norteamericana en la materia y transitar hacia un esquema similar al de la Unión Europea (Zuckerberg, 2019). En seguida, se exponen los pormenores del modelo de regulación norteamericano de datos personales hasta ahora vigente, para después proceder a contrastarlo con el de Europa.

28

III. LA REGULACIÓN NORTEAMERICANA DE DATOS PERSONALES EN INTERNET

●
○
● La regulación norteamericana sobre privacidad, datos personales y tecnologías de la información y comunicación se remonta por lo menos a fines del siglo XVIII, cuando se declaró ilegal la apertura de la correspondencia postal (1782). Desde entonces y hasta ahora se reconoce ampliamente la constante y cambiante relación y tensión que existe entre cambio tecnológico en el mundo de las telecomunicaciones y la vida privada de los individuos (Goldfarb y Tucker, 2011).

El primer antecedente se encuentra en la cuarta enmienda de la Declaración de Derechos de 1791, que protege básicamente los derechos a la privacidad y a no sufrir una invasión arbitraria, al establecer el

derecho del pueblo a la seguridad de sus personas, hogares, documentos y pertenencias frente a allanamientos y registros arbitrarios será inviolable, y no se expedirá ningún mandamiento, sino en virtud de causa probable, apoyado en juramento o promesa, que describa el lugar que ha de ser registrado y las personas o cosas que han de ser detenidas o incautadas.

Sin embargo, es ampliamente reconocido que no fue hasta un siglo después, en 1890, con la publicación del artículo seminal “El derecho a la privacidad”, de Warren y Brandeis, si bien referido al impacto negativo de las cámaras portátiles y las fotos en la privacidad de las personas, cuando se emprendieron los primeros pasos para incluir el aspecto electrónico en el derecho a la privacidad, cuando también se dio a luz al derecho a la privacidad entre las personas y con respecto al gobierno, y se pusieron los fundamentos para la responsabilidad civil por los daños ocasionados.

Posteriormente, hay una serie de desarrollos en el ámbito jurisdiccional, como lo es la opinión disidente de 1928 del juez de la Suprema Corte, Louis Brandeis, en el caso *Olmstead* contra los Estados Unidos, en el que se proclamó el derecho a estar solo contra la intervención del gobierno, lo que fue interpretado de la manera más amplia y abarcadora posible. En

1939, el tratado de jurisprudencia de expresión de agravios reconoció la invasión a la privacidad como base para el derecho de acción. Y en 1967, una nueva interpretación de la Corte Suprema en el caso Katz contra Estados Unidos estableció que las expectativas subjetivas de privacidad están protegidas cuando se consideran razonables.

Fue en las décadas de los setenta y ochenta del siglo pasado, con el surgimiento de las computadoras y de las grandes bases de datos, cuando se construyó en Estados Unidos el andamiaje jurídico vigente hasta la actualidad, sobre manejo de datos personales en ciertos sectores económicos y en las plataformas tecnológicas a ellos asociadas.

En 1970 se emitió la primera de las regulaciones sectoriales, la Ley de Información de Crédito Justo (Fair Credit Reporting Act o FCRA, por sus siglas en inglés), cuyo objetivo es, de conformidad con el apartado b) del artículo 602,

exigir que las agencias de informes de consumidores adopten procedimientos razonables para satisfacer las necesidades de comercio de crédito al consumidor, personal, seguros y otra información de manera justa y equitativa para el consumidor, con respecto a la confidencialidad, exactitud, relevancia y uso adecuado de dicha información.

El año de 1973 fue crucial para los desarrollos futuros en materia de protección de la información de las personas en un entorno caracterizado por el uso cada vez más extensivo de las computadoras y los sistemas de registros vinculados a éstas. Es en tal año cuando, en un influyente reporte intitulado “Registros, Computadoras y los Derechos de los Ciudadanos” (*Records, Computers and the Rights of Citizens*), elaborado a instancias del Departamento de Salud, Educación y Bienestar, se enuncian los cinco Principios Prácticos de Información Justa (*Fair Information Practice Principles* o simplemente FIPPS, por sus siglas en inglés), y que se transcriben a continuación (Ohm, 2014: 97):

1. No debe haber sistemas de registro y posesión de datos personales cuya existencia sea secreta.
2. Debe haber una forma para que la persona sepa qué información sobre ella es registrada y cómo es usada.
3. Debe haber una manera para que la persona prevenga que la información obtenida sobre ella con un propósito sea usada o esté disponible para otros propósitos sin el consentimiento de la misma persona.



MAURICIO AUGUSTO CALCANELO MONTS

4. Debe haber una manera para que una persona corrija o enmiende un registro de información acerca de ella.
5. La organización que genere, mantenga, use o propague registros identificables de datos personales debe asegurarse de la confiabilidad de los datos para el uso intentado, y debe tomar precauciones para prevenir usos inadecuados.

30 Son cinco principios concisos sobre la recopilación y uso de los datos personales en el amanecer de los tiempos de las computadoras, que, como se desprende de su lectura, implican que no debían existir sistemas secretos de registro y posesión de datos personales; posibilitan a las personas conocer cómo y para qué se usa su información; desautorizan el uso de la información para objetivos distintos a los que se plantearon al momento de su recolección; permiten la corrección o enmienda de los datos de las personas, y enuncian obligaciones de confiabilidad y prevención para las organizaciones que trabajen con estos datos.

Los cinco principios, no obstante, adolecieron de obligatoriedad, por lo que “en la práctica, con excepción de unos pocos sectores, como el del cuidado a la salud, el enfoque de los FIPPs en los Estados Unidos ha sido reducido a los procedimientos para asegurar el aviso y consentimiento” (Strandburg, 2014: 10). Su aplicación quedó entonces a merced de la autorregulación de los sectores económicos, lo que ha desembocado en un procedimiento de aviso, en la mayoría de los casos ininteligible, por parte de las empresas para recolección, almacenaje y procesamiento de los datos personales de los usuarios, y a un consentimiento de éstos bastante desinformado y limitado con relación a los datos que se recolectan y los usos que se darán éstas (White House, 2012; White House, 2014a y 2014b; Cate, 2014; Strandburg, 2014; Ohm, 2014).

Es posterior a los cinco Principios Prácticos de Información Justa que se emiten toda una serie de legislaciones, principalmente sectoriales, en materia de datos personales. En diciembre de 1974 se expidió la Ley de Privacidad (Privacy Act of 1974), con el fin de establecer restricciones y salvaguardas contra la invasión de la privacidad personal a través del uso indebido de datos y registros por parte de las agencias federales. La Ley define el término “registro” como

cualquier artículo, recopilación o agrupación de información sobre un individuo que es mantenido por una agencia, incluyendo, pero no limitado a, su educación, transacciones financieras, historial médico y criminal o historial de empleo. Mientras que, en el apartado de condiciones de divulgación, se establece que “ninguna agencia divulgará registro alguno que esté contenido

en un sistema de registros, por ningún medio de comunicación, a ninguna persona u otra agencia, excepto en virtud de una solicitud por escrito o con el consentimiento previo por escrito de la persona a quien el registro pertenece”.

En el mismo 1974 se emitió la Ley de Privacidad y Derechos Educativos de la Familia (Family Educational Rights and Privacy Act o FERPA, por sus siglas en inglés), que regula la información personal relacionada con las escuelas, en específico los registros de los estudiantes; ya en la década de los noventa, en 1996, tocó el turno a la Ley de Responsabilidad y Portabilidad del Seguro de Salud (Health Insurance Portability and Accountability Act o HPAA, por sus siglas en inglés), que regula la información atinente a la industria de la salud; en 1998, entró en vigor la Ley de Protección de la Privacidad en Línea de los Niños (The Children’s Online Privacy Protection Act o COPPA), que obliga a obtener el consentimiento de los padres para el caso de los servicios en línea dirigidos a los menores de trece años o que colectan datos de éstos; en 1999 se emitió la Ley Gramm-Leach-Bliley, que ordena a las instituciones financieras, respetar la privacidad, la seguridad y la confidencialidad de sus clientes.

Se trata de una serie de regulaciones que se caracterizan por (White House, 2014a y 2014b; Cate, 2014; Strandburg, 2014; Ohm, 2014):

1. Su enfoque eminentemente sectorial, que abarca de manera transversal al Internet en su conjunto, al ocuparse de sectores particulares, como son los de la salud, el crediticio y otros.
2. Sustentarse en el aviso y consentimiento como mecanismo para obtener el visto bueno de los usuarios para la recolección y procesamiento de sus datos, lo que conlleva problemáticas tales como la falta de capacidades de los usuarios para leer y asimilar los alcances e implicaciones de su consentimiento; la posibilidad de almacenar y usar la información obtenida por largos periodos de tiempo, e inclusive de manera indefinida, y el uso de la información con los más diversos fines y alcances.
3. Concentrarse en la recolección y revelación de la información más que en el uso que se dé a ésta, lo que conlleva a una situación en la que pretendidamente hay ciertos límites a lo que se puede recopilar y hacer público, y plena libertad en cuanto a cómo se utiliza dicha información, y
4. Todo lo cual da un amplio margen de autorregulación a las empresas que recolectan y procesan datos personales de los individuos en el Internet.



MAURICIO AUGUSTO CALCANELO MONTS

Ante los retos que implican el *big data* y el *big data analytics* en términos de recolección y análisis del ingente y cada vez más detallado y preciso volumen de datos personales de los millones de usuarios del Internet, es patente que a estas alturas es insuficiente el modelo norteamericano de autorregulación sectorial de datos personales en el Internet.

32 A la fecha, son varios los intentos para que Estados Unidos cuente con una legislación transversal en materia de datos personales en el Internet: la propuesta de Ley de Derechos de Privacidad del Consumidor del presidente Obama de 2012; el llamado de 2014 de la Comisión Federal de Comercio para regular a los *data brokers*, y la regulación de “Protección de la Privacidad de los Clientes de Banda Ancha y Otros Servicios de Telecomunicaciones” de la Comisión Federal de Comunicaciones, que fue rechazada el 3 de abril de 2017 por una declaración conjunta del Congreso estadounidense (Ley Pública 115-22).

A nivel de los estados de la Unión Americana resalta el caso de California, donde se aprobó, el 25 de junio de 2018, la Ley de Privacidad del Consumidor, en vigor a partir del 1o. de enero de 2020. La que señala en el inciso g) de la sección 2, que “en marzo de 2018, salió a la luz que los datos personales de millones de personas habían sido mal utilizados por una empresa de extracción de datos llamada *Cambridge Analytica*... Como resultado, se ha fortalecido nuestro deseo de privacidad y transparencia en las prácticas asociadas a los datos...”.

Por lo que la Ley de Privacidad otorga a los individuos el control sobre sus datos personales, mediante los siguientes derechos: saber qué información se está recolectando sobre ellos; si su información está siendo vendida o hecha pública, y a quién; tener acceso a su información, y negarse a que su información sea vendida.

Aparentemente, ni a la opinión pública ni a los tomadores de decisiones estadounidenses les basta ya con el modelo de autorregulación imperante de datos personales en el Internet. Existe lo que figura ser una fuerte corriente de opinión sobre la necesidad de regular el manejo de datos personales en Estados Unidos, aunque es difícil prever si esto llevará a un acuerdo sobre el tema y cuál será su contenido. Por ello, cobra especial relevancia lo que se está realizando en la Unión Europea mediante el Reglamento General de Protección Datos, cuestión que se aborda en el apartado siguiente.

IV. EL REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS DE LA UNIÓN EUROPEA

En contraposición al modelo estadounidense de autorregulación sectorial de datos personales en el Internet, la Unión Europea cuenta desde el 25 de mayo de 2018 con el Reglamento General de Protección Datos, conforme al cual la privacidad es concebida como un derecho humano fundamental, por lo que se otorga una vigorosa protección en favor de los titulares de los datos personales, y ahora se está en presencia de una regulación transversal respaldada por una fuerte intervención estatal.

33

El caso europeo, al igual que el norteamericano, tiene una serie de antecedentes de larga data. El primero de ellos es el Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales del Consejo de Europa de 1950, cuyo artículo 8 establece el derecho a la privacidad, al señalar que “toda persona tiene derecho al respeto de su vida privada y familiar, de su domicilio y de su correspondencia”.

No obstante, los primeros años de la década de los ochenta fueron cruciales en materia de protección de datos personales en el contexto de la expansión de las comunicaciones electrónicas, con la emisión de dos documentos con profundo impacto a futuro: las Directrices de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre Protección de la Privacidad y Flujos Transfronterizos de Datos Personales de 1980, y el Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter Personal de 1981.

Las Directrices de la OCDE de 1980 planteaban en su segunda parte ocho principios básicos de aplicación nacional, que a la letra señalan:

Principio de limitación de recogida: Deberán existir límites para la recogida de datos personales y cualquiera de estos datos deberán obtenerse con medios legales y justos y, siempre que sea apropiado, con el conocimiento o consentimiento del sujeto implicado.

Principio de calidad de los datos: Los datos personales deberán ser relevantes para el propósito de su uso y, en la medida de lo necesario para dicho propósito, exactos, completos y actuales.

Principio de especificación del propósito: El propósito de la recogida de datos se deberá especificar a más tardar en el momento en que se produce dicha recogida, y su uso se verá limitado al cumplimiento de los objetivos u otros que no sean incompatibles con el propósito original, especificando en cada momento el cambio de objetivo.

MAURICIO AUGUSTO CALCANELO MONTS

Principio de limitación de uso: No se deberá divulgar, poner a disposición o usar los datos personales para propósitos que no cumplan lo expuesto en el apartado 9, excepto si se tiene el consentimiento del sujeto implicado o por imposición legal o de las autoridades.

Principio de salvaguardia de la seguridad: Se emplearán salvaguardias razonables de seguridad para proteger los datos personales contra riesgos, tales como pérdida, acceso no autorizado, destrucción, uso, modificación o divulgación de los mismos.

34

Principio de transparencia: Deberá existir una política general sobre transparencia en cuanto a evolución, prácticas y políticas relativas a datos personales. Se deberá contar con medios ágiles para determinar la existencia y la naturaleza de datos personales, el propósito principal para su uso y la identidad y lugar de residencia habitual de quien controla esos datos.

-
-
-

Principio de participación individual: Todo individuo tendrá derecho a: que el controlador de datos u otra fuente le confirme que tiene datos sobre su persona; que se le comuniquen los datos relativos a su persona en un tiempo razonable; a un precio, si existiese, que no sea excesivo; de forma razonable; y de manera inteligible; que se le expliquen las razones por las que una petición suya según los subapartados (a) y (b) haya sido denegada, así como poder cuestionar tal denegación; y expresar dudas sobre los datos relativos a su persona y, si su reclamación tiene éxito, conseguir que sus datos se eliminen, rectifiquen, completen o corrijan.

Principio de responsabilidad: Sobre todo controlador de datos debe recaer la responsabilidad del cumplimiento de las medidas que hagan efectivos los principios señalados anteriormente.

Las Directrices de la OCDE de 1980 no tenían fuerza obligatoria y vinculante para los Estados. No obstante, fueron incluidos como parte sustantiva del Convenio 108 del Consejo de Europa, cuyo fin, según su artículo 1, es “garantizar... a cualquier persona física... 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...”. En los artículos 5 y 8 del Convenio se estableció lo que sigue:

Artículo 5. Calidad de los datos.

Los datos de carácter personal que sean objeto de un tratamiento automatizado: a) Se obtendrán y tratarán leal y legalmente; b) Se registrarán para finalidades determinadas y legítimas, y no se utilizarán de una forma incompatible con dichas finalidades; c) Serán adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se haya registrado; d) Serán exactos y si fuera necesario puestos al día; e) Se conservarán bajo una forma que permita la identificación de las personas concernidas durante

el período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.

Artículo 8. Garantías complementarias para la persona concernida

Cualquier persona deberá poder: a) Conocer la existencia de un fichero automatizado de datos de carácter personal, sus finalidades... así como la identidad y residencia... de la autoridad controladora del fichero; b) Obtener... la confirmación de la existencia o no en el fichero automatizado de datos de carácter personal que conciernen a dicha persona, así como la comunicación de dichos datos en forma inteligible; c) Obtener... la rectificación de dichos datos o el borrado de los mismos...; d) Disponer de un recurso si no se ha atendido a una petición de confirmación o... de comunicación, de ratificación o de borrado.

35

Tanto las Directrices de la OCDE de 1980 como el Convenio 108 del Consejo de Europa contemplan una serie de disposiciones de suma importancia para el tratamiento de los datos personales en los tiempos de las comunicaciones electrónicas en al menos dos sentidos: reconocen una serie de derechos para las personas titulares de los datos personales, entre los que se encuentran los relativos a requerir su consentimiento, saber de su existencia, pedir su rectificación o eliminación, e interponer recursos de inconformidad, y garantizan el uso adecuado de los datos personales, al señalar límites para su recolección, los fines de ésta y las medidas de seguridad para el supuesto de pérdida o destrucción.

En 1995, en el contexto de la Unión Europea, se expidió la Directiva 95/46/EC del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, sobre la protección de los individuos con respecto al procesamiento de los datos personales y el libre movimiento de dichos datos, cuyo objeto es, acorde con su artículo 1, que los Estados miembros garanticen “la protección de las libertades y de los derechos fundamentales de las personas físicas, y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales”, y prohibir la restricción a “la libre circulación de datos personales entre los Estados miembros...”.

Adicionalmente, la Directiva 95/46/EC contempló un conjunto de disposiciones a subrayarse: es aplicable al tratamiento automatizado y no automatizado de datos personales (artículo 3); los Estados miembros quedaron obligados a implementar en sus legislaciones nacionales las disposiciones de la Directiva (artículo 4); se estableció que los datos personales serían tratados de manera leal y lícita; recogidos con fines determinados, explícitos y legítimos, sin que sean tratados posteriormente de manera incompatible con dichos fines; adecuados, pertinentes y no excesivos; exactos y actualizados, y conservados en un periodo no superior al necesario

MAURICIO AUGUSTO CALCANELO MONTS

36 ●
○
● para cumplir con los fines de su recolección (artículo 6); se requirió que el tratamiento de los datos personales sólo pudiera efectuarse si el interesado daba su consentimiento de forma inequívoca (artículo 7); se obligó a los responsables del tratamiento de los datos a revelar su identidad e indicar los fines de la recolección (artículo 10); se reconoció el derecho de las personas titulares de los datos recabados a confirmar la existencia o inexistencia de los mismos, los fines de su uso, la rectificación, la supresión o el bloqueo de los datos (artículo 12); se contempló el derecho de oposición de las personas para el tratamiento de sus datos para su uso con fines de prospección (artículo 14); se obligó a los Estados miembros a establecer que toda persona disponía de un recurso judicial en caso de violación de sus derechos en esta materia y que hayan sido garantizados conforme a la normatividad nacional (artículo 22); se estableció que los Estados miembros dispondrían de autoridades públicas encargadas de vigilar la aplicación de la Directiva en su territorio (artículo 28), y se creó un grupo de protección de las personas en lo que respecta al tratamiento de datos personales (artículo 29).

La Directiva 95/46/EC ahonda en las medidas de protección de los datos personales contempladas en las Directrices de la OCDE de 1980 y en el Convenio 108 del Consejo de Europa, al incluir derechos tales como el de oposición y al recurso judicial, al tiempo de prever la existencia de autoridades públicas encargadas de la vigilancia de la aplicación de la Directiva en los Estados miembros.

El 27 de abril de 2016, el Parlamento y Consejo Europeo aprobaron el Reglamento General de Protección Datos de la Unión Europea, aplicable a partir del 25 de mayo de 2018. A diferencia de la Directiva 95/46/EC, el Reglamento no requiere de su traducción al ámbito nacional, sino que es aplicable de manera directa en todos los Estados, e inclusive en superiores jerárquicamente (Elias, 2014). Además, el Reglamento es una normatividad transversal, que protege fuertemente a los sujetos titulares de los datos personales, que pone límites a las actividades de quienes recaban y procesan dichos datos, y que implica una vigorosa intervención estatal. El Reglamento es un intento por poner al día la legislación en materia de datos personales con los desarrollos tecnológicos observados durante los últimos treinta años a raíz del surgimiento y uso cada vez más extendido del Internet.

El artículo 1 establece como objeto del Reglamento “la protección de las personas físicas en lo que respecta al tratamiento de los datos personales... [y la protección] de los derechos y libertades fundamentales de las personas físicas, y en particular, su derecho a la protección de los datos

personales”. El artículo 3 se refiere a su ámbito territorial, al señalar que “se aplica al tratamiento de datos personales en el contexto de las actividades de un establecimiento... independientemente de que el tratamiento tenga lugar en la Unión o no”.

El artículo 5 versa sobre los principios relativos al tratamiento de los datos personales, al señalar que serán

tratados de manera lícita, leal y transparente en relación con el interesado... recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines... adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados... exactos y, si fuera necesario, actualizados... mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales.

37



El artículo 6, por su parte, dispone que el tratamiento de los datos personales será lícito sólo si la persona da su consentimiento para tal efecto. De modo que el artículo 7 establece como condiciones para dicho consentimiento, que “el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales... la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo... el interesado tendrá derecho a retirar su consentimiento en cualquier momento...”.

El artículo 13 desglosa la información que los responsables del tratamiento de los datos deberán proporcionar a los titulares de éstos, siendo las siguientes:

La identidad y los datos de contacto del responsable... los fines del tratamiento de los datos personales... los destinatarios o las categorías de destinatarios de los datos personales... la intención del responsable de transferir datos personales a un tercer país u organización internacional... el plazo durante el cual se conservarán los datos personales... la existencia del derecho a solicitar el acceso a los datos personales y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos... el derecho a presentar una reclamación ante una autoridad de control... la existencia de decisiones automatizadas, incluida la elaboración de perfiles...

El artículo 16 establece el derecho a la rectificación en caso de inexactitud en los datos personales. El artículo 17 contempla el derecho de

MAURICIO AUGUSTO CALCANELO MONTS

supresión o al olvido cuando los datos personales “ya no sean necesarios en relación a los fines para los que fueron recogidos o tratados... el interesado retire su consentimiento... [o] se oponga al tratamiento...”. El artículo 18 se refiere al derecho a la limitación del tratamiento. El artículo 19 trata del derecho a la portabilidad de datos, que consiste en el derecho del interesado a “recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento”. El artículo 21 regula el derecho de los interesados a oponerse a que los “datos personales que le conciernan sean objeto de un tratamiento”.

38

●
○
● El artículo 30 obliga a los responsables del tratamiento a llevar un registro de tales actividades. El artículo 32 les obliga a aplicar “medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo”. Los artículos 33 y 34 obligan a los responsables del tratamiento a dar aviso a las autoridades y a los particulares, dentro de las 72 horas siguientes, en caso de violación de la seguridad de los datos personales. El artículo 35 instaura la evaluación de impacto relativa a la protección de datos cuando “sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías... entrañe un alto riesgo para los derechos y libertades de las personas”.

El artículo 51 prevé la existencia de autoridades públicas independientes en cada Estado miembro, encargadas de “supervisar la aplicación del... Reglamento, con el fin de proteger los derechos y las libertades fundamentales de las personas físicas en lo que respecta al tratamiento y de facilitar la libre circulación de datos personales en la Unión”. El artículo 68 establece la creación del Comité Europeo de Protección de Datos como organismo de la Unión encargado de supervisar y garantizar la correcta aplicación del Reglamento, asesorar a la Comisión Europea en materia de datos personales, y emitir directrices, recomendaciones y buenas prácticas en el ámbito de los datos personales (artículo 70).

El artículo 77 prevé que “sin perjuicio de cualquier otro recurso administrativo o acción judicial, todo interesado tendrá derecho a presentar una reclamación ante una autoridad de control”. A su vez, el artículo 78 señala que “sin perjuicio de cualquier otro recurso administrativo o extrajudicial, toda persona física o jurídica tendrá derecho a la tutela judicial efectiva contra una decisión jurídicamente vinculante de una autoridad de control que le concierna”.

El artículo 82 otorga el derecho a la indemnización y responsabilidad a “toda persona que haya sufrido daños y perjuicios materiales o inmateriales

como consecuencia de una infracción del... Reglamento”. Mientras que el artículo 83 contempla las distintas multas administrativas aplicables por violaciones al Reglamento, las que tratándose de empresas pueden alcanzar el 4% del volumen de negocio total anual global del ejercicio financiero anterior.

En suma, el Reglamento actualiza a los desarrollos que han tenido lugar en los últimos treinta años, las disposiciones de la Unión Europea en materia de datos personales en el Internet. Es un punto de inflexión en la regulación sobre dicha materia al incluir disposiciones tales como su aplicación extraterritorial a quienes procesen datos de residentes europeos, independientemente de su localización; las condiciones para el otorgamiento del consentimiento para el tratamiento de los datos personales; los derechos de los titulares de los datos a la rectificación, al olvido, a la limitación del tratamiento, a la portabilidad, a oponerse al tratamiento, a la reclamación, a la tutela judicial efectiva y a la indemnización; las obligaciones de los responsables del tratamiento de datos, como es llevar un registro de las actividades de tratamiento, garantizar niveles adecuados de seguridad, dar aviso en caso de violaciones a la seguridad y hacer la evaluación de impacto para el uso de nuevas tecnologías; la creación de autoridades en la materia tanto a nivel nacional como comunitario, y la aplicación de multas administrativas por hasta el 4% del volumen de negocios globales de las empresas.

Las disposiciones del Reglamento han sido llevadas a nivel del derecho nacional de los países miembros de la Unión Europea, como es el caso de España y su Ley Orgánica 3/2018 de Protección de Datos Personales y Garantía de los Derechos Digitales, del 5 de diciembre de 2018. Su objeto es, acorde con el artículo 1, “adaptar el ordenamiento jurídico español al Reglamento (UE) 2016/679 del Parlamento Europeo y el Consejo... relativo a la protección de las personas físicas en lo que respecta al tratamiento de sus datos personales y a la libre circulación de estos datos, y completar sus disposiciones”.

El Reglamento es, sin duda, un paso firme para fortalecer la protección del derecho de las personas sobre sus datos personales y el uso que de éstos se haga por terceros, y para inhibir y, en su defecto, sancionar de manera firme los comportamientos de las empresas que se aparten de las reglas establecidas para la obtención, almacenamiento, procesamiento y análisis de datos personales en el Internet.



MAURICIO AUGUSTO CALCANELO MONTS

V. CONCLUSIONES

Las preocupaciones sobre la privacidad y los datos personales en los tiempos del Internet abarcan el cada vez mayor volumen de información disponible sobre las personas y el nivel de detalle y profundidad alcanzado (*big data*), y, más importante, las crecientes capacidades en términos predictivos y su uso para intentar moldear los comportamientos humanos en las más distintas esferas de nuestra actividad (*big data analytics*).

40 A dicho respecto, son dos los grandes modelos de regulación que están vigentes en el ámbito de las democracias occidentales: el norteamericano y el europeo.

- El modelo estadounidense de autorregulación empresarial está siendo cada vez más cuestionado, tanto desde el ámbito político como desde el académico y el ciudadano, por los grandes márgenes de discreción que se otorgan a las empresas en perjuicio de los individuos en aspectos tan medulares como los relativos a qué información personal se recolecta y cómo se usa ésta. Sin embargo, habida cuenta de la enorme polarización política prevaleciente en el vecino del norte, es poco probable que en el futuro cercano se tomen medidas a este respecto a pesar de las distintas propuestas existentes y de la presión cada vez mayor.

En Europa, la situación es diametralmente diferente, pues desde el 25 de mayo de 2018 está en vigor el Reglamento General de Datos Personales. Se trata, sin duda, de una regulación con un enfoque más acorde con la tradición jurídica romano-germánica y, por ende, más cercana a la cultura jurídica mexicana. Es una regulación con carácter obligatorio en los distintos Estados que integran a la Unión Europea, que abarca a la totalidad de los sectores involucrados, y que establece medidas en favor de los usuarios, como son los derechos al consentimiento expreso, a retractarse, al olvido, a la rectificación, a conocer qué datos tienen las empresas y cómo los usan, entre otros. Al tiempo que acota el actuar de las empresas mediante la posibilidad de aplicar sanciones de hasta el 4% de su volumen de negocios globales.

La regulación europea sobre datos personales en el Internet es, desde esta perspectiva, la respuesta más acorde a los desafíos que implican el *big data*, el *big data analytics* y los datos personales en los tiempos del Internet. Sin embargo, el debate no está cerrado ni mucho menos; por el contrario, hay toda una agenda de investigación por desarrollar, que comprende aspectos tales como el análisis minucioso de las distintas disposiciones de la regulación europea; los efectos a corto, mediano y largo plazos de su

entrada en vigor, tanto en el Internet como en las distintas industrias, en el *big data*, en el *big data analytics* y en la innovación tecnológica; la aplicación concreta de sus disposiciones tanto en el ámbito administrativo como en el jurisdiccional; el impacto que tendrá allende las fronteras sobre los distintos sistemas jurídicos y en los regímenes jurídicos nacionales, por mencionar sólo algunos. Tal es el reto en este tema de enorme incidencia y alcance para el presente y el futuro de nuestras sociedades.

41

VI. FUENTES

- ALTMAN, Micah *et al.*, 2018, “Practical Approaches to Big Data Privacy over Time”, *International Data Privacy Law*, vol. 8.
- BOND, Robert M. *et al.*, 2012, “A 61-Million-Person Experiment in Social Influence and Political Mobilization”, *Nature*, vol. 489.
- CATE, Fred H., 2014, “The Big Data Debate”, *Science*, vol. 346.
- CUBILLOS VÉLEZ, Ángela, 2017, “La explotación de los datos personales por los gigantes del Internet”, *Estudios en Derecho a la Información*, núm. 3.
- DIAMOND, Larry, 2019, “The Threat of Postmodern Totalitarianism”, *Journal of Democracy*, vol. 30.
- EINAV, Liran y LEVIN, Jonathan D., 2013, “The Data Revolution and Economic Analysis”, *National Bureau of Economic Research Working Paper Series*, Working Paper 10635.
- ELIAS, Peter, 2014, “A European Perspective on Research and Big Data Analysis”, en LANE, Julia *et al.*, *Privacy, Big Data, and the Public Good*, Nueva York, Cambridge University Press.
- FEDERAL TRADE COMMISSION, 2014, *Data Brokers. A Call for Transparency and Accountability*, disponible en: <https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf> (fecha de consulta: 17 de mayo de 2018).
- FREEDOM HOUSE, 2017, *Freedom on the Net 2017. Manipulating Social Media to Undermine Democracy*, disponible en: <https://freedomhouse.org/report/freedom-net/freedom-net-2017> (fecha de consulta: 10 de junio de 2018).
- FUKUYAMA, Francis, 2018, “Facebook vs. Democracy. A Conversation with Francis Fukuyama”, *Monday Note*, 14 de mayo, disponible en: <https://mondaynote.com/facebook-vs-democracy-a-conversation-with-francis-fukuyama-a01e513b9820> (fecha de consulta: 5 de junio de 2018).

MAURICIO AUGUSTO CALCANEO MONTS

GOLDFARB, Avi y TUCKER, Catherine, 2011, "Privacy and Innovation", *National Bureau of Economic Research Working Paper Series*, Working Paper 17124.

JAIN, Priyank *et al.*, 2016, "Big Data Privacy: a Technological Perspective and Review", *Journal of Big Data*.

42 KOSINSKI, Michal *et al.*, 2013, "Private Traits and Attributes are Predictable from Digital Records of Human Behavior", *Proceedings of the National Academy of Sciences of the United States of America*, vol. 110, núm. 15.

● KOSINSKI, Michal y BEHREND, Tara, 2017, "Editorial Overview: Big Data in the Behavioral Sciences", *Current Opinion in Behavioral Sciences*, vol. 18.

○ LAZER, David *et al.*, 2009, "Computational Social Science", *Science*, vol. 323.

● LYMAN, Peter y VARIAN, Hal R., 2003, "How Much Information 2003?", disponible en: <http://groups.ischool.berkeley.edu/archive/how-much-info-2003/> (fecha de consulta: 15 de mayo de 2018).

MATZ, Sandra C. *et al.*, 2017, "Using Big Data as a Window into Consumers' Psychology", *Current Opinion in Behavioral Sciences*, vol. 18.

OHM, Paul, 2014, "Changing the Rules: General Principles for Data Use and Analysis", en LANE, Julia *et al.*, *Privacy, Big Data, and the Public Good*, Nueva York, Cambridge University Press.

PENDERGAST, Tom, 2018, "The Next Cold War is Here, and It's All About Data", *Wired*, 28 de marzo, disponible en: <https://www.wired.com/story/opinion-new-data-cold-war/> (fecha de consulta: 12 de mayo de 2018).

PERSILY, Nathaniel, 2017, "Can Democracy Survive the Internet?", *Journal of Democracy*, vol. 28, núm. 2.

SHOREY, Samantha y HOWARD, Philip N., 2016, "Automation, Big Data, and Politics: A Research Review", *International Journal of Communication*, núm. 10.

STRANDBURG, Katherine J., 2014, "Monitoring, Datafication, and Consent: Legal Approaches to Privacy in the Big Data Contest", en LANE, Julia *et al.*, *Privacy, Big Data, and the Public Good*, Nueva York, Cambridge University Press.

TUCKER, Joshua A. *et al.*, 2017, "From Liberation to Turmoil: Social Media and Democracy", *Journal of Democracy*, vol. 28, núm. 4.

TUCKER, Joshua A., 2018, *Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature*, disponible en: <https://www.hewlett.org/wp-content/uploads/2018/03/Social-Media-Political-Polarization-and-Political-Disinformation-Literature-Review.pdf> (fecha de consulta: 11 de junio de 2018).

- VARIAN, Hal R., 2010, "Computer Mediated Transactions", *American Economic Review: Papers and Preceedings*, núm. 100.
- WHEELER, Tom, 2018, "Can Europe Lead on Privacy?", *New York Times*, 1o. de abril, disponible en: <https://www.nytimes.com/2018/04/01/opinion/europe-privacy-protections.html> (fecha de consulta: 12 de mayo de 2018).
- WHITE HOUSE, 2012, "Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy", *Journal of Privacy and Confidentiality*, núm. 2. 43
- WHITE HOUSE, 2014a, *Big Data: Seizing Opportunities, Preserving Values*, Washington, D. C., Executive Office of the President, disponible en: https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf (fecha de consulta: 16 de mayo de 2018). ● ○ ●
- WHITE HOUSE, 2014b, *Big Data and Privacy: A Technological Perspective*, Washington, D. C., Executive Office of the President-President's Council of Advisors on Science and Technology, disponible en: https://bigdatatwg.nist.gov/pdf/pcast_big_data_and_privacy_-_may_2014.pdf (fecha de consulta: 16 de mayo de 2018).
- ZUCKERBERG, Mark, 2019, "The Internet Needs New Rules. Let's Start in these Four Areas", *The Washington Post*, 31 de marzo, disponible en: https://www.washingtonpost.com/opinions/mark-zuckerberg-the-internet-needs-new-rules-lets-start-in-these-four-areas/2019/03/29/9e6f0504-521a-11e9-a3f7-78b7525a8d5f_story.html?utm_term=.fbabc7d7beb7 (fecha de consulta: 1o. de abril de 2019).

Marco normativo

- California Privacy Consumer Act, disponible en: https://leginfo.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375 (fecha de consulta: 12 de abril de 2019).
- Constitución de los Estados Unidos de América, disponible en: <https://www.archives.gov/espanol/constitucion> (fecha de consulta: 12 de abril de 2019).
- Convenio del Consejo de Europa para la Protección de los Derechos Humanos y de las Libertades Fundamentales de 1950, disponible en: <https://www.coe.int/en/web/human-rights-convention/the-convention-in-1950> (fecha de consulta: 12 de abril de 2019).
- Convenio 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de carácter Per-

MAURICIO AUGUSTO CALCANELO MONTS

sonal del 28 de enero de 1981, disponible en: <http://inicio.ifai.org.mx/Estudios/B.28-cp--CONVENIO-N-1o--108-DEL-CONSEJO-DE-EUROPA.pdf> (fecha de consulta: 13 de abril de 2019).

Directrices de la OCDE sobre Protección de la privacidad y flujos transfronterizos de datos personales de 1980, disponible en: <https://www.oecd.org/sti/ieconomy/15590267.pdf> (fecha de consulta: 13 de abril de 2019).

- 44 Directiva 95/46/EC del Parlamento Europeo y del Consejo, del 24 de octubre de 1995, sobre la protección de los individuos con respecto al procesamiento de los datos personales y el libre movimiento de dichos datos, disponible en: <https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:31995L0046&from=EN> (fecha de consulta: 13 de abril de 2019).

● Fair Credit Reporting Act, disponible en: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/fair-credit-reporting-act> (fecha de consulta: 13 de abril de 2019).

● Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, disponible en: <https://www.boe.es/buscar/doc.php?id=BOE-A-2018-16673> (fecha de consulta: 13 de abril de 2019).

Privacy Act of 1974, disponible en: <https://www.govinfo.gov/content/pkg/USCODE-2012-title5/pdf/USCODE-2012-title5-partI-chap5-subchapII-sec552a.pdf> (fecha de consulta: 13 de abril de 2019).

Reglamento General de Protección Datos de la Unión Europea, disponible en: <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN> (fecha de consulta: 13 de abril de 2019).

GOBIERNO CERCANO Y MODERNO: UNA MIRADA
DESDE LOS ESTÁNDARES INTERNACIONALES
DEL ACCESO A LA INFORMACIÓN PÚBLICA
*CLOSE AND MODERN GOVERNMENT: A VIEW
FROM THE INTERNATIONAL STANDARDS
OF ACCESS TO PUBLIC INFORMATION*



*Arturo Miguel CHIPULI CASTILLO**

RESUMEN: El Programa para un Gobierno Cercano y Moderno (PGCM) representó uno de los diversos programas transversales de política pública implementados por el gobierno federal mexicano como parte del Plan Nacional de Desarrollo para el periodo 2013-2018. Entre sus objetivos fundamentales se planteó la construcción de una política de gobierno abierto, que implicó diversas estrategias y líneas de acción tendientes, entre otras cosas, al desarrollo de la transparencia y del acceso a la información pública en el ámbito de la administración pública federal. Derivado de lo anterior, cabe preguntarse en qué medida el programa integró en su diseño el enfoque de derechos humanos para cumplir con las obligaciones en materia de acceso a la información pública. El argumento principal que el PGCM, a pesar de que estableció algunas estrategias y acciones con relación al derecho de acceso a la información pública, cumplió parcialmente con los estándares internacionales del citado derecho. Con motivo de lo anterior, el presente documento analiza los objetivos, las estrategias y las líneas de acción que integraron

* Es licenciado en derecho por la Universidad Veracruzana; maestro en derecho constitucional y juicio de amparo por la Universidad de Xalapa; maestro en derechos humanos y democracia por la Facultad Latinoamericana de Ciencias Sociales (FLACSO), sede México; y doctor en derecho por la Universidad de Xalapa. Actualmente es investigador adscrito al Instituto de Investigaciones Jurídicas de la Universidad Veracruzana. Correo: a_chipuli@hotmail.com.

Fecha de recepción: 25 de enero de 2019.

Fecha de dictamen: 28 de marzo de 2019.

ARTURO MIGUEL CHIPULI CASTILLO

al PGCM a través de cinco unidades de análisis, de donde se concluye que el programa transversal observó un nivel bajo de cumplimiento del estándar internacional del derecho de acceso a la información pública.

46

PALABRAS CLAVE: acceso a la información, gobierno cercano y moderno, políticas públicas, derechos humanos.

-
-
-

ABSTRACT: The Close and Modern Government Program (PGCM) represented one of the several transversal public policy programs implemented by the Mexican federal government as part of the National Development Plan for the period 2013-2018. Among its fundamental objectives was the construction of an open government policy, which involved manifold lines of action and strategies tending, among other things, to the development of transparency and access to public information in the Federal scope of Public Administration. In view of the above, it should be questioned to what extent did the program integrate the human rights approach into its design in order to accomplish obligations in matter of access to public information. The main argument is that, even though the program established actions and strategies in relation to the right of access to public information, they partially achieve international standards in the matter. In view of the above, this document analyzes the objectives, lines of action and strategies that integrated the program through five analysis units, from which it is concluded that the transversal program observed a low level of achievement of the international standards of the right to access to public information.

KEY WORDS: access to information, close and modern government, public policy, human rights.

I. INTRODUCCIÓN

El Programa para un Gobierno Cercano y Moderno (PGCM) fue un programa de política pública de corte transversal que surgió como parte del Plan Nacional de Desarrollo 2013-2018. Dicho programa puso gran énfasis en los principios del gobierno abierto, particularmente sobre la transparencia y

el acceso a la información pública, con la finalidad de mejorar la rendición de cuentas. Derivado de lo anterior, cabe preguntarse en qué medida el PGCM integró en su diseño el enfoque de derechos humanos para cumplir con las obligaciones en materia de acceso a la información pública. El argumento principal es que a pesar de que estableció algunas acciones y estrategias con relación al derecho de acceso a la información, el PGCM cumple parcialmente con los estándares internacionales del citado derecho.

Derivado de lo antes expuesto, el presente artículo tiene como propósito fundamental analizar el grado de incidencia del derecho internacional de los derechos humanos (DIDH) sobre el diseño del PGCM, particularmente en lo que respecta al derecho humano de acceso a la información pública. En ese sentido, en el primer apartado se analiza, de forma general, lo relativo a las políticas públicas, su evolución, sus características, y la creciente necesidad de incorporar el enfoque de derechos humanos en todo su ciclo. El segundo apartado se dedica al estudio del derecho de acceso a la información pública, así como al conjunto de obligaciones que le son propias conforme al DIDH. En el tercer apartado, y con base en las obligaciones en materia de acceso a la información, se construyó una matriz de indicadores a través de la cual se valora el nivel de cumplimiento/incumplimiento del programa de política pública en examen. Finalmente, en el último apartado se presentan los resultados de la evaluación al programa en estudio.

47



II. METODOLOGÍA

Para el logro del objetivo antes planteado se recurrirá parcialmente a la metodología del enfoque de derechos humanos. Dicho enfoque requiere tener presentes dos conjuntos de elementos: *a*) los estándares internacionales de derechos humanos, y *b*) los elementos transversales (mecanismos de exigibilidad, principio de igualdad y perspectiva de género, participación, etcétera). El presente documento se ceñirá al primero de estos conjuntos, derivado de lo cual, en primer lugar, se procede a la identificación de las obligaciones contenidas en las diversas fuentes de *hard* y *soft law* del DIDH, y sobre las cuales se construye un estándar en materia de acceso a la información pública. De los componentes descritos en el citado estándar se seleccionaron cinco categorías como unidades de análisis: *a*) transparencia pasiva; *b*) transparencia activa; *c*) obligación de capturar o producir informa-

ARTURO MIGUEL CHIPULI CASTILLO

ción; *d*) gestión adecuada de archivos, y *e*) protección de servidores públicos o *whistleblowers*.¹

48 A partir de dichas unidades se examinan los objetivos y líneas de acción del PGCM, a fin de dilucidar, primero, los rubros cuyo contenido se vincula al derecho a la información; segundo, el grado de cumplimiento/incumplimiento de las obligaciones en materia de acceso a la información pública, calificando la incidencia del estándar en el diseño del programa de política pública mediante una escala de cinco niveles, al cual se le asigna un valor que va del 0 al 4.²

● Finalmente, para la calificación del programa en general se sumó el
○ puntaje total de cada categoría analizada (donde cada componente puede
● tener una calificación máxima de 4 y mínima de 0), con base en lo cual se construyó una escala de seis niveles, donde el nivel más alto se califica con 20 puntos (cumplimiento total del estándar: calificación de 4 en todas las categorías), y el más bajo con 0 (incumplimiento total: calificación de 0 en todas las categorías).

III. DERECHOS HUMANOS Y POLÍTICAS PÚBLICAS

Las políticas públicas representan una forma de racionalizar la actividad pública, en la cual la acción gubernamental se encuentra orientada hacia la resolución de problemas de impacto general en un contexto determinado, a través de decisiones, estrategias y recursos del Estado. En este sentido, el enfoque de políticas públicas conlleva la necesidad de entender a lo público como aquella dimensión de la actividad humana que requiere algún tipo de intervención o regulación por parte del Estado (Parsons, 2007), y a las políticas (*policy*) como la capacidad del gobierno de intervenir racionalmente en la solución de problemas públicos (Del Castillo y Méndez, 2010).

¹ Los elementos restantes (adecuación normativa, recurso para la satisfacción del derecho de acceso a la información, recurso judicial efectivo, cultura de transparencia y entrenamiento de servidores públicos), por sus características, se ha considerado más pertinente abordarlos en un documento posterior, desde los elementos transversales del enfoque de derechos humanos, particularmente en los rubros de mecanismos de exigibilidad y capacitación en derechos humanos.

² La escala se construyó tomando como criterio la medida en que el programa cumple (o incumple) con las conductas señaladas por el estándar. Un cumplimiento total de los elementos será calificado con 4 puntos; un cumplimiento alto (más del 50% de los elementos del estándar) con 3; un cumplimiento medio (50% del estándar) con 2; un cumplimiento bajo (menos del 50% del estándar) con 1; y finalmente, un cumplimiento nulo (el programa no contempla ningún elemento del estándar) con 0.

Con el surgimiento del estudio de las políticas públicas se inició una nueva etapa en la acción y administración estatal tendiente a generar los mayores beneficios a partir de recursos limitados y, sobre todo, a través de un serio replanteamiento de las ciencias de la administración pública y del gobierno. En este contexto, surgen procesos de estudio, diseño y evaluación de políticas públicas, que han contribuido al desarrollo de soluciones racionales a problemas de la esfera pública. Empero, uno de los temas ausentes en el enfoque de políticas públicas ha sido el cumplimiento de las obligaciones que los Estados han adoptado con motivo de su incorporación a los sistemas internacionales de derechos humanos, a través de la firma y ratificación de los instrumentos internacionales de DD.HH. Dichas obligaciones se traducen en elementos que reconocen a la persona como titular de derechos frente al Estado, lo cual pone en evidencia problemas públicos más complejos y que, de acuerdo con el derecho internacional de los derechos humanos (DIDH), corresponde al Estado resolver.

El enfoque de derechos humanos representa un aporte de carácter sustantivo para los contenidos de las políticas públicas, que pone énfasis en las obligaciones estatales, consagrándose éstas como directrices de contenido. De tal forma que las políticas públicas se vislumbran como medios de satisfacción de derechos, y no sólo como mecanismos para la solución de problemas y demandas insatisfechas (Salazar, 2014), reconociendo a las personas como titulares de derechos, empoderándolas para exigir o demandar acciones concretas del Estado, a través de un marco de obligaciones consagradas por el DIDH.

IV. EL ACCESO A LA INFORMACIÓN PÚBLICA EN EL DERECHO INTERNACIONAL DE LOS DERECHOS HUMANOS: HACIA UN ESTÁNDAR INTERNACIONAL

Los estándares internacionales parten de la premisa de que el DIDH representa un marco conceptual que es aceptado por la comunidad internacional, y que puede ofrecer un sistema coherente de principios y reglas que contribuye a definir con mayor precisión las obligaciones de los Estados frente a los derechos humanos (Abramovich, 2006: 36). El DIDH se encuentra integrado por instituciones y órganos de diversa naturaleza, que encuentran sus fuentes (*corpus iuris*) dentro de una diversidad de sistemas, los cuales comúnmente se agrupan en dos grandes rubros: el sistema universal de derechos humanos (SUDH) y los sistemas regionales (europeo, africano e interamericano), los cuales operan en muchas ocasiones de manera si-



ARTURO MIGUEL CHIPULI CASTILLO

50 multánea. En la práctica, estas fuentes se interconectan y operan de forma conjunta, de ahí que para poder advertir con mayor claridad las obligaciones de los Estados en materia de derechos humanos es importante realizar una lectura transversal de las distintas fuentes que lo componen. A partir de lo anterior, y en el marco de las políticas públicas, los estándares internacionales fungen como marco de referencia para la articulación de intervenciones estatales a partir de un conjunto de obligaciones previamente establecidas por el DIDH, las cuales permiten advertir un cierto grado de certeza respecto de las conductas exigibles al Estado.³ En las líneas que siguen se analizarán algunas fuentes del DIDH que abordan el derecho de acceso a la información.

● El derecho humano de acceso a la información pública es aquel que tiene toda persona para “acceder a la información que está en posesión, custodia o control de cualquier autoridad pública” (Negro, 2014: 64). Su trascendencia parte del reconocimiento explícito que el sistema universal, así como los sistemas regionales y nacionales, le han dado como un derecho humano fundamental para la construcción de la ciudadanía y vital para el funcionamiento y la preservación del sistema democrático, en tanto la información pública es esencial para abrir y profundizar mecanismos y espacios de participación popular directa, que permiten informar a la ciudadanía sobre las acciones de gobierno que se adoptan en ejercicio de la acción política (Rossi y Moro, 2014: 83), así como para proteger derechos y prevenir abusos por parte del Estado, luchar contra la corrupción, el secretismo y la realización de otros derechos humanos (CIDH, 2012).

En el contexto del SUDH, el punto de partida de la institucionalización del derecho de acceso a la información pública fue la libertad de información, reconocida por la Asamblea General de Naciones Unidas en su Resolución 59 (1), y posteriormente, por los artículos 19 de la Declaración Universal de los Derechos Humanos de 1948⁴ y 19 del Pacto Internacional de Derechos Civiles y Políticos.⁵

³ No obstante lo vertido, es menester señalar que la idea de “estándar internacional” representa una categoría en disputa, pues a pesar del progreso en la fijación de contenidos obligacionales respecto de los diversos derechos inscritos en los tratados internacionales, la naturaleza del DIDH es cambiante y con muchos espacios por llenar, lo cual supone un problema a la supuesta estabilidad que significa la determinación de un estándar.

⁴ “Artículo 19.- Todo individuo tiene derecho a la libertad de opinión y de expresión; este derecho incluye el de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión” (Declaración Universal de los Derechos Humanos).

⁵ “Artículo 19.2.- Toda persona tiene derecho a la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin

Al respecto, y más allá de las citadas fuentes, los órganos del sistema universal de derechos humanos han realizado algunas consideraciones en torno al derecho de acceso a la información, mismas que han quedado asentadas en diversas observaciones generales, informes de la Relatoría Especial para la Libertad de Opinión e Información, y que han abonado a la construcción, interpretación y ampliación del marco obligacional del derecho en estudio. Por su parte, en el ámbito regional, y específicamente respecto del sistema interamericano de derechos humanos (SIDH), del cual México forma parte, la Convención Americana sobre Derechos Humanos (CADH) ha reconocido la libertad de información dentro de su artículo 13,⁶ mismo que conlleva al derecho de acceso a la información en poder del Estado.

51

Con base en lo antes referido, y para analizar del diseño del programa de política pública “Programa para un Gobierno Cercano y Moderno 2013-2018” del gobierno federal, nos enfocaremos en los estándares interamericanos del derecho de acceso a la información pública, que han sido desarrollados por la CIDH.⁷ Sin embargo, no pasamos por alto que a pesar del progreso del SIDH en la fijación de estándares, todavía hay muchos espacios por llenar en las interpretaciones de los órganos internacionales, ya que la jurisprudencia internacional no es estática, sino dinámica (Serrano y Vázquez, 2013: 49), motivo por el cual, para la elaboración de los esquemas de obligaciones, también se retomarán algunas iniciativas propias de otros sistemas de derechos humanos, así como algunas iniciativas de órganos internacionales relacionadas con el tema.

consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección” (Pacto Internacional de Derechos Civiles y Políticos).

⁶ “Artículo 13.1.- Toda persona tiene derecho a la libertad de pensamiento y de expresión. Este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección” (Convención Americana sobre Derechos Humanos).

⁷ El trabajo de los órganos del SIDH ha sido trascendental para el desarrollo de los estándares del derecho a la información pública. A partir de la sentencia de la Corte Interamericana de Derechos Humanos (CoIDH) sobre el caso Claude Reyes y otros vs. Chile, los órganos del SUDH y del SIDH empiezan a generar un amplio consenso sobre la existencia y características del derecho a la información. De tal forma que el SIDH ha generado un amplio contenido que ha sido replicado y complementado por los demás sistemas internacionales de protección de los derechos humanos.

ARTURO MIGUEL CHIPULI CASTILLO

El desempaque del derecho de acceso a la información pública

Los derechos humanos están constituidos por múltiples componentes o atributos, que pueden denominarse “subderechos”. Éstos se definen como “los factores integrantes de cada uno de los derechos humanos, algunos puntualmente precisados en los tratados y otros fruto del desarrollo del *corpus iuris* internacional. En consecuencia, se trata de una lista abierta para satisfacer las necesidades que los cambios políticos, sociales y económicos imponen a las personas” (Serrano y Vázquez, 2013: 54 y 55). El acceso a la información pública representa un subderecho del derecho a la libertad expresión,⁸ que involucra la potestad de toda persona de acceder a la información en control del Estado, amparando el derecho a recibir, buscar y difundir dichos datos, y generando la obligación positiva a cargo del Estado, de suministrarlos (caso Claude Reyes y otros vs. Chile: 43).

De acuerdo con el SIDH, el derecho humano en análisis se compone por dos principios fundamentales: el principio de máxima divulgación y el principio de buena fe (caso Gomes Lund y otros vs. Brasil: 86). Estos principios deben regir la gestión estatal, orientando cualquier tipo de intervención estatal que tenga que ver con la transparencia (CIDH, 2012: 4). Asimismo, y siguiendo las pautas establecidas por la CIDH, las obligaciones que integran al derecho de acceso a la información pública son:

⁸ La razón por la cual el derecho de acceso a la información se entiende como elemento integrante del derecho a la libertad de expresión puede encontrar sus bases en lo señalado por la CoIDH: “la libertad de expresión es un elemento fundamental sobre el cual se basa la existencia de una sociedad democrática. Es indispensable para la formación de la opinión pública. Es también *conditio sine qua non* para que... quienes deseen influir sobre la colectividad puedan desarrollarse plenamente. Es, en fin, condición para que la comunidad, a la hora de ejercer sus opciones esté suficientemente informada. Por ende, es posible afirmar que una sociedad que no está bien informada no es plenamente libre” (caso Claude Reyes y otros vs. Chile: 46).

CUADRO I
 OBLIGACIONES QUE INTEGRAN AL DERECHO DE ACCESO
 A LA INFORMACIÓN PÚBLICA

		<i>Descripción</i>
<i>Principios</i>	Máxima divulgación	Implica que la transparencia y el acceso a la información deben ser la regla general, por lo cual: 1) deben estar sometidos a un régimen limitado de excepciones, el cual se interpreta de manera estricta; 2) la carga probatoria corresponde al Estado, y 3) el derecho de acceso a la información tiene preeminencia en caso de conflicto de normas o falta de regulación (CIDH, 2012: 4).
	Buena fe	Establece que los sujetos obligados deben actuar siempre de buena fe, es decir, interpretando la ley de manera tal que sirva para cumplir con los fines perseguidos por el derecho de acceso a la información (estricta aplicación, medios de asistencia, cultura de transparencia, actuación con diligencia, profesionalidad y lealtad institucional) (CIDH, 2012: 4).
<i>Obligaciones</i>	Transparencia pasiva	El Estado debe garantizar la existencia de un procedimiento administrativo adecuado para la tramitación y resolución de las solicitudes de información. El Estado debe responder sustancialmente a las solicitudes de información que le sean formuladas (caso Claude Reyes y otros vs. Chile: 62; Caso Gomes Lund y otros vs. Brasil: 86; CIDH, 2012: 9).
	Transparencia Activa	Las autoridades y órganos públicos tienen la obligación de publicar, de manera dinámica e incluso en ausencia de solicitudes, información de interés público (OEA, 2004). Es decir, se trata de una obligación de suministrar al público la máxima cantidad de información en forma oficiosa (CIDH, 2012: 12).
	Derecho a un recurso administrativo	El Estado está obligado a establecer un mecanismo especial de naturaleza administrativa que sea adecuado para la tramitación y resolución de las solicitudes de información, que fijen los plazos para resolver y entregar la información, y que se encuentre bajo la responsabilidad de funcionarios debidamente capacitados (caso Claude Reyes y otros vs. Chile: 62; CIDH, 2012: 9).



ARTURO MIGUEL CHIPULI CASTILLO

54



		<i>Descripción</i>
<i>Obligaciones</i>	Derecho a un recurso judicial	El Estado está comprometido a establecer un recurso judicial idóneo y efectivo que permita controvertir las decisiones de los funcionarios públicos que niegan el derecho de acceso a una determinada información o que omiten dar respuesta a la solicitud (caso Claude Reyes y otros vs. Chile: 62; CIDH, 2012: 11).
	Obligación de capturar o producir información	El Estado tiene la obligación de producir y/o capturar información necesaria para el cumplimiento de sus deberes. Esto implica la producción de información estadística desagregada, bases de datos e indicadores de evaluación (CIDH, 2012: 14; OEA, 2008: Resolutivo 10).
	Derecho a una cultura de transparencia	De acuerdo con la CIDH (2012: 14), una de las obligaciones de los Estados, con relación al derecho de acceso a la información pública, es la de generar una cultura de transparencia. En este sentido, y con fundamento en el resolutivo 10 de los Principios sobre el Derecho de Acceso a la Información del Comité Jurídico Interamericano (OEA, 2008), “deben adoptarse medidas para promover, implementar y asegurar el derecho de acceso a la información, incluyendo... la implementación de programas para aumentar la importancia en el público de este derecho”.
	Gestión adecuada de archivos	El Estado debe adoptar normas, políticas y prácticas que permitan conservar y administrar adecuadamente la información, de tal forma que cumplan al menos con las normas mínimas de gestión de archivos (CIDH, 2012: 15; OEA, 2004).
	Capacitación de servidores públicos	Los Estados deben realizar, en un plazo razonable, la capacitación a los órganos, autoridades y agentes públicos encargados de atender las solicitudes de acceso a información bajo control del Estado sobre la normativa que rige este derecho, que incorpore los parámetros convencionales que deben respetarse en materia de restricciones al acceso a dicha información (caso Claude Reyes y otros vs. Chile: 62); es decir, la implementación adecuada del derecho de acceso a la información en los Estados debe sujetarse a una política sistemática de entrenamiento y capacitación de los servidores públicos, la cual está destinada a la satisfacción del mismo en todas sus facetas (CIDH, 2012: 15).

		<i>Descripción</i>
<i>Obligaciones</i>	Obligación de adecuación normativa	Los Estados se encuentran obligados a adecuar su ordenamiento jurídico interno a los estándares internacionales. Esto conlleva tres cuestiones particulares: <i>a)</i> implementar un marco jurídico adecuado; <i>b)</i> remover obstáculos legales y/o administrativos; <i>c)</i> promover la implementación de derecho de acceso dentro de todas las entidades y autoridades, y <i>d)</i> adoptar una política favorable al pleno ejercicio del derecho (CIDH, 2012: 16).
	Protección de servidores públicos o <i>whistleblowers</i>	El Estado debe garantizar la protección de denunciantes de irregularidades frente a sanciones legales, administrativas o laborales (OEA, 2004), así como a la imposición de normativas que prohíban o limiten la divulgación de información. De igual manera, los periodistas deben quedar excluidos de responsabilidad por la publicación de información clasificada o confidencial siempre que no hayan cometido un ilícito para obtenerla (OEA, 2010).



FUENTE: Elaboración propia.

V. EL ENFOQUE DE DERECHOS HUMANOS EN LAS POLÍTICAS PÚBLICAS: UNA MIRADA AL PGCM

1. *El Programa para un Gobierno Cercano y Moderno 2013-2018*

El 20 de mayo de 2013, Enrique Peña Nieto, presidente constitucional de los Estados Unidos Mexicanos para el periodo 2012-2018, presentó el Plan Nacional de Desarrollo (PND) 2013-2018, que fue publicado en esa misma fecha en el *Diario Oficial de la Federación*. EL PND 2013-2018 tuvo como objetivo general “llevar a México a su máximo potencial”, lo cual se realizaría a partir de cinco metas nacionales y tres estrategias transversales. Dentro de estas últimas encontramos al PGCM, que consideró un conjunto de objetivos, estrategias y acciones encaminados a impulsar una administración pública eficiente, eficaz, innovadora y transparente, orientada a resultados y bajo los principios del gobierno abierto, así como con la capacidad tecnológica que permitiría la cercanía con las y los gobernados a través de las tecnologías de la información y la comunicación (PGCM, 2013).

El programa contempló cinco grandes objetivos: 1) impulsar un gobierno abierto para fomentar la rendición de cuentas en la administración pública federal (APF) mediante 7 estrategias y 57 líneas de acción; 2) for-

ARTURO MIGUEL CHIPULI CASTILLO

tales el presupuesto basado en resultados de la APF mediante 5 estrategias y 32 líneas de acción; 3) optimizar el uso de los recursos en la APF mediante 4 estrategias y 22 líneas de acción); 4) mejorar la gestión pública gubernamental en la APF mediante 5 estrategias y 36 líneas de acción, y 5) establecer una estrategia digital nacional mediante 7 estrategias y 62 líneas de acción.

56 Con base en lo anterior, el PGCM conjuntó una serie de herramientas proyectadas para impulsar el gobierno abierto,⁹ que encuentra uno de sus pilares fundamentales en la transparencia y el acceso a la información pública. De ahí que, para el presente programa, el desarrollar acciones concretas en dicho rubro fue uno de los objetivos principales. Sin embargo, es menester analizar si los citados objetivos, las estrategias y las acciones del programa de política pública fueron concebidos a partir de la observancia de los estándares internacionales del derecho de acceso a la información pública, cuestión que se aborda en los apartados siguientes.

2. Obligaciones y elementos institucionales

Una vez identificados los diversos componentes del derecho, es menester advertir cuáles son las obligaciones específicas insertas en cada uno de ellos. Las obligaciones en materia de derechos humanos son aquellas que “recorren a todos y cada uno de los derechos, las relaciones entre ellos y determinan la actividad estatal... son el mapa que nos permite ubicar las conductas exigibles tanto respecto de casos particulares como en relación a la adopción de medidas y de legislación” (Serrano y Vázquez, 2013: 49 y 50). En ese sentido, y siguiendo a los autores en cita, esta dinámica permite pensar a los derechos humanos a partir de sus obligaciones, lo que hace posible establecer un “marco analítico general que examine los derechos de forma más completa” (Serrano y Vázquez, 2013: 50), operacionalizándolos y traducéndolos en herramientas analíticas que permitan su aplicación práctica y exigibilidad. Partiendo de lo anterior, las obligaciones pueden tener distinta naturaleza, dependiendo de la conducta que llevan

⁹ Aunque se trata de un concepto en construcción y con múltiples definiciones, de manera general un gobierno abierto se refiere al “conjunto de mecanismos y estrategias que contribuyen a la gobernanza pública y al buen gobierno, basado en los pilares de la transparencia, la participación ciudadana, rendición de cuentas, colaboración e innovación, centrande e incluyendo a la ciudadanía en el proceso de toma de decisiones, así como en la formulación e implementación de políticas públicas, para fortalecer la democracia, la legitimidad de la acción pública y el bienestar colectivo” (CLAD, 2016: 5).

implícita. Siguiendo las pautas de los autores antes citados, estas obligaciones pueden esquematizarse de la siguiente manera:

CUADRO 2
 OBLIGACIONES EN MATERIA
 DE DERECHOS HUMANOS

<i>Obligaciones generales</i>	<i>Principios de aplicación</i>	<i>Elementos institucionales</i>	<i>Deberes</i>
Respetar	Contenidos esenciales	Disponibilidad	Verdad-investigación
Proteger	Progresividad	Accesibilidad	Reparación
Garantizar	Prohibición de regresión	Calidad	Sanción
Promover	Máximo uso de recursos disponibles	Aceptabilidad	

FUENTE: Serrano y Vázquez (2013: 12).

Siendo principalmente las obligaciones generales y los elementos institucionales los que se abordarán con relación al derecho de acceso a la información pública dentro del programa en estudio, a continuación se explica brevemente en qué consisten:

Las obligaciones generales, conforme a la tipología antes señalada, responden a su abundante uso en la dogmática y en la teoría, y se sustentan sobre la base de tres cuestiones: los objetivos respecto del derecho (mantener, realizar, mejorar), la conducta requerida para salvaguardar el derecho (negativa o positiva), y el momento de cumplimiento (inmediato o progresivo), de tal forma que abarcan cuatro obligaciones: respetar, proteger, garantizar y promover (Serrano y Vázquez, 2013: 59 y 60). La primera obligación (respetar) es la más básica e inmediata, ya que se cumple mediante abstenciones y, *a contrario sensu*, se incumple por acciones, es decir, la obligación consiste en no interferir o poner en peligro los derechos. Por su parte, la obligación de proteger constituye una conducta de carácter positivo para la creación del marco jurídico y las instituciones necesarias para prevenir las violaciones, y en su caso, hacer exigibles los derechos frente a la conculcación de los mismos. Respecto de la obligación de garantía, ésta tiene por objetivo mantener el disfrute de un derecho humano y mejorarlo, de ahí que se trate de una obligación positiva que organice el aparato es-

ARTURO MIGUEL CHIPULI CASTILLO

tatal y asegure la capacidad de disfrute del derecho mediante la remoción de obstáculos y provisión de recursos. Finalmente, la obligación de promover implica el suministro de información sobre los derechos, su ejercicio y exigibilidad, así como las tareas de sensibilización necesarias para que las personas los respeten y los promuevan (Serrano y Vázquez, 2013: 61-81).

58 Por su parte, los elementos institucionales son obligaciones que constriñen la acción gubernamental al momento de diseñar la aplicación de los derechos, y que son fundamentales para la realización del mismo (Serrano y Vázquez, 2013: 83 y 84). Derivado de lo anterior, y siguiendo la línea propuesta por Serrano y Vázquez, dichos elementos son: disponibilidad, accesibilidad, aceptabilidad y calidad. La disponibilidad implica garantizar la suficiencia de los servicios, instalaciones, mecanismos, procedimientos, o cualquier otro medio por el cual se materializa un derecho para toda la población. La accesibilidad involucra la forma de asegurar que los medios por los cuales se materializa un derecho se encuentren al alcance de todos, sin discriminación, y con las posibilidades geográficas y económicas de acceder a ellos. La aceptabilidad refiere que el medio y los contenidos para materializar el derecho sean aceptados por las personas a quienes van dirigidos, lo que conlleva el reconocimiento de especificidades y, consecuentemente, la flexibilidad para modificarlos u adaptarlos. Por último, la calidad implica que los medios y contenidos por los cuales se materializa un derecho aseguren los requerimientos y propiedades necesarios para cumplir con su función (Serrano y Vázquez, 2013: 84-89).

Tomando como base el modelo antes señalado, en el siguiente apartado se advertirá el nivel de cumplimiento de los componentes aplicables al programa de política pública.

3. El PGCM: una revisión desde el estándar internacional

En el cuadro 1 se presentaron los componentes del derecho de acceso a la información pública, de los cuales se han seleccionado cinco, que fungirán como unidades de análisis. Cada uno de estos cinco componentes se desarrolla en el cuadro que a continuación se presenta (cuadro 3). En general, se desarrollan a partir de la obligación de garantizar, que se materializa a través de la conducta positiva del Estado para crear la maquinaria institucional necesaria para la realización del derecho. Empero, y dado que las obligaciones identificadas no nos especifican por sí mismas los extremos de cumplimiento, se recurre a los elementos institucionales para advertir con mayor detalle las medidas concretas que el Estado debe

adoptar para la realización del derecho. De ahí que la primera columna señale el marco obligacional establecido por el DIDH, mientras que en la segunda, se realiza una *checklist* de dichas obligaciones en el marco del PGCM, señalando las acciones concretas respecto de cada uno de los rubros indicados.

Como podrá advertirse, de los cinco grandes objetivos del PGCM, el primero (impulsar un gobierno abierto) es el que pone mayor énfasis en el derecho en estudio. No obstante lo anterior, los otros objetivos del programa, aunque de forma menos objetiva y sin ser su eje medular, también retoman el derecho de acceso a la información, sobre todo en lo que toca a acciones en materia de información presupuestaria o en el acceso a tecnologías de la información.



CUADRO 3
 MAPA DE OBLIGACIONES DEL DERECHO DE ACCESO
 A LA INFORMACIÓN PÚBLICA Y ACCIONES DEL PGCM
 QUE SE VINCULAN

<i>I. Transparencia pasiva</i>		<i>PGCM</i>
<i>Elemento institucional</i>	A) Disponibilidad: i. Establecer una política pública que garantice procedimientos de acceso universal a la información pública, y el derecho a la respuesta.	Sin acciones
	B) Accesibilidad: i. Económica: los procedimientos de acceso a la información no deben tener costo. ii. Física: el procedimiento de acceso a la información debe ser sencillo y abierto.	Sin acciones
	C) Aceptabilidad: i. El procedimiento debe ser culturalmente adecuado. ii. Debe contemplarse la posibilidad de que los procedimientos y la información puedan presentarse en lenguas indígenas y/u otros lenguajes.	Sin acciones
	D) Calidad: i. Las respuestas deben ser oportunas. ii. Las respuestas deben ser completas. iii. Las respuestas negativas deben estar fundadas y motivadas	Acción 1.3.7

ARTURO MIGUEL CHIPULI CASTILLO

60



<i>II. Transparencia activa</i>		<i>PGCM</i>
<i>Elemento institucional</i>	A) Disponibilidad: i. El Estado debe garantizar la máxima cantidad de información de interés público disponible en forma oficiosa al menos sobre los siguientes aspectos: a) Estructura, funciones y presupuesto de operación e inversión del Estado. b) Información que requieren las personas para el ejercicio de otros derechos. c) Oferta de servicios, beneficios, subsidios o contratos de cualquier tipo. Información sobre los procedimientos para interponer quejas o consultas.	Acciones 1.3.1, 1.3.9, 2.4.1, 3.4.1, 4.3.2, 4.3.6, 4.5.6, y 5.2.2.
	B) Accesibilidad: i. Física: el Estado debe encontrar formas eficaces para realizar esta obligación en contextos de falta de acceso a las nuevas tecnologías.	Acciones 1.3.6, 5.6.1, 5.6.2, y 5.6.3
	C) Aceptabilidad: i. Debe contemplarse la posibilidad de presentar la información en lenguas indígenas y/u otros lenguajes.	Sin acciones
	D) Calidad: i. La información debe ser completa. ii. La información debe ser comprensible (lenguaje accesible). iii. La información debe estar actualizada.	Acciones 1.4.9, 1.5.2, 2.4.1, 2.4.2, 3.4.1, y 4.3.6
<i>III. Producción y captura de información</i>		<i>PGCM</i>
<i>Elemento institucional</i>	A) Disponibilidad: i. Debe garantizarse la existencia de lineamientos y procedimientos para la producción de bases de información, indicadores e información estadística, la cual debe ser publicada de manera proactiva por el Estado, incluso en ausencia de solicitudes.	Sin acciones
	B) Calidad: i. El Estado está obligado a crear bases de datos que permitan la validación de indicadores de progreso en materia de derechos económicos sociales, culturales y ambientales (DESCA). ii. El Estado debe producir información estadística desagregada por colectivos vulnerables, excluidos e históricamente discriminados.	

GOBIERNO CERCANO Y MODERNO: UNA MIRADA DESDE LOS ESTÁNDARES...

	iii. Asimismo, queda obligado a realizar la investigación y recopilación de información estadística pertinente sobre las causas, consecuencias y frecuencia de la violencia contra la mujer.	
<i>IV. Gestión adecuada de archivos y documentos</i>		<i>PGCM</i>
Elemento institucional	A) Disponibilidad: i. Estudio preliminar del sistema de gestión de documentos (RTA, 2015: 59) ii. Sistema de mantenimiento, archivo y eliminación de activos de información. iii. Metodología del sistema de gestión de documentos (RTA, 2015: 59)	Acciones 1.7.1, 1.7.2, 1.7.3, 1.7.4, 1.7.5,y 1.7.6
	B) Calidad: i. Modelo de requisitos y especificaciones del sistema de gestión de documentos (RTA, 2015: 59)	Sin acciones
<i>V. Protección de servidores públicos y denunciantes de irregularidades (whistleblowers)</i>		<i>PGCM</i>
Elemento institucional	A) Disponibilidad: i. Existencia de medidas y sistemas para proteger a los funcionarios públicos y ciudadanos particulares que denuncien actos de corrupción (artículos 32, 33 y 37, párr. 4, de la Convención de las Naciones Unidas contra la Corrupción; art. III, puntos 8, 9, 10, 11 y 12 de la Convención Interamericana contra la Corrupción). ii. Medidas y sistemas que faciliten que los servidores públicos denuncien actos de corrupción, que alienten la cooperación del sector privado, de los delincuentes y faciliten una coordinación interinstitucional (artículos 8, párr. 4, 13, párr. 2, 37, 38 y 39 de la Convención de las Naciones Unidas contra la Corrupción).	Acciones 1.2.8, 1.1.10, 1.2.4, 1.2.6, 1.2.7, y 1.2.9
	B) Accesibilidad: i. No discriminación: toda persona debe poder acceder a los mecanismos de protección de denunciantes de irregularidades, sin importar su estatus laboral o jurídico, siempre que la denuncia se haya realizado de buena fe y la información se haya obtenido por vías lícitas. ii. Física: el Estado debe garantizar la existencia de canales abiertos de denuncia.	Sin acciones



ARTURO MIGUEL CHIPULI CASTILLO

62

<i>Elemento institucional</i>	<p>C) Calidad:</p> <p>i. Deben existir mecanismos de protección frente a sanciones legales, administrativas o laborales.</p> <p>ii. Medidas contra represalias, tratos injustificados o intimidación.</p> <p>iii. Debe garantizarse la posibilidad de denunciar de forma anónima.</p> <p>iv. El Estado debe establecer mecanismos de protección de la identidad del denunciante.</p>	Sin acciones
-------------------------------	--	--------------

FUENTE: Elaboración propia.

Como se adelantó en el apartado metodológico, se calificará la incidencia del estándar en una escala de cinco niveles (nulo, bajo, medio, alto y total). A cada uno de estos niveles se les asignará una calificación, que va del 0 al 4, dependiendo del porcentaje de apego a las obligaciones internacionales.

En materia de transparencia pasiva, el programa se acerca al estándar en su punto 1.3.7, consagrando acciones concretas de mejora de los tiempos de respuesta y fomento de la generación de información de calidad, bajo los criterios de veracidad, oportunidad y confiabilidad. Sin embargo, no establece mecanismos o acciones de acceso a la información pública que permitan que las respuestas sobre solicitudes de información sean culturalmente aceptables, o que en ciertas condiciones la entrega de información pueda realizarse conforme a los requerimientos específicos de lengua o situación de discapacidad. En este sentido, la incidencia del estándar es baja (calificación: 1).

Respecto de la transparencia activa, puede advertirse que el cumplimiento del estándar internacional del derecho de acceso a la información pública es alto (calificación: 3), tomando en consideración que los cuatro elementos institucionales advertidos (disponibilidad, accesibilidad, aceptabilidad y calidad) se integran por diez puntos u obligaciones específicos, y el PGCM cumple con seis de estas pautas. Pese a lo anterior, los principales vicios se presentan en el rubro de disponibilidad (estructura y funciones de las entidades públicas, así como información sobre procedimientos de queja o consulta), y aceptabilidad (toda vez que no contempla formas diferenciadas de información).

En cuanto a la producción y captura de información, en el punto 2.1.1 se establece como acción del programa la incorporación de indicadores de los objetivos sectoriales al sistema de evaluación por desempeño (SED); sin embargo, tales indicadores no se encuentran relacionados con el en-

foque de derechos humanos y no dan cumplimiento a los componentes mínimos de calidad señalados por el DIDH: indicadores de avance en materia de DESCAs, información estadística desagregada por colectivos vulnerables, excluidos o históricamente discriminados, o sobre las causas, consecuencias y frecuencia de violencia contra la mujer. En este sentido, si bien el programa establece la obligación de captura y producción de información, ésta no cumple con los elementos del estándar internacional (incumplimiento total: 0).

63

En lo que atañe al componente de gestión de archivos y documentos, el programa incumple con el primer elemento de disponibilidad: la existencia de un estudio previo de la situación del sistema de gestión de documentos. Por lo que respecta a la disponibilidad de reglas, acciones o estrategias tendientes a establecer o mejorar un sistema de mantenimiento, archivo y eliminación de activos de información, el programa consagra acciones tendientes a la consolidación de los sistemas institucionales de archivo y administración de documentos. Con relación a los requisitos de calidad en materia archivística, cabe señalar que no existe propiamente un estándar de gestión de documentos. Empero, la OEA en 2014 se incorporó a la Red de Transparencia y Acceso a la Información (RTA), que cuenta con un modelo de archivos (la norma ISO 15489-1: 2001), el cual sirve de sustento para el diseño e implementación de un sistema de gestión de documentos (RTA, 2016: 53). El programa y sus lineamientos no hacen mención expresa de la norma ISO 15489; sin embargo, dichos documentos sí cumplen con los requerimientos de la norma al menos en tres puntos: archivos de gestión, archivo central y archivos históricos y de valor permanente, los cuales se consagran como elementos necesarios de todo acervo de información oficial con enfoque de DD.HH., de acuerdo con la Oficina del Alto Comisionado de Naciones Unidas para los Derechos Humanos (2015). Cabe observar que los documentos que establecen dichas líneas de gestión de archivos son anteriores al programa y al PND. Derivado de lo anterior, en el citado componente el cumplimiento del estándar internacional es alto (calificación de 3).

Finalmente, con relación al componente de protección de denunciantes de irregularidades, el PGCM observa un nivel de incidencia bajo (calificación: 1), pese a que sí dispone de medidas y/o sistemas para proteger a los funcionarios públicos y ciudadanos particulares que denuncien actos de corrupción. Sin embargo, ni el PGCM ni sus bases de operación ni los indicadores de resultados sostienen criterios, acciones o indicadores que permitan dar cumplimiento a los estándares señalados por la Convención de las Naciones Unidas contra la Corrupción, o la Convención Interame-

ARTURO MIGUEL CHIPULI CASTILLO

ricana contra la Corrupción. Es decir, pese a que se dispone de acciones específicas para la protección de denunciantes de actos de corrupción, dichos mecanismos no cumplen con los elementos de accesibilidad y calidad arriba señalados. Asimismo, es omiso en señalar estrategias concretas para garantizar la denuncia de actos de corrupción.

64

VI. RESULTADOS

Partiendo de lo antes señalado, y tomando en consideración la escala establecida, a continuación se presentan los resultados de cumplimiento del programa en estudio:

-
-
-

CUADRO 4
NIVEL DE CUMPLIMIENTO DEL ESTÁNDAR INTERNACIONAL
POR COMPONENTE

<i>Componente</i>	<i>Calificación</i>
Transparencia pasiva	1
Transparencia activa	3
Producción y captura de información	0
Gestión adecuada de archivos y documentos	3
Protección de servidores públicos y denunciantes de irregularidades (<i>whistleblowers</i>)	1
Total	8

FUENTE: Elaboración propia.

Como es de advertirse, el PGCM en ninguno de sus rubros cumple totalmente con el estándar internacional de acceso a la información pública. Cuenta con dos componentes con cumplimiento alto de las obligaciones (transparencia activa y gestión de documentos); sin embargo, advierte un rubro con niveles críticos de incumplimiento (producción y captura de información), que desatiende totalmente lo señalado por el DIDH. Por su parte, la transparencia pasiva y la protección de denunciantes de irregularidades tienen un cumplimiento bajo del estándar.

Para la calificación total se sumó el puntaje de cada una de las categorías analizadas, a fin de determinar el nivel de cumplimiento del programa. La escala utilizada es la siguiente:

CUADRO 5
ESCALA DE CALIFICACIÓN DEL PROGRAMA

<i>Nivel</i>	<i>Criterio de calificación</i>
Cumplimiento total	20 puntos
Cumplimiento alto	16 a 19 puntos
Cumplimiento medio	11 a 15 puntos
Cumplimiento bajo	6 a 10 puntos
Cumplimiento muy bajo	1 a 5 puntos
Incumplimiento total	0 puntos

65

FUENTE: Elaboración propia.

En ese tenor, y con relación al total del puntaje obtenido respecto del estándar, se puede considerar que el cumplimiento del programa es bajo, ya que de los cinco componentes establecidos solamente dos observaron un cumplimiento alto del estándar internacional, mientras que los tres restantes no se ajustaron a los mandatos internacionales en materia de acceso a la información pública.

VII. CONCLUSIONES

El enfoque de derechos humanos, como directriz de contenido y guía de orientación de las políticas públicas, considera la inclusión de ciertos elementos que permiten, por un lado, el empoderamiento de la persona, y por el otro, el cumplimiento de las obligaciones estatales contenidas en las diversas fuentes que integran al DIDH. Con base en lo anterior, sumado a la construcción de políticas y presupuestos públicos de forma racional, se establecen elementos sustanciales que permiten la adaptación de su contenido a los principios de los derechos humanos.

A raíz de lo arriba señalado, el presente trabajo se centró en el estudio del diseño del Programa para un Gobierno Cercano y Moderno 2013-2018, bajo el citado enfoque de derechos humanos, particularmente respecto del derecho de acceso a la información pública. El PGCM fue una política pública transversal derivada del PND 2013-2018, cuyo objetivo fue el impulso de una administración eficiente, eficaz, innovadora, y orientada a la consolidación de un gobierno abierto.

ARTURO MIGUEL CHIPULI CASTILLO

66 Partiendo de lo antes señalado, y para los efectos del presente trabajo, el estándar internacional del derecho a la información se construyó a partir de las siguientes obligaciones: transparencia pasiva, transparencia activa, producción y captura de información, gestión de archivos y documentos, y protección de denunciantes de irregularidades. Con base en tales elementos, se llevó a cabo el análisis de cumplimiento de las obligaciones del derecho de acceso a la información pública en el diseño del programa de política pública “Programa para un Gobierno Cercano y Moderno 2013-2018”. De ese examen se estableció que la política pública cuenta con un nivel bajo de cumplimiento de las obligaciones que el DIDH ha dispuesto en materia de acceso a la información pública, lo cual pone en evidencia que en el diseño de ese programa no permeó un enfoque de derechos humanos de manera contundente, dejando de lado muchas cuestiones necesarias para el desarrollo efectivo del derecho.

Finalmente, una lectura de los resultados de cada uno de los componentes puede llevarnos a concluir que, pese al énfasis en materia de gobierno abierto, el compromiso político plasmado en el diseño del programa para abatir los vicios en materia de acceso a la información dentro de la APF fue menor, acotado a la transparencia activa y la cultura archivística, y alejado en gran medida de las acciones necesarias para la materialización plena del derecho de acceso a la información.

VIII. FUENTES DE CONSULTA

- ABRAMOVICH, Víctor, 2006, “Una aproximación al enfoque de derechos en las estrategias y política de desarrollo”, *Revista de la CEPAL*, núm. 88, abril.
- CASTILLO, Gloria del y MÉNDEZ, Irma, 2010, *Introducción a la teoría de las políticas públicas*, México, Flacso-México.
- CENTRO LATINOAMERICANO DE ADMINISTRACIÓN PARA EL DESARROLLO (CLAD), 2016, *Carta Iberoamericana de Gobierno Abierto*.
- COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS (CIDH), 2012, *El derecho de acceso a la información en el marco jurídico interamericano*, 2a. ed., Organización de Estados Americanos, disponible en: <https://www.oas.org/es/cidh/expresion/docs/publicaciones/acceso%20a%20la%20informacion%202012%202da%20edicion.pdf>.
- NEGRO, Dante, 2014, “Recientes avances y desafíos en los procesos de reforma de los marcos jurídicos en materia de acceso a la información pública en la región”, *Taller de Alto Nivel. Acceso Equitativo a la Información*

Pública, celebrado en Guatemala los días 27 y 28 de agosto de 2014, OEA, disponible en: http://www.oas.org/es/sla/ddi/docs/acceso_informacion_taller_alto_nivel_guatemala_2014_publicacion.pdf.

OFICINA DEL ALTO COMISIONADO DE NACIONES UNIDAS PARA LOS DERECHOS HUMANOS (OACNUDH), 2015, *Instrumentos del Estado de derecho para sociedades que han salido de un conflicto: Archivos*, HR/PUB/14/4, Ginebra y Nueva York, Naciones Unidas, disponible en: https://www.ohchr.org/Documents/Publications/HR_PUB_14_4_Archives_sp.pdf.

67

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), 1969, Convención Americana sobre Derechos Humanos.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), 1996, Convención Interamericana contra la Corrupción.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), 2004, Declaración Conjunta de los Relatores para la Libertad de Expresión sobre Acceso a la Información y sobre la Legislación que Regula el Secreto, disponible en: http://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), 2008, Principios sobre el Derecho de Acceso a la Información, CJI/RES. 147 (LXXIII-O/08), disponible en: http://www.oas.org/es/sla/ddi/docs/CJI-RES_147_LXXIII-O-08.pdf.

ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), 2010, *Declaración Conjunta de los Relatores para la Libertad de Expresión sobre Wikileaks*, disponible en: http://www.oas.org/es/cidh/expresion/documentos_basicos/declaraciones.asp.

ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU), 1948, Declaración Universal de los Derechos Humanos.

ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU), 1966, Pacto Internacional de Derechos Civiles y Políticos.

ORGANIZACIÓN DE LAS NACIONES UNIDAS (ONU), 2003, Convención de las Naciones Unidas contra la Corrupción.

PARSONS, Wayne, 2007, *Políticas públicas. Una introducción a la teoría y la práctica del análisis de políticas públicas*, México, FLACSO-México.

RED DE TRANSPARENCIA Y ACCESO A LA INFORMACIÓN (RTA), 2014, *Modelo de Gestión de Documentos y Administración de Archivos para la Red de Transparencia y Acceso a la Información*, disponible en: http://mgd.redrta.org/mgd/site/artic/20150123/asocfile/20150123093820/mg_modelo_general.pdf.

ARTURO MIGUEL CHIPULI CASTILLO

ROSSI, Julieta y MORO, Javier, 2014, *Ganar derechos. Lineamientos para la formulación de políticas públicas basadas en derechos humanos*, Buenos Aires, Instituto de Políticas Públicas en Derechos Humanos del Mercosur.

SALAZAR, Pedro, 2014, “Capítulo 7. La reforma y las políticas públicas”, en SALAZAR, Pedro (coord.), *La reforma constitucional sobre derechos humanos: una guía conceptual*, México, Instituto Belisario Domínguez.

68 SERRANO, Sandra y VÁZQUEZ, Daniel, 2013, *Los derechos en acción. Obligaciones y principios de derechos humanos*, México, Flacso-México.

●
○
●
Marco jurídico

Caso Claude Reyes y otros vs. Chile. Corte Interamericana de Derechos Humanos, sentencia del 19 de septiembre de 2006.

Caso Gomes Lund y otros (Guerrilha do Araguaia) vs. Brasil. Corte Interamericana de Derechos Humanos, sentencia del 24 de noviembre de 2010.

Programa para un Gobierno Cercano y Moderno (PGCM), 2013, México, *Diario Oficial de la Federación*, 30 de agosto de 2013.

EL EFECTO TRANSFORMADOR DE LA TENSION ENTRE DEMOCRACIA, LIBERTAD DE EXPRESIÓN E INFORMACIÓN Y DIGNIDAD INDIVIDUAL DURANTE EL CORREATO

THE TRANSFORMATIVE EFFECT OF THE TENSION BETWEEN DEMOCRACY, FREE SPEECH & INFORMATION AND INDIVIDUAL DIGNITY DURING RAFAEL CORREA'S ADMINISTRATION

• ○ •

*María Fernanda COBO MANTILLA**

RESUMEN: El artículo sugiere que el gobierno de Rafael Correa creó una tensión entre democracia, libertad de expresión e información y dignidad individual utilizando la fuerza del Estado, desde su dimensión ejecutiva, judicial y legislativa, para neutralizar, modificar o eliminar un poder de dominio: los medios de comunicación privados y la voz civil.

PALABRAS CLAVE: libertad de expresión e información, dignidad, democracia, censura.

ABSTRACT: The article suggests that Rafael Correa's administration created a tension between democracy, free speech & information and individual dignity by using the State force, on its executive, judicial and legislative dimension, to neutralize, modify or eliminate private media and civil voice.

KEY WORDS: *free speech & information, dignity, democracy, censorship.*

* Maestra en derechos humanos por la Universidad Iberoamericana (UIA); especialista en gobierno, gerencia y asuntos públicos. Actualmente es profesora de periodismo digital en UIA. Correo: mariafernandacobom@gmail.com.

Fecha de recepción: 21 de febrero de 2019.

Fecha de dictamen: 28 de marzo de 2019.

MARÍA FERNANDA COBO MANTILLA

Vamos a luchar con toda nuestra fuerza contra estos cobardes, sicarios de tinta y contra sus mentiras, ladre quien ladre, basta de tantas mentiras.

Rafael CORREA DELGADO

Presidente constitucional de la República del Ecuador, 2007-2017

70

I. INTRODUCCIÓN

El Ecuador, durante la década de 2007 a 2017, vivió una constante tensión entre democracia, libertad de expresión¹ e información y dignidad individual. Dicha tensión se convirtió en el eje central del discurso político del gobierno constitucional de Rafael Correa, identificando a los medios de comunicación como la principal fuerza de oposición, ante la fragilidad y fragmentación de los partidos políticos del país; oposición que obedecería a una visión del poder político desde la estructura social, donde los medios de comunicación privados constituyen poderes fácticos con la capacidad de influir directa o indirectamente en la toma de decisiones por encima de las instituciones democráticas (Serrano y Vázquez, 2013: 185-232). Así, esta tensión política generada durante la década del correato provocó una transformación de los medios de comunicación en el país y el empoderamiento de su voz civil.

Dos derechos conviven en esta tensión política: por un lado, la libertad de expresión e información, que constituye la esencia de la dimensión social del ser humano, reflejada en el bien común de la opinión pública; y por otro, la dignidad de la persona, que representa la autonomía de valor

¹ La libertad de expresión es un derecho fundamental reconocido en la Declaración Americana sobre los Derechos y Deberes del Hombre; en la Convención Americana sobre Derechos Humanos; en la Declaración Universal de Derechos Humanos; en la Resolución 59 (I) de la Asamblea General de las Naciones Unidas; en la Resolución 104 adoptada por la Conferencia General de la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO); en el Pacto Internacional de Derechos Civiles y Políticos, así como en otros instrumentos internacionales. El Ecuador ratificó la Convención Americana sobre Derechos Humanos el 12 de agosto de 1977. La Constitución del Ecuador, en su artículo 1o., señala: “El Ecuador es un Estado constitucional de derechos...”, y en el artículo 16: “Todas las personas, en forma individual o colectiva, tienen derecho a: 1. Una comunicación libre, intercultural, incluyente, diversa y participativa, en todos los ámbitos de la interacción social, por cualquier medio y forma, en su propia lengua y con sus propios símbolos”.

humano, reflejada en el bien individual del honor y la reputación,² dos pilares fundamentales de la democracia que obedecen a la realidad natural del convivir social, y que al mismo tiempo se fortalecen con el ejercicio efectivo de los derechos para transformar las condiciones de vida de la sociedad.

Frente a esta tensión entre los dos derechos (entre el bien colectivo y el bien individual) entra en acción el Estado como articulador de este juego de fuerzas, donde el principio de justicia se instrumentaliza a través del justo equilibrio entre los poderes Ejecutivo, Legislativo y Judicial. Un equilibrio que sostiene la legalidad del poder en el sistema democrático como garante³ del respeto de los derechos humanos y sus límites. La transgresión de este equilibrio desde la fuerza del Estado constituye la realidad política del Ecuador durante la década del correato,⁴ donde a mayor intervención del poder, mayor intensidad de censura⁵ y autocensura vive la prensa⁶ y la sociedad civil. Mientras mayor es el reclamo de la dignidad del “ciudadano-presidente”, mayor es la demanda de transparencia e impunidad por parte de la prensa y la voz civil.

A través de un análisis en perspectiva de la política de Estado del gobierno de Rafael Correa frente a la libertad de expresión e información y la dignidad individual, se transitará por las distintas intensidades de esta lucha de fuerzas, donde modificar, eliminar o neutralizar a la contraparte

² Convención Americana sobre Derechos Humanos, “Art. 13... 2. El ejercicio del derecho previsto en el inciso precedente no puede estar sujeto a previa censura sino a responsabilidades ulteriores, las que deben estar expresamente fijadas por la ley y ser necesarias para asegurar: a. el respeto a los derechos o a la reputación de los demás, o b. la protección de la seguridad nacional, el orden público o la salud o la moral pública”.

³ Luigi Ferrajoli califica al modelo garantista de la democracia constitucional como el sistema que da legitimidad del orden político, a través de la tutela y efectividad de los principios y derechos fundamentales, cuya incorporación en el nivel constitucional asigna a la jurisdicción (el juez y la ley) una función de garantía del ciudadano frente a las violaciones de cualquier nivel de la legalidad por parte de los poderes públicos (Ferrajoli, 2016: 26).

⁴ El correato es entendido con el sufijo que indica dignidad, cargo o jurisdicción; por ejemplo, generalato, o bien se trata del tiempo durante el que se ocupa este cargo o dignidad; por ejemplo, califato. Es un debate abierto hablar de correísmo, donde el sufijo “ismo” identificaría a Rafael Correa como el representante de un movimiento, una teoría política, un sistema, o bien una doctrina.

⁵ La censura previa supone el control y veto de la información antes de que ésta sea difundida, impidiendo tanto al individuo, cuya expresión ha sido censurada, como a la totalidad de la sociedad, ejercer su derecho a la libertad de expresión e información. El artículo 13 de la Convención Americana explícitamente prohíbe la censura previa.

⁶ Los principios de la Declaración de Chapultepec constituyen un documento básico que contempla las garantías y la defensa de la libertad de expresión, la libertad e independencia de la prensa y el derecho a la información.

MARÍA FERNANDA COBO MANTILLA

constituirá el efecto transformador de los medios de comunicación y las demandas sociales del Ecuador.

Lo anterior se refleja en la clasificación mundial de la libertad de prensa, publicada por Reporteros sin Fronteras (2018), donde el Ecuador ascendió trece puestos en 2018, ocupando la posición 92. De acuerdo con el informe, esta mejoría obedece al cambio de gobierno, que permitió calmar las tensiones entre el gobierno de Rafael Correa y los medios de comunicación privados.

Epistemológicamente, este análisis se sostiene en la dimensión tridimensional del derecho, donde los principios, la norma y los hechos interactúan en el ejercicio progresivo del derecho a la libertad de expresión e información como un efecto transformador de la democracia en el Ecuador.

II. DEMOCRACIA, LIBERTAD DE EXPRESIÓN E INFORMACIÓN Y DIGNIDAD INDIVIDUAL

La democracia constituye el escenario natural del ejercicio del derecho a la libertad de expresión e información. El liberalismo pondrá en el centro a la autonomía de la persona ante el poder del Estado, que a su vez será un garante de esta autonomía. “El Estado es, entonces un mal necesario al que limitar en pos de la libertad de las personas, que entendidas como agentes morales autónomos, hay que preservar de la interferencia del poder” (Bobbio, 1989: 17).

Por su parte, el republicanismo pondrá en el centro la vida pública como garante del desarrollo del Estado. Así, el “rechazo de la tiranía de toda forma de dominación, la reivindicación del estado libre, cuya fórmula para limitar la dominación es la participación activa de los ciudadanos en la vida pública, de lo público, o en otras palabras la virtud cívica” (Gargarella, 2005: 163). En este sentido, el ciudadano expresa activamente su virtud cívica a través del ejercicio de sus derechos.

Desde la visión del comunitarismo, el reconocimiento de la diversidad cultural constituye el centro de diálogo social en el orden público. “Las personas son plenamente libres cuando logran el reconocimiento simbólico de los otros como iguales. Lo importante no sólo es ser ciudadanos de una misma comunidad política, sino obtener el reconocimiento de diferentes grupos como simbólicamente iguales sin desconocimiento de las diferencias” (Taylor, 1993: 55). Así, la neutralidad del Estado se ejercerá a través del reconocimiento no sólo de la igualdad, sino también de la diferencia.

El marxismo tradicional identificará al Estado como un mecanismo de control y dominación. La tensión entre clases sociales y propiedad será el eje articulador del orden social, donde “es necesario utilizar el derecho como uno de los medios de lucha por el socialismo, como uno de los medios para transformar la sociedad humana sobre las bases socialistas” (Hernández Gil, 1970: 53). Su visión contemporánea identifica en los derechos fundamentales un potencial transformador de la construcción de los espacios democráticos (Luckes, 1981: 1). Entonces, el ejercicio de los derechos constituye una oportunidad para estimular demandas sociales.

En el sistema democrático de valores y derechos, la dignidad (al ser inherente a la persona) constituye un principio transversal más allá de su contexto social y político, donde la valoración de la existencia de la persona se integra al derecho del ser humano como fuerza de ley para garantizar su existencia y autonomía; es decir, el libre desarrollo de su personalidad.

Para Kant, el respeto a la dignidad de la persona constituye un imperativo categórico intangible, al señalar: “en el reino de los fines todo tiene o un precio o una dignidad. Lo que tiene un precio, en su lugar puede ponerse alguna otra cosa como equivalente; lo que, en cambio, está por encima de todo precio y, por lo tanto, no admite equivalente alguno, eso tiene una dignidad” (Kant, 2016: 115).

La doctrina alemana convertirá a la dignidad en un derecho accionable dentro de la operatividad jurídica a través de su delimitación susceptible a un proceso de valoración ponderada, donde a partir del reconocimiento de la dignidad como valor intangible, respetarla y protegerla es una obligación del poder público. Así, la Ley Fundamental de la República Federal de Alemania señala en su artículo primero que toda persona tiene el derecho al libre desarrollo de su personalidad siempre que no viole los derechos de otros ni atente contra el orden constitucional o la ley moral.

La dignidad exige reciprocidad a través de un consenso social. De acuerdo con Hofmann (citado en Gutiérrez, 2005: 56):

La dignidad se constituye... en el reconocimiento, a través de la valoración positiva de pretensiones sociales de respeto. En sentido jurídico la dignidad es necesariamente... un concepto que atañe a relaciones humanas o a la comunicación. La dignidad debe ser comprendida como una categoría propia de la disposición del individuo a convivir... En consecuencia, la dignidad no puede ser pensada al margen de una concreta comunidad de reconocimiento recíproco.



MARÍA FERNANDA COBO MANTILLA

Un reconocimiento de la dimensión subjetiva de la persona donde el honor y la reputación determinan el límite cuando se ejerce el derecho a la libertad de expresión.

74 En la doctrina jurídica suele hablarse del honor en dos sentidos: subjetivo y objetivo. El honor en sentido subjetivo es el sentimiento de nuestra propia dignidad; el honor en sentido objetivo es el reconocimiento que de esa dignidad hacen los demás. El primero es la propia estimación; el segundo la buena reputación (Gutiérrez, 2005: 840).

● La dinámica entre ciudadano y Estado dentro de un orden político
○ democrático crea una relación entre autonomía, autodeterminación y dig-
● nidad que, a través del ejercicio de los derechos humanos, construye trans-
formaciones sociales con un vínculo jurídico que se debate entre la regu-
lación y la institucionalidad, y que a su vez se fortalece con el monitoreo y
control de la comunidad nacional e internacional.

El ciudadano, al tener conciencia de sus derechos, construye un proceso que se transforma con el tiempo: sus demandas evolucionan de ser individuales a ser sociales; el agravio se vive como un problema particular para luego ser general. El ejercicio del derecho transita entonces desde una experiencia individual hacia una vivencia colectiva de justicia social.⁷

Esta tensión entre Estado y ciudadano, al demandar un derecho, busca ante todo transformar un poder de dominio que se articula en diferentes intensidades: neutralizar, modificar o eliminar a la contraparte. Estas intensidades son las que marcaron la interacción entre el gobierno del Ecuador y los medios de comunicación en torno al derecho de la libertad de expresión e información y el derecho a la dignidad individual.

III. PODER EJECUTIVO: LA CENSURA OFICIAL

De acuerdo con Reporteros Sin Fronteras (2018), la Sociedad Interamericana de Prensa (SIP) y Knight Center of Journalism in the Americas, en 2008 se reportaron en Ecuador veintidós amenazas directas (agresión, amenazas y encarcelamiento) a la prensa, y durante 2009 el número se elevó a 103. En 2015 se reportaron más de 370 incidentes solamente de hostigamiento verbal, físico o legal hacia los medios de comunicación, perpetrados por au-

⁷ Es importante considerar que esta construcción social a partir de una demanda individual es compleja y muy poco analizada; sin embargo, puede considerarse un valor diferencial en el efecto transformador que busca la defensa de los derechos humanos.

toridades y ciudadanos ecuatorianos, lo que representa un incremento con relación a los 254 incidentes presentados en 2014.

La demanda de libertad de expresión e información generó diferentes reacciones por parte de sus actores sociales, que se movieron entre la represión, la negación y la concesión retórica, dejando fuera toda posibilidad de negociación, lo cual marcó la transición del gobierno de Rafael Correa de la democracia participativa hacia el control del autoritarismo.

Este autoritarismo se refleja, por ejemplo, en la estrategia digital de comunicación del gobierno del Ecuador, donde

75

El 74% de los tuits y retuits registrados busca desmentir noticias, atacar y criticar los contenidos de los medios de comunicación, recurso que hemos denominado “*verdad absoluta, verdad oficial*”. El recurso de la “*doble moral*” está presente en el 12% de tuits donde se asegura que la prensa utiliza un doble discurso en la información que difunde; un 8% son “*agravios puros y duros*” contra medios privados; un 1,08% de tuits se utiliza el recurso del “*dónde están, qué dirán*” con el cual se ironiza sobre las reacciones de organismos y organizaciones sociales sobre el trabajo de la prensa (Arias y Guerrero, 2016: 1-10).

Una estrategia que generó un debate en dos direcciones: por un lado, la búsqueda de protección a funcionarios públicos, y en general a quienes cuentan con el poder para investigar sus actos alentando a una administración pública fuera del alcance del escrutinio de los medios, y por otro, el poner límites a los excesos de los medios de comunicación y sancionarlos (Arcos, 2014: 15-17), sanción que se remite a la obra de Foucault, *Vigilar y castigar* (2018), en la cual se identifican tres grandes transformaciones del poder de castigar en el tiempo: 1) como un derecho monárquico, donde el castigo es un ceremonial de soberanía; 2) como una concepción preventiva, utilitaria, correctiva, donde el individuo es sujeto de derecho para recalificarlo para su interacción social; 3) como un derecho del orden social, donde el castigo es institucionalizado como técnica de coerción.

Es así como la gobernanza en el país es controlada por el Poder Ejecutivo. La oposición de los partidos políticos, que por otra parte no es leal con el sistema ni con la idea de democracia representativa, deja prácticamente de existir, y la imagen de un caudillo concentra en torno a su personalidad las capacidades gubernamentales, convirtiéndolo en el actor oficial central en esta tensión entre Estado y medios de comunicación.

En la publicidad oficial del gobierno se refleja un protagonismo, al identificar un mecanismo indirecto y sutil para debilitar económicamente a determinados medios de comunicación, y al mismo tiempo concentrar en los medios oficiales, no sólo fondos públicos, sino un contenido en tor-

MARÍA FERNANDA COBO MANTILLA

no a la figura presidencial, que constituyó a la vez su principal plataforma propagandista.

La publicidad estatal no puede ser propaganda encubierta de quienes controlan el gobierno o de sus intereses, ni debe ser utilizada para la estigmatización de sectores opositores o críticos del gobierno... publicitarios nunca deben ser distribuidos discriminando, positiva o negativamente de acuerdo a la línea editorial de los medios de comunicación (CIDH, 2010a:15).

76

De acuerdo con registros del Servicio de Contratación Pública, el gobierno asignó, entre enero y septiembre de 2015, un promedio de 386 mil dólares diarios en servicios para promocionar su imagen, difundir actividades o campañas y defender propuestas (*El Universo*, 2015).

El control institucional de los medios de comunicación fue una de las principales estrategias del gobierno para fortalecer su política de Estado en contra de los monopolios⁸ privados de los medios de comunicación:

A partir del 2007, desde la presidencia, Correa inició un proceso de reestructuración y democratización del sistema de medios del país con el fin de terminar con la, por él denominada, anarquía mediática. El objetivo del gobierno es acabar con los monopolios de empresas de comunicación privadas pertenecientes a la arraigada élite financiera y empresarial. La fundación de medios estatales, la expropiación y el control de medios privados, así como el fomento del sector comunitario son factores que contribuyen a la competencia en el sector de la comunicación (Gehrke *et al.*, 2016: 8).

Un juego de fuerzas entre medios privados que representan la oposición y medios públicos condicionados por el discurso oficial para mantener la tensión política en torno a la figura presidencial.

⁸ De acuerdo con la Comisión Interamericana de Derechos Humanos, en su Declaración de Principios sobre la Libertad de Expresión “los monopolios u oligopolios en la propiedad y control de los medios de comunicación deben estar sujetos a leyes antimonopólicas por cuanto conspiran contra la democracia al restringir la pluralidad y diversidad que asegura el pleno ejercicio del derecho a la información de los ciudadanos”.

Por su parte, la Comisión Interamericana de Derechos Humanos, en su Declaración Conjunta sobre la independencia y la diversidad de los medios de comunicación en la era digital, del 2 de mayo de 2018, señala que “los Estados deben establecer requisitos estrictos de transparencia para la propiedad de los medios de comunicación, junto con normas y sistemas eficaces para evitar los monopolios y la concentración indebida o la propiedad cruzada de los medios. Se debe requerir la aprobación de órganos reguladores independientes antes que puedan realizarse fusiones o adquisiciones que planteen una amenaza a la libre competencia o a la diversidad. Estos requisitos podrían incluir límites a la concentración de los medios de comunicación o la propiedad cruzada de los mismos”.

IV. PODER JUDICIAL: CASO *EL UNIVERSO*

El agravio contra medios de comunicación privados constituye uno de los principales recursos políticos que el gobierno de Rafael Correa institucionizó en su lucha contra la prensa y la libertad de expresión e información al crear auténticos detonantes jurídicos para vitalizar su discurso político.

La columna de opinión “No a las mentiras”, de Emilio Palacio, el 6 de febrero de 2011 en el diario *El Universo*,⁹ dio lugar a que el presidente Correa acusara al periodista y a los directivos del medio de comunicación a través de un juicio donde la Corte Nacional de Justicia del Ecuador dictó una sentencia condenatoria a tres años de prisión y al pago de cuarenta millones de dólares por concepto de daños y perjuicios por la comisión del delito de injuria calumniosa grave a la autoridad.¹⁰

77

La acusación endilgada a los directivos del diario y a la empresa que lo edita la “responsabilidad coadyuvante” en la publicación de este artículo de opinión, suscrito por Emilio Palacio, algo impensable en una democracia moderna y contrario a la Constitución de Montecristi, de 2008, que expresamente reconoce la cláusula de conciencia y prohíbe la censura previa. La acusación les endosaba esa responsabilidad porque los directivos no habían aplicado una censura previa a la opinión de Palacio. Y así mismo, pretendía poner límites a la opinión y al derecho del columnista a la irreverencia y al desacato, sin lo cual es imposible imaginar una opinión genuinamente libre, circunscrita a la ética periodística, a la veracidad y al sentido común (Cornejo, 2013: 13-20).

Aunado a la idea anterior, Romero Parducci señala:

Cuando ocurre que en el ejercicio periodístico se afectan derechos de terceros, las sanciones deben procesarse por la vía civil y deben ser decididas por jueces independientes y probos, ese es el camino que conduce a sentencias imparciales. Pero, en este caso, la vía escogida fue la penal y los jueces, sospechosos de servilismo (Romero Parducci, 2013:15).

⁹ *El Universo* fue fundado en 1921, es editado en Guayaquil y administrado por una empresa familiar. Se le considera el diario independiente más importante del Ecuador por su circulación, y uno de los más influyentes en la opinión pública.

¹⁰ Los funcionarios públicos están sujetos a un mayor escrutinio por parte de la sociedad. Las leyes que penalizan la expresión ofensiva dirigida a funcionarios públicos generalmente conocidas como “leyes de desacato” atentan contra la libertad de expresión y el derecho a la información.

MARÍA FERNANDA COBO MANTILLA

Por su parte, Emilio Palacio y los directivos del diario *El Universo* sostienen que

78 Las condenas impuestas son contrarias a las obligaciones internacionales del Estado en materia de derechos humanos, especialmente el derecho a la libertad de expresión; se enmarcan en un contexto de falta de independencia del Poder Judicial y demuestran la ‘sistematicidad’ por la cual el Estado de Ecuador utiliza el poder público para perseguir a periodistas y así censurarlos (CIDH, 2015).

● Sobre la falta de independencia del Poder Judicial, Barragán Romero
○ señala lo siguiente:
●

Lo ocurrido en las audiencias de las dos instancias confirma que el señor Correa actuó en ellas como presidente y no como ciudadano: se sumaron las medidas de autoridad que dictó al señalar las fechas de las audiencias, y al disponer quiénes podían estar en ellas y quiénes no. Coincidió con estas actuaciones excepcionales el cambio de magistrados y el temor de otros a ser reemplazados. Por último, ‘el ciudadano-presidente’ obtuvo que se acogiera su cuantiosa demanda en una sentencia de validez cuestionable (Barragán Romero, 2011: 17).

La sistematicidad en la persecución del diario *El Universo* se evidencia en los diferentes discursos políticos del Poder Ejecutivo. El presidente Rafael Correa, de forma directa, atacó a través del Enlace ciudadano, del 28 de mayo de 2011, al diario *El Universo*, aseverando que eran una *porquería, mala fe, sinvergüenzas, mentirosos, ignorantes, bestias, enemigos personales*, entre otras expresiones que instigan al odio en el convivir social, creando un clima de hostigamiento y discriminación en el ejercicio del derecho de la libertad de expresión.

En 2008, el presidente Correa atribuyó al diario *El Universo*, que no pagaba impuestos, exponiendo que “no caigan en las garras de los tramosos, muchos de ellos, medios de comunicación que no pagan impuestos. ¡Sinvergüenzas!”. También los habría acusado de corruptos: “así es la corrupción, así es la desinformación de medios de comunicación corruptos. Ya señores, no se dejen insultar por este periódico, por este periodicocho; una vergüenza” (CIDH, 2015: 20).

En 2010, el presidente indicó, refiriéndose al diario *El Universo*, “esta es la prensa libre. En verdad es la prensa buitre. No es que denuncia la carroña, la putrefacción, la genera, la crea, porque de eso vive, de esa ca-

roña, de esa putrefacción, de esa pestilencia. No le creamos nada a esa prensa buitre, compatriotas” (CIDH, 2015).

Un efecto natural en el desarrollo del conflicto entre libertad de expresión e información y dignidad individual en el Ecuador es su internacionalización, impulsada principalmente por la confirmación de la condena a un pago de treinta millones de dólares y tres años de cárcel para Emilio Palacio, Carlos, César y Nicolás Pérez; y un pago de diez millones de dólares a la Compañía Anónima El Universo, por parte de la Corte Nacional de Justicia del Ecuador, el 16 de febrero de 2012 (CIDH, 2015).

Esta condena generó medidas cautelares dictadas el 21 de febrero de 2012, a favor del señor Emilio Palacio Urrutia y de los tres hermanos Pérez, por la Comisión Interamericana de Derechos Humanos (CIDH) de la Organización de los Estados Americanos (OEA). Al respecto, Rafael Correa señaló:

En definitiva, con su espíritu de ONG la CIDH pretende que los Estados siempre sean sospechosos, las autoridades públicas tengamos menos derechos humanos que los demás ciudadanos, los periodistas y medios no tengan ni siquiera responsabilidad ulterior,¹¹ todo lo cual atenta expresamente contra la Convención Interamericana de Derechos Humanos, que es lo vinculante para los Estados, y no, repito, las opiniones de la CIDH (Correa, 2012).

La persecución política del gobierno de Correa obligó a los hermanos Pérez a solicitar asilo¹² político a Panamá, y a Emilio Palacio a Estados Uni-

¹¹ Las responsabilidades ulteriores se encuentran reguladas en el artículo 13 de la Convención Americana sobre Derechos Humanos, y sólo proceden de manera restringida cuando fuere necesario para asegurar el respeto de los derechos o la reputación de otros. “La restricción de la posibilidad de establecer responsabilidades ulteriores se dispone como garantía de la libertad de expresión evitando que ciertas personas, grupos, ideas o medios de expresión queden a priori excluidos del debate público”. La legitimidad no constituye un concepto vacío que los Estados pueden determinar libre o arbitrariamente, sino que configuran lo que la doctrina jurídica conoce como conceptos jurídicos indeterminados. Éstos consisten en conceptos cuyo contenido debe ser predecible, utilizando las reglas de la razonabilidad y la sana lógica, y cuya interpretación en definitiva sólo permite una solución justa.

¹² La Declaración Americana de los Derechos y Deberes del Hombre de 1948 incluyó el derecho al asilo en su artículo XXVII, en que se reconoce el derecho individual de buscar y recibir asilo en las Américas. Este desarrollo fue seguido a ámbito universal con la adopción en 1948 de la Declaración Universal de los Derechos Humanos, en la cual “el derecho de buscar asilo, y a disfrutar de él, en cualquier país”, fue explícitamente reconocido en el artículo 14. A partir de ese momento, el asilo se empezó a codificar en instrumentos de derechos humanos, y no sólo en tratados de naturaleza netamente interestatal.



MARÍA FERNANDA COBO MANTILLA

dos. “El máximo tribunal de justicia de Ecuador debe mostrar que es independiente del Poder Ejecutivo y revocar esta sentencia vergonzosa. En las dictaduras, quien ofende o critica al dictador se va a la cárcel o al exilio”. “En Ecuador, quien ofende o critica al presidente Correa no solamente se va a la cárcel o al exilio, sino que también se va a la quiebra”, afirmó en una carta enviada al magistrado Thor Halverssen, presidente de Human Rights Foundation (HRF, 2011).

80

La presión internacional llevó al gobierno de Rafael Correa dar un giro en su posición a través de la concesión retórica del perdón, declarando lo siguiente:

●
○
● Aunque sé que muchos quieren que no se haga ninguna concesión a quienes no la merecen, así como tomé la decisión de iniciar este juicio, he decidido ratificar algo que hace tiempo estaba decidido en mi corazón: perdonar a los acusados, concediéndoles la remisión de las condenas que merecidamente recibieron, incluyendo a la compañía El Universo... Hay perdón, pero no olvido. Tenemos que aprender del presente y de la historia... esperamos que los injuriados dejen de mostrarse como víctimas, no les queda bien ese papel, no les cabe ese papel (Correa, 2012).

Esta concesión táctica en el discurso oficial llevó a Ecuador a reposicionar internacionalmente al gobierno de Rafael Correa como un protector de la libertad de expresión, aunado a la concesión de asilo político a Julian Assange, fundador de *WikiLeaks*, el 29 de junio de 2012 en la embajada del Ecuador en Londres.

El gobierno del Ecuador consideró lo siguiente:

1) Que Julian Assange es un profesional de la comunicación galardonado internacionalmente por su lucha a favor de la libertad de expresión, la libertad de prensa y de los derechos humanos en general; 2) Que el señor Assange compartió con el público global información documental privilegiada que fue generada por diversas fuentes, y que afectó a funcionarios, países y organizaciones; 3) Que existen serios indicios de retaliación por parte del país o los países que produjeron la información divulgada por el señor Assange, represalia que puede poner en riesgo su seguridad, integridad, e incluso su vida (Declaración del Gobierno del Ecuador, 2012).

En contraparte, la comunidad universitaria internacional, a través de la Universidad de Columbia, otorgó el 25 de octubre de 2012, una mención especial al diario *El Universo* en la 74 edición de los premios de periodismo María Moors Cabot, donde se declaró lo siguiente:

Entre los enemigos más siniestros de la libertad de prensa en América Latina están las leyes de difamación, que permiten a jueces enviar a periodistas a la cárcel por difamar a una persona o corporación. Varios países ya no permiten esta legislación; sin embargo, uno de los que más usan esta ley es Ecuador, donde el liderazgo reciente parece enamorado del poder de enviar a prisión a periodistas que están en desacuerdo con el partido gobernante (*El Univiso*, 2012).

Este enfrentamiento abierto entre gobierno y medios de comunicación ha tenido en Ecuador una reformulación constante con el fin de mantener la tensión en el conflicto y sostener el discurso de oposición política por parte del Ejecutivo contra la prensa.

81

V. TRANSFORMACIÓN DE LOS MEDIOS DE COMUNICACIÓN Y LAS DEMANDAS SOCIALES

En este contexto, los medios de comunicación se fragmentan entre prensa tradicional y prensa emergente. Mientras la prensa tradicional responde ante las demandas judiciales por injurias calumniosas contra la autoridad y fundamenta su defensa jurídica en el derecho a la libertad de expresión y las garantías judiciales, tanto en el sistema de justicia interno como internacional, la prensa emergente encuentra en el escenario digital la nueva arena de movilización social.

Surgen así nuevos medios de comunicación con capacidad de agencia para construir demandas en torno a la libertad de pensamiento, información y expresión, con un cierto grado de autonomía. A continuación se mencionan algunos ejemplos.

La plataforma informativa *4Pelagatos* fue creada en enero de 2016, e inspirada por el manifiesto de Albert Camus de 1939 sobre la lucidez, la desobediencia, la ironía y la obstinación. Su nombre se atribuye a Rafael Correa, al referirse a protestas y movilizaciones de grupos indígenas y sindicalistas. Se caracteriza por describir e investigar la realidad de la sociedad y contribuir a anticipar y diseñar su futuro. Busca ser un medio que sirva de herramienta para la sociedad y para que los poderes se miren sin autoindulgencias. Repudia cualquier tipo de censura y busca ser un espacio democrático, auspiciando la expansión de los derechos de las minorías y propone la convivencia con mayor equidad. Cuenta con 2.4 millones de visitas, y han creado 12.2 millones de páginas; 68% de sus visitantes son lectores permanentes; han recibido 18,500 comentarios, con un promedio de 50.5 por día. Tienen 7.4 millones de sesiones (*4Pelagatos*, 2018).

MARÍA FERNANDA COBO MANTILLA

“En redes sociales fuimos el medio más denunciado y acosado por el aparato de censura del gobierno. Fuimos *hackeados* y sacados del aire por ataques cibernéticos. Y los pelagatos fuimos víctimas de hostigamiento y amenazas que provenían directamente de la oficina de Carondelet” (*4Pelagatos*, 2018).

CrudoEcuador, página de sátira política en Facebook y Twitter a través de memes, fue creada en julio de 2012. Se caracteriza por ser un sitio de opinión y libre expresión con toque humorístico y sarcástico. En su descripción señala que todo está manipulado, todo es ficticio y aumentado. Cuenta con más de 302,000 seguidores.

82

●
○
● En la *Sabatina* de enero de 2015, Rafael Correa se refirió a *CrudoEcuador* de la siguiente manera: “Vamos a ver si cuando salgan del anonimato siguen siendo tan jocosos”. Ante la amenaza oficial, *CrudoEcuador* respondió: “Estos días meditaré bien si continúo o no con esta página, por un lado está mi tranquilidad y la de mi familia, pero por otro lado sería dar la razón a los que no tienen razón y dejar callar mi opinión” (*CrudoEcuador*, 2015).

Fundamedios es una fundación creada en 2006. Nace como un grupo multidisciplinario (no sólo integrado por periodistas, sino por arquitectos, antropólogos, economistas, entre otros) para establecer un diálogo claro y directo entre el periodismo y la ciudadanía, así como para abrir las discusiones y líneas de acción en un ámbito regional, no sólo en Ecuador. Desde mayo de 2007 está enfocada en la defensa de la libertad de expresión, así como en la observación e investigación del contenido de los medios.

César Ricaurte, director de *Fundamedios*, señala lo siguiente:

Nuestro trabajo no ha sido sencillo. Somos una organización de la sociedad civil que ha conseguido ubicar el tema de los derechos y libertades fundamentales en la agenda de discusión pública. Creo que antes muy pocos sospechaban que había una Convención Americana de Derechos Humanos, una Relatoría Especial de Libertad de Expresión, informes, parámetros y estándares de Libertad de Expresión que los países están obligados a cumplir. De alguna forma eso ha dado bases para un debate, porque se corre el riesgo de pensar que esto es una guerra entre medios y gobierno y se deja de lado el sentido real: esto es defensa de derechos. Sin *Fundamedios* esto se quedaba en un asunto solo de enfrentamiento (Varas, 2017).

El grado de autonomía del Estado y los medios de comunicación permiten construir una serie de demandas que se contraponen y transforman conforme evoluciona el conflicto de derechos. Mientras el Estado, a través de procesos judiciales, demanda rendición de cuentas a los medios de comunicación tradicionales y emergentes ante las injurias calumniosas a

la autoridad movilizándolo al Poder Judicial, también sincroniza su retórica política hacia la corrupción y desinformación de los medios de comunicación. En respuesta a la posición oficial, los medios de comunicación que se ubican en la oposición integran a sus demandas de libertad de expresión nuevas denuncias sociales centralizadas en la corrupción y la impunidad del gobierno de Rafael Correa.

83

VI. PODER LEGISLATIVO: EL CONTRAATAQUE

En 2011, el presidente Correa, a través de una clara estrategia de movilización legal, convocó a una consulta popular, en la que, entre otras, se planteaba la siguiente pregunta: “¿Está usted de acuerdo que la Asamblea Nacional, sin dilaciones..., expida una Ley de Comunicación que cree un Consejo de Regulación que regule la difusión de contenidos en la televisión, radio y publicaciones de prensa escrita que contengan mensajes de violencia, explícitamente sexuales o discriminatorios, y que establezca criterios de responsabilidad ulterior de los comunicadores o los medios emisores?” Esta pregunta recibió el sí del 51.68% de quienes sufragaron en aquella consulta, según el Consejo Nacional Electoral (Asamblea Nacional del Ecuador, 2013).

La Ley Orgánica de Comunicación (LOC) entró en vigor en 2013. De acuerdo con Human Rights Watch:

La Ley contiene disposiciones imprecisas que posibilitan procesos penales arbitrarios y actos de censura. Al hacer referencia al derecho constitucional a recibir información “verificada, contrastada, precisa y contextualizada”, la ley abre la puerta a la censura, en tanto otorga al gobierno o los jueces la potestad de decidir si la información es veraz. Asimismo, los periodistas responsables de “linchamiento mediático” —que se define como la difusión de información crítica reiterada destinada a desprestigiar a una persona natural o jurídica o reducir su credibilidad pública— podrán ser obligados a emitir una disculpa pública y podrían ser juzgados penalmente por otros delitos (Human Rights Watch, 2014).

El Relator Especial de las Naciones Unidas sobre el Derecho a la Libertad de Opinión y de Expresión, David Kaye, y el Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, Edison Lanz, alertaron sobre los graves efectos que tiene la Ley Orgánica de Comunicaciones y su aplicación en la libertad de expresión en Ecuador, e instaron a las autoridades a adecuar la normativa a los estándares internacionales en la materia:

MARÍA FERNANDA COBO MANTILLA

los Relatores han advertido sobre la falta de adecuación de varios aspectos de la ley a estándares internacionales y han observado con preocupación que su aplicación ha sido un instrumento para intervenir de manera indebida en el contenido de los medios de comunicación y sancionarlos, sobre todo cuando las coberturas son desfavorables o cuestionan los actos y decisiones del gobierno (ONU, 2016).

84 Para la Corte Interamericana de Derechos Humanos, la imposición de sanciones penales por las expresiones utilizadas en las denuncias ante las autoridades puede conducir a impedir o inhibir el control social sobre los funcionarios públicos. “La ejecución de esta decisión no solo tendría un efecto intimidatorio (*chilling effect*) sino que podría resultar desproporcionado el uso del derecho penal para proteger la honra de servidores públicos frente a las denuncias relacionadas con el ejercicio de sus funciones” (CIDH, 2010b).

El artículo 26 de la LOC tipifica el delito de linchamiento mediático o difamación mediática, definido como la “difusión de información que sea publicada reiterativamente con el propósito de desprestigiar a una persona natural o jurídica o reducir su credibilidad pública”. El texto de la ley prohíbe a los periodistas, criticar a políticos o instituciones con el fin de “reducir su credibilidad pública”. Se trata de un concepto único en el mundo. No existen otras legislaciones de comunicación que contemplen este delito. El artículo 26 es el más criticado de la ley, por ser considerado un instrumento de autocensura (Gehrke *et al.*, 2016: 8).

Sobre las sanciones ulteriores por la publicación de expresiones de interés público, la CIDH indicó que “no solo impiden que las personas conozcan informaciones relevantes para el ejercicio de sus derechos, sino que generan un efecto intimidatorio que contradice la obligación del Estado de establecer un marco institucional en el cual el debate sobre todos los asuntos públicos pueda ser abierto, plural, desinhibido y vigoroso” (CIDH, 2010b).

Un ejemplo del uso de la Ley de Comunicación por parte del gobierno es la publicación en el diario *El Universo*, de una serie de *tweets* de Rafael Correa, en los cuales explicaba su decisión de permitir la explotación petrolera en el parque nacional Yasuní, y *tweets* enviados a Correa por otras personas que se oponían a tal decisión.

El Secretario de Comunicación, citando disposiciones de la ley que definen los asuntos de relevancia pública y el derecho a que se publiquen correcciones cuando se difunda información imprecisa, ordenó al periódico *El Universo* que ofreciera una disculpa pública por escribir *tweets* que, según

afirmó, atentaban contra el honor y la reputación del presidente. El secretario acusó a *El Universo* de “descontextualización” y “ligereza”, y de publicar información sin “relevancia pública” (Human Rights Watch, 2014).

Sobre los contenidos en Internet, la LOC señala:

Artículo 4. Esta ley no excluye las acciones penales o civiles a las que haya lugar por las infracciones a otras leyes que se cometan a través del internet.

85

Artículo 5. Para efectos de esta ley, se consideran medios de comunicación social a las empresas, organizaciones públicas, privadas y comunitarias, así como a las personas concesionarias de frecuencias de radio y televisión, que prestan el servicio público de comunicación masiva que usan como herramienta medios impresos o servicios de radio, televisión y audio y video por suscripción, cuyos contenidos pueden ser generados o replicados por el medio de comunicación a través de internet.



De acuerdo con *Fundamedios*, al momento se registran 483 sanciones a medios y a periodistas por la Ley de Comunicación, y 234 casos por derechos digitales, cifras que reflejan la sistematización del conflicto de libertad de expresión y respeto a la dignidad individual, no sólo en su esfera legal territorial, sino también en la esfera transnacional-digital (*Fundamedios*, 2017).

VII. EL EMPODERAMIENTO DIGITAL DE LA VOZ CIVIL

El conflicto de la libertad de expresión y la dignidad individual en el Ecuador se integra entonces al eje del cosmopolitismo digital, donde la democracia virtual es parte del poder transformador en los procesos de participación ciudadana en el sistema democrático, y la sociedad civil se debate en la neutralidad de la red poniendo en acción sus derechos fundamentales.

De acuerdo con la CIDH (2009):

Maximizar el número y la diversidad de voces que puedan participar de la deliberación pública es al mismo tiempo condición y finalidad esencial del proceso democrático. En este sentido, las garantías robustas para el ejercicio de la libertad de expresión a través de Internet son, en la actualidad, una condición de posibilidad para esa apertura de la esfera pública.

La consecuencia de esta tensión entre democracia, libertad de expresión e información, y dignidad individual refleja el rompimiento de la voz

MARÍA FERNANDA COBO MANTILLA

de la sociedad civil ecuatoriana, que hoy se debate entre la autocensura y la desilusión, y ha resultado en una década de sanción a más de 477 medios de comunicación y periodistas y más de dos mil agresiones contra la prensa (*El Economista*, 2017), donde el esfuerzo por reconstruir y garantizar el patrimonio de la voz ciudadana exige la certidumbre que sólo la seguridad jurídica alcanza, para fomentar un diálogo abierto, incluyente y fructífero, que fortalezca la gobernanza del sistema político en el país.

86

El Ecuador necesita recuperar la fortaleza de su soberanía, donde el Estado de derecho sea el articulador de los poderes públicos, que a su vez garanticen y reconozcan los derechos fundamentales de un ciudadano activo, un ciudadano que viva la libertad como un valor moral, la igualdad como una fuerza de ley y la dignidad como un principio de vida.

Un ciudadano libre y autónomo para elevar su voz y demandar al Estado sus obligaciones inmediatas: fortalecer la paz y la seguridad nacional que el país reclama, donde la ausencia y pasividad del Estado se refleja en la desaparición y asesinato de tres periodistas a través del movimiento *#NosFaltan3*. Tres periodistas cuyo secuestro y asesinato no es más que el reflejo de una sociedad víctima de la delincuencia organizada, y donde la voz ciudadana se moviliza hacia *#UnidosPorLaPaz*.

VIII. CONCLUSIONES

El conflicto de la libertad de expresión e información y la dignidad individual en el Ecuador durante el correato estuvo atrapado en una tensión política entre dos poderes: el Estado como poder político e institucional, y la prensa, como poder fáctico real. Asimismo, la estrategia oficial de judicializar penalmente violaciones de derechos a la dignidad por injurias calumniosas a la autoridad constituye una experiencia fallida por parte del Estado, estrategia que obligó al Poder Ejecutivo a redefinir su retórica política en torno al “perdón, sin olvido” al pasar en los procesos judiciales de víctima a victimario, gracias a la presión internacional.

Los medios de comunicación tradicionales deben asumir su responsabilidad civil ante la falta de estándares exigibles en el ejercicio periodístico a partir del entendimiento de que el ejercicio de la libertad de expresión e información, si bien es un derecho fundamental, éste no es absoluto, y está sujeto a límites razonables y particulares, como son el honor y la reputación, límites que exigen una práctica periodística veraz en torno al derecho a la personalidad como una expresión del valor de la dignidad humana. Esta práctica permite al ejercicio periodístico, legitimar su rol en el

sistema democrático a partir de la imparcialidad, que a su vez exige la investigación diligente para cumplir el requisito constitucional de veracidad de la información.

En contraparte, este escenario político reclama un liderazgo abierto ante el vigor de la voz civil, donde es necesario aceptar el riesgo del exceso, haciendo de la tolerancia un valor diferenciador en la acción política que reclama libertad, pluralidad y transparencia, un trinomio fundamental para la democracia.

La Ley Orgánica de Comunicación, donde se integra el Poder Legislativo en esta tensión democrática en Ecuador, constituyó el principal instrumento para fortalecer la posición autoritaria del Estado frente una demanda social que evolucionó, de ser un conflicto de libertad de expresión e información, a ser una exigencia de transparencia ante la corrupción, la impunidad y la legitimidad tanto del Estado como de los medios de comunicación. Una Ley que necesariamente debía ajustarse a los estándares internacionales jurídicamente vinculantes para el Ecuador y que exigió integrar a esta lucha de fuerzas un activismo legislativo efectivo.

Este conflicto se ha enmarcado en el escenario nacional-jurídico y en el escenario transnacional digital, lo que ha permitido mantener la tensión viva. Sin embargo, con diferentes momentos de intensidad y sin resultados trascendentes de cambio, tanto en la arquitectura e ingeniería jurídica como en su institucionalización, donde es determinante reconstruir el modelo de comunicación política en el país para que sea posible ejercer el derecho a la libertad de expresión e información en un clima de seguridad jurídica, transparencia y no discriminación.

Hoy, la participación ciudadana se integra y vive de manera más activa este conflicto de derechos entre poderes desde las nuevas tecnologías, ejerciendo una auténtica ciudadanía digital, donde el ciberactivismo y la ciberdesobediencia civil constituyen la plataforma más oportuna, conmovedora y eficaz para estimular la movilización civil.

Empieza a ganar fuerza el rol de la democracia virtual deliberativa en un orden político que exige fortalecer el contrapeso del Estado a través de una oposición política con mayor definición e integración, así como con una prensa con mayores estándares en su ejercicio informativo. El ciudadano comunicador juega un rol determinante al convertir el derecho a la libertad de expresión e información en un pilar fundamental del pluralismo y el bienestar social en una democracia participativa, donde silenciar no es digno, donde silenciar no es opción.



MARÍA FERNANDA COBO MANTILLA

IX. FUENTES

- ARCOS, Carlos, 2014, “El fusilamiento mediático: nuevas armas en el ejercicio del poder en Ecuador”, en GONZÁLEZ, Silvana (coord.), *La restauración conservadora del correísmo*, Quito, Arcoiris Producción Gráfica.
- ARIAS, Daniela y GUERRERO, Érika, 2016, “Tuitómetro: la batalla en 140 caracteres”, *Observatorio de Medios del Ecuador (OME)*, Fundamedios.
- 88 BARRAGÁN ROMERO, Gil, 2011, “Sentencias en el caso *El Universo*”, *Vistazo*, octubre.
- BOBBIO, Norberto, 2009, *Liberalismo y democracia*, México, Fondo de Cultura Económica.
 -
 -
- CERBINO, Mauro, 2016, *Los enlaces ciudadanos del presidente Rafael Correa*, Quito, Flacso.
- COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, 2018, *Declaración conjunta sobre la independencia y la diversidad de los medios de comunicación en la era digital*, 2 de mayo, disponible en: <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1101&IID=2> (fecha de consulta: 16 de abril de 2019).
- COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, 2015a, *Informe núm. 66/15*, Petición 1436-11 Informe de Admisibilidad, Emilio Palacio Urrutia y otros Ecuador, 27 de octubre de 2015.
- COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, 2015b, “Capítulo 11: Derecho a buscar asilo”, *Movilidad humana. Estándares interamericanos*, 31 de diciembre de 2015.
- COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, 2010a, *Informe núm. 88/10*, Caso 12.661. Fondo. Néstor José y Luis Uzcátegui y otros Venezuela, 14 de julio de 2010.
- COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, 2010b, *Informe núm. 82/10. Caso 12.524*. Fondo. Jorge Fontevicchia y Héctor d’Amico. Argentina, 13 de julio de 2010.
- COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, 2010c, *Declaración conjunta del décimo aniversario: diez desafíos claves para la libertad de expresión en la próxima década*, reunidos en Washington, D. C., 2 de febrero, disponible en: <http://www.cidh.org/Comunicados/Spanish/2010/18-10sp.htm> (fecha de consulta: 16 de abril de 2019).
- COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, 2009, “Capítulo III: Marco Jurídico Interamericano del Derecho a la Libertad de Expresión”,

Informe Anual 2009. Informe de la Relatoría Especial para la Libertad de Expresión. OEA/Ser.L/V/II. Doc. 51, 30 de diciembre.

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, *Declaración de Principios sobre la Libertad de Expresión*, disponible en: <https://www.cidh.oas.org/basicos/declaracion.htm> (fecha de consulta: 2 de noviembre de 2018).

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS, *Libertad de expresión e Internet*, disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf (fecha de consulta: 2 de noviembre de 2018).

89

CONVENCIÓN AMERICANA DE DERECHOS HUMANOS, disponible en: http://www.oas.org/dil/esp/tratados_B32_Convencion_Americana_sobre_Derechos_Humanos.htm (fecha de consulta: 16 de abril de 2019).

CORNEJO MENACHO, Diego, 2013, *Cátedra y hoguera*, en *El Caso El Universo*, Quito, Paradiso Editores.

CORREA, Rafael, 2012, *Carta a mi pueblo, a nuestra América y al mundo*, 27 de febrero.

CORTE IDH, 2017, *Estándares internacionales de la libertad de expresión: guía básica para operadores de justicia en América Latina*, disponible en: <http://www.corteidh.or.cr/tablas/r37048.pdf> (fecha de consulta: 2 de noviembre de 2018).

Dipublico, “Declaración del Gobierno de la República del Ecuador sobre la solicitud de asilo de Julian Assange”, *Dipublico.org*, disponible en: <https://www.dipublico.org/9584/texto-completodeclaraciondelgobierno-de-la-republica-del-ecuador-sobre-la-solicitud-deasilo-de-julian-assange/> (fecha de consulta: 2 de noviembre de 2018).

El Economista, 2017, “Correa y su legado: 477 medios sancionados”, *El Economista*, 6 de febrero, disponible en: <https://www.eleconomista.com.mx/internacionales/Correa-y-su-legado477-medios-sancionados-20170206-0082.html> (fecha de consulta: 18 de junio de 2018).

El Universo, 2015, “Gobierno lidera gasto en difusión y publicidad con \$105,6 millones”, *El Universo*, disponible en: <https://www.eluniverso.com/noticias/2015/11/30/nota/5271276/gobierno-lidera-gasto-difusion-publicidad-1056-millones> (fecha de consulta: 2 de noviembre de 2018).

El Universo, 2015, “CrudoEcuador: Este pleito de un presidente contra un ciudadano que hace memes creo que lo está ridiculizando”, *El Universo*, 27 de enero, disponible en: <https://www.eluniverso.com/noticias/2015/01/27/nota/4490131/crudoecuadorestepleito-presidente-contra-ciudadano-que-hace> (fecha de consulta: 2 de noviembre de 2018).

MARÍA FERNANDA COBO MANTILLA

El Universo, 2012, “*El Universo* recibe hoy premio de Universidad de Columbia”, *El Universo*, Ecuador, 25 de octubre, disponible en: <https://www.eluniverso.com/2012/10/25/1/1355/universo-recibe-hoy-premioucolumbia.html> (fecha de consulta: 2 de noviembre de 2018).

FERRAJOLI, Luigi, 2016, *Derechos y garantías. La ley del más débil*, Madrid, Trotta.

90 ● ○ ● *Fundamedios*, “Cifras contra la libertad de expresión. Violaciones y ataques a la libertad de expresión por años en Ecuador”, *Fundamedios*, 26 de diciembre, disponible en: <http://www.fundamedios.org/tag/cifras-contra-libertad-de-expresion/> (fecha de consulta: 2 de noviembre de 2018).

FOUCAULT, Michel, 2018, *Vigilar y castigar*, México, Siglo XXI Editores.

GARGARELLA, Roberto, 2005, *Las teorías de la justicia después de Rawls*, Barcelona, Paidós.

GEHRKE, Mirjam *et al.*, 2016, *Panorama de los medios en Ecuador*, Media Development Studies, Bonn, Deutsche Welle.

GUTIÉRREZ, Ignacio, 2004, *El patrimonio. El pecuniario y el moral o derechos a la personalidad*, México, Porrúa.

GUTIÉRREZ, Ignacio, 2005, *Dignidad de la persona y derechos fundamentales*, Madrid, Marcial Pons-Ediciones Jurídicas y Sociales.

HERNÁNDEZ GIL, Antonio, 1970, *Marxismo y positivismo lógico. Sus dimensiones jurídicas*, Madrid.

HUMAN RIGHTS FOUNDATION, 2011, *Carta a la Corte Nacional de Justicia de la República de Ecuador*, 31 de octubre, disponible en: http://lahrf.com/documents/Carta_Jueces%20EPU.pdf (fecha de consulta: 2 de noviembre de 2018).

HUMAN RIGHTS WATCH, 2014, *Informe Mundial*, disponible en: <https://www.hrw.org/es/world-report/2014/country-chapters/260117> (fecha de consulta: 20 de mayo de 2018).

KANT, Immanuel, 2016, *Fundamentación de la metafísica de las costumbres*, Barcelona, Espasa Libros.

LUCKES, Steven, 1981, “Can a Marxist Believe in Human Rights?”, *Praxis Internacional*, núm. 1.

MARIA MOORS CABOT PRIZES, disponible en: https://journalism.columbia.edu/system/files/content/past_cabot_winner_list.pdf (fecha de consulta: 2 de noviembre de 2018).

NAVA GARCÉS, Alberto, 2013, *El derecho en la era digital*, México, Porrúa.

ONU-CIDH, Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos, “Ecuador / libertad de expresión”, 3 de noviem-

- bre de 2016, disponible en: <http://www.ohchr.org/SP/NewsEvents/Pages/DisplayNews.aspx?NewsID=20827&LangID=S#sthash.7VAltRSD.dpu> (fecha de consulta: 2 de noviembre de 2018).
- ORGANIZACIÓN DE LOS ESTADOS AMERICANOS (OEA), 2018, *Declaración de Principios sobre libertad de expresión*, disponible en: <http://www.oas.org/es/cidh/expresion/showarticle.asp?artID=132&IID=2> (fecha de consulta: 17 de junio de 2018).
- PONCE, Alexis, 2016, “¿Es correísmo, o correato?”, *Aporrea.org*, disponible en: <https://www.aporrea.org/internacionales/a226344.html> (fecha de consulta: 1o. de septiembre de 2018).
- REPORTEROS SIN FRONTERAS, *Informe anual 2018*, disponible en: <https://www.informeanualrsf.es/news/ecuador-18/> (fecha de consulta: 31 de marzo de 2018).
- ROMERO PARDUCCI, Emilio, 2013, *El caso El Universo, cuestiones jurídicas*, Quito, Paradiso Editores.
- RUIZ RODRÍGUEZ, Virgilio, 2011, *El derecho a la libertad de expresión e información en el sistema europeo e interamericano*, México, Universidad Iberoamericana.
- RONSON, Jon, 2015, *So You've been Publicly Shamed*, Nueva York, River Head Books.
- SCHWABE, Jürgen, 2009, *Jurisprudencia del Tribunal Constitucional Federal alemán*, Berlín, Konrad-Adenauer-Stiftung.
- SERRANO, Sandra y VÁZQUEZ, Luis Daniel, 2013, “La postura del Ecuador frente al proceso de fortalecimiento del sistema interamericano de derechos humanos. La disputa por los conceptos y sus consecuencias”, *Pensamiento Propio*, núm. 18, julio-diciembre.
- SUMMER, Harlow y SALAVERRÍA, Ramón, 2016, “Regenerating Journalism: Exploring the «Alternativeness» and «Digital-Ness» of Online-Native Media in Latin America”, *Digital Journalism*, vol. 4, núm. 8.
- TAYLOR, Charles, 1993, *Multiculturalismo y política del reconocimiento*, México, Fondo de Cultura Económica.
- VARAS, Eduardo, 2017, “Historia de fundamedios”, *Fundamedios*, disponible en: <http://www.fundamedios.org/quienessomos/historia-de-fundamedios/> (fecha de consulta: 20 de mayo de 2018).
- 4Pelagatos, 2017, “4Pelagatos cumple un año”, *4Pelagatos*, 23 de enero, disponible en: <http://4pelagatos.com/2017/01/23/4pelagatos-cumple-un-ano/> (fecha de consulta: 20 de mayo de 2018).



MARÍA FERNANDA COBO MANTILLA

Marco jurídico

Constitución de la República del Ecuador, disponible en: <https://www.wipo.int/edocs/lexdocs/laws/es/ec/ec030es.pdf> (fecha de consulta: 16 de abril de 2018).

92 Ley Fundamental de la República Federal de Alemania, disponible en: <https://www.btg-bestellservice.de/pdf/80206000.pdf> (fecha de consulta: 16 de abril de 2019).

● Ley Orgánica de Comunicación (LOC), Registro Oficial núm. 22, 25 de junio de 2013, disponible en: <https://www.wipo.int/edocs/lexdocs/laws/es/ec/ec067es.pdf> (fecha de consulta: 2 de noviembre de 2018).
○
●

COMENTARIOS JURÍDICOS



COMENTARIO JURÍDICO A LA RECOMENDACIÓN GENERAL 29 “SOBRE EL EXPEDIENTE CLÍNICO COMO PARTE DEL DERECHO A LA INFORMACIÓN EN MATERIA DE SALUD” EMITIDA POR LA CNDH



*Alejandro DÍAZ PÉREZ**
*Rita Astrid MUCIÑO CORRO***

I. INTRODUCCIÓN

El 31 enero de 2017, la Comisión Nacional de los Derechos Humanos (en adelante la Comisión o CNDH) emitió la Recomendación General 29 “Sobre el expediente clínico como parte del derecho a la información en materia de salud”. Lo hizo de acuerdo con la atribución contenida en la fracción VIII del artículo 6o. de su Ley, que la faculta para proponer que se promuevan los cambios y modificaciones de leyes y reglamentos, así como de prácticas administrativas, que procuren y garanticen una mejor y más amplia protección de los derechos humanos a las diversas autoridades del país en el exclusivo ámbito de su competencia.

Esta decisión tiene una profunda importancia, por varias razones. Por una parte, la temática específica del documento es única en su tipo en

* Licenciado en derecho y ciencias sociales, Universidad Michoacana de San Nicolás de Hidalgo. Especialista en derechos humanos y máster en derecho constitucional por la Universidad de Castilla-La Mancha, España. Máster en derechos humanos por la Universidad Autónoma de Madrid, España. Exvisitante profesional en la Corte Interamericana de Derechos Humanos, en San José, Costa Rica. Actualmente, abogado del Grupo de Recomendaciones de la Cuarta Visitaduría General de la Comisión Nacional de los Derechos Humanos.

** Maestra en derechos humanos y democracia por la Facultad Latinoamericana de Ciencias Sociales, con especialidad en derechos humanos por la Universidad Castilla-La Mancha. Fue Visitante profesional en la Corte Interamericana de Derechos Humanos

Fecha de recepción: 24 de enero de 2019.

Fecha de dictamen: 28 de marzo de 2019.

ALEJANDRO DÍAZ PÉREZ / RITA ASTRID MUCIÑO CORRO

México, en tanto contiene elementos de análisis sobre la forma en cómo el expediente clínico es una vía directa para garantizar el derecho a la información en el ámbito de la salud.

96 Asimismo, desde otra perspectiva, la motivación de la Comisión para emitir la Recomendación General guarda relación con la cuantiosa evidencia empírica, basada en 96 casos ocurridos entre 2010 y 2016, en los que diversas autoridades públicas incumplieron con la debida integración del expediente clínico (CNDH, 2017a: 5), al tiempo que da cuenta de las dificultades existentes en el sistema de sanidad del país para el tratamiento de los datos personales en el ámbito médico.

●
○
● A partir del estudio de dichos casos, el organismo de derechos humanos identificó el posible origen de las problemáticas existentes y formuló una serie de recomendaciones, que pudieran servir para solucionar aquellos hechos violatorios que dan lugar al menoscabo del derecho a la información en materia de salud, entre otros.

El presente comentario jurídico pretende realizar una revisión crítica de la Recomendación General 29. Se partirá de los enfoques de derechos humanos y de género para sostener que no obstante su indudable importancia, ésta cuenta con algunos puntos “ciegos”; que tendrán que ser reorientados, profundizados y, en su caso, reformulados.

De esta manera, los argumentos del texto se construyen sobre criterios de revisión relacionados con aspectos del derecho de acceso a la información aplicables a la integración de expedientes médicos, la protección de datos personales en posesión de médicos e instituciones de salud pública y privada, la titularidad y propiedad del mismo, el plazo para la conservación del expediente clínico, la vulnerabilidad de la información y medidas de seguridad, así como la importancia de abordar la temática desde la perspectiva de género.

II. RECOMENDACIÓN GENERAL 29 “SOBRE EL EXPEDIENTE CLÍNICO COMO PARTE DEL DERECHO A LA INFORMACIÓN EN MATERIA DE SALUD”

La justificación de la emisión de la Recomendación General 29 encuentra su base en al menos dos cuestiones sustanciales. La primera, relacionada con la documentación de omisiones sistemáticas (CNDH, 2017a: 5) por parte del personal de salud de diversas instituciones en la elaboración de los expedientes clínicos de las y los pacientes; y segunda, en el carácter incremental (CNDH, 2017a: 6), de este tipo de vulneraciones a lo largo de los

últimos años. La suma de estos factores permite inferir la razón por la que ésta se dirigió a prácticamente todas las instituciones de salud del Estado mexicano, en los diversos órdenes de gobierno.¹

El análisis parte de los antecedentes que dieron forma a los desarrollos normativos del expediente clínico. Al respecto, éste se implementó desde 1986, pasando por una reforma en 1993, para finalmente expedirse en 2012 la Norma Oficial Mexicana NOM-004-SSA3-2012, “Del Expediente Clínico” (en lo sucesivo NOM-004).

Asimismo, países como Estados Unidos, España, Francia, Bélgica, Argentina, Costa Rica, Colombia y Uruguay (CNDH, 2017a: 13-19) tienen importantes avances jurídicos, lo que da cuenta de la prevalencia de un cierto consenso a nivel comparado de la inclusión del expediente clínico o historia clínica como un elemento del derecho a la información.

Ahora bien, respecto al análisis central de la integración del expediente clínico como parte del derecho a la información en materia de salud, debe partirse de la inevitable interrelación del derecho a la protección de la salud (en sentido amplio) previsto en el artículo 4o. de la Constitución Política de los Estados Unidos Mexicanos, con el derecho a la información contemplado en el artículo 6o. del mismo ordenamiento.

Sumando a lo anterior, el Comité de Derechos Económicos, Sociales y Culturales de la ONU (Comité DESC) ha interpretado que en materia de salud el derecho a la información comprende “el derecho de solicitar, recibir y difundir información e ideas acerca de las cuestiones relacionadas con la salud. Con todo, el acceso a la información no debe menoscabar el derecho de que los datos personales relativos a la salud sean tratados con confidencialidad” (Comité DESC, 2000: 12).

De forma más específica, del expediente clínico y su relación con el derecho a la información han sido abordados por la Corte Interamericana de Derechos Humanos (Corte IDH), al referir que “un expediente médico, adecuadamente integrado, es instrumento guía para el tratamiento médico, y fuente razonable de conocimiento acerca de la situación del enfermo, las medidas adoptadas para controlarla y, en su caso, las consecuentes responsabilidades” (caso Albán Cornejo y otros vs. Ecuador: 68).

A nivel interno, a decir de la Comisión, la Ley General de Salud contempla al expediente clínico en una doble dimensión: 1) como una obli-

¹ Secretarías de Salud, de la Defensa Nacional y de Marina; gobernadores de las entidades federativas; jefe de gobierno de la Ciudad de México, y directores generales del Instituto Mexicano del Seguro Social, del Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado y de Petróleos Mexicanos.



ALEJANDRO DÍAZ PÉREZ / RITA ASTRID MUCIÑO CORRO

gación vinculada con el principio de calidad² en el servicio, y 2) como un derecho contenido en el artículo 77 bis 37³ (CNDH, 2017a: 30).

Bajo esta perspectiva, el derecho a la información en materia de salud, relativo al expediente clínico de las personas, es “aquella libertad atribuible a los usuarios de servicios médicos para solicitar, recibir y conocer todas las constancias y elementos que integran dicho expediente clínico”(CNDH, 2017a: 32), y estaría conformada por al menos tres aspectos fundamentales: 1) el acceso para recibir todo tipo de información relacionada con la atención de la salud; 2) la protección de los datos personales, y 3) la información en disposición bajo los principios de accesibilidad, confiabilidad, verificabilidad, veracidad y oportunidad (CNDH, 2017a: 34).

No obstante este cúmulo de previsiones normativas, cabe preguntarse en dónde se concentran las problemáticas relevantes sobre la cuestión. En un primer momento, de acuerdo con la propia recomendación general de la CNDH, las omisiones más recurrentes sobre la integración del expediente clínico —que pudieran llamarse formales— se refieren al incumplimiento de los requisitos contenidos en la NOM-0042, relacionados con el asentamiento de datos, como hora, fecha, y nombre de quienes realizan las notas médicas, datos de exploración y tratamientos médicos, notas de evolución, hojas de enfermería, entre otros (CNDH, 2017a: 39).

En otro sentido, concurren problemas que son de índole estructural; esto es, la existencia de un vínculo entre las condiciones laborales del personal médico que dificulta la manera en que se asientan con debida diligencia los datos del expediente clínico, y la existencia de un problema en la lógica de funcionamiento de las instituciones de salud (CNDH, 2017a: 42).

A su vez, la Comisión agrega que en relación con la práctica médica, “la sobrecarga de trabajo derivada del alto número de pacientes que deben atender en poco tiempo, haciendo materialmente imposible su debida integración”; es decir, alude a un criterio pragmático, al tiempo que enfatiza la existencia de “extenuantes jornadas laborales que surgen como consecuencia del entendimiento de la cultura del trabajo en las instituciones de salud y la visión social generalizada del trabajo y práctica médica” (CNDH, 2017: 43). En otra línea, subraya la prevalencia de “deficiencias de infraes-

² Por calidad, el Comité DESC ha descrito que los servicios de salud deben ser culturalmente adecuados y aceptables tanto científica como médicamente. Ello requiere, entre otras cosas, personal médico capacitado, medicamentos y equipo hospitalario científicamente aprobados y en buen estado, agua limpia potable y condiciones sanitarias adecuadas.

³ Artículo 77 bis 37: “Los beneficiarios del Sistema de Protección Social en Salud tendrán además los derechos establecidos en el artículo anterior, los siguientes... VII. Contar con su expediente clínico...”.

estructura, recursos tecnológicos y la falta de implementación de sistemas automatizados o electrónicos” (CNDH, 2017: 44).

Como formas de solución a estos obstáculos, el organismo nacional plantea distintos niveles de aproximación. Al respecto, sugiere cinco medidas, a saber: 1) la adopción de medidas administrativas, financieras, jurídicas o de cualquier otra índole, para que se procure el debido cumplimiento en la integración de los expedientes clínicos; 2) la realización de estudios que permitan advertir cuál es la relación de causalidad existente entre las condiciones laborales del personal médico y la indebida integración de los expedientes clínicos; 3) se proporcionen los recursos tecnológicos necesarios que faciliten al personal de salud la debida integración del expediente clínico; 4) desde el ámbito institucional o intersectorial, se articulen asimetrías regulatorias que permitan vigilar el cumplimiento de la NOM-004, y 5) la impartición de cursos de capacitación y formación en materia de derechos humanos, así como del conocimiento, manejo y observancia de las normas oficiales mexicanas del expediente clínico (CNDH, 2017a: 20 y 21).

Habida cuenta de estas propuestas de posible solución en el tratamiento de los datos e información contenida en los expedientes clínicos, se advierte que existen aspectos que la Recomendación General 29 debió cuestionar, y que deben incorporarse en futuros esfuerzos, al tiempo que considerarse por las diversas instituciones de salud pública del país, como a continuación se analiza.

III. LOS VACÍOS QUE DEJA LA RECOMENDACIÓN GENERAL 29

En un primer momento, puede identificarse que la Recomendación General no fue construida a la par de organizaciones de la sociedad civil, instituciones académicas en el ámbito médico y/o con órganos autónomos pares a la CNDH, como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Lo anterior hubiera permitido concentrar todas las voces que pudieran aportar al debate público sobre la temática en cuestión. Sobre ello, el documento no hace ninguna referencia a este proceso de socialización del contenido de la Recomendación.⁴

⁴ Sobre la relevancia de enriquecer estos procesos institucionales con los aportes de la sociedad civil y otros organismos no jurisdiccionales, los Principios de París disponen que en el marco de sus actividades, las instituciones nacionales deben: “6. mantener la coordinación con los demás órganos de carácter jurisdiccional o de otra índole encargados



ALEJANDRO DÍAZ PÉREZ / RITA ASTRID MUCIÑO CORRO

Asimismo, no se advierte que en la resolución se haya tenido en cuenta la forma en que esto sucede en las entidades federativas, cuestión que hubiera sumado al entendimiento de dicho fenómeno, al brindar un panorama más amplio acerca de las circunstancias que imperan tanto en los centros de salud estatales como en los municipales, al igual que en los ubicados en zonas rurales —siendo éstos donde se concentra el mayor número de población susceptible de verse afectada por este problema—.

100

Por otra parte, avanzando en los aspectos propios de la resolución, no contempla a la Ley General de Transparencia y Acceso a la Información Pública, y/o a la Ley Federal de Transparencia y Acceso a la Información Pública como un marco de referencia o fuente de obligación para las diversas instituciones del Estado mexicano en relación con el expediente clínico.

Asimismo, un aspecto relevante que fue omitido tiene que ver con el desarrollo de las obligaciones existentes sobre el derecho a la información en materia de salud, cuando se trata de protección frente a terceros o particulares. En este punto, la Ley Federal de Protección de Datos Personales en Posesión de los Particulares⁵ y su Reglamento debió ser abordada por la Comisión como un marco esencial.

También debe recordarse que de acuerdo con las normas de derechos humanos, las autoridades de un Estado pueden ser responsables por cualquier violación a los derechos humanos cometida por particulares que ocurra dentro de su jurisdicción si devienen tres condiciones: *i*) al momento de los hechos existe una situación de riesgo real e inmediato; *ii*) las autoridades conocían o debían tener conocimiento de dicha situación, y *iii*) no adoptar las medidas razonables y necesarias para prevenir o evitar ese riesgo (caso Rodríguez Vera y otros vs. Colombia: 523).

Esta cuestión cobra suma relevancia en tanto que aproximadamente el 24% de las personas en México son usuarios del sector privado de salud (Inmujeres, 2010), cuyos datos personales contenidos en los expedientes

de la promoción y protección de los derechos humanos...; 7. establecer relaciones con organizaciones no gubernamentales que se ocupen de la promoción y protección de los derechos humanos...". Principios de París, adoptados por la Asamblea General de las Naciones Unidas en 1993. Por su parte, el artículo 51, inciso B), fracciones I a III del Reglamento de la CNDH, establece que se deberán impulsar los procesos de colaboración y consolidar la relación con las organizaciones de la sociedad civil para la implementación de una agenda de derechos humanos. Reglamento Interno de la Comisión Nacional de los Derechos Humanos, última reforma incorporada: 22 de diciembre de 2017.

⁵ Al respecto, la fracción VI del artículo 3 de dicha Ley hace referencia al estado de salud presente y futuro de una persona como un dato personal sensible.

clínicos son tratados por médicos y hospitales privados, y que exigen una actuación del Estado frente a esta circunstancia.

Otro elemento que merece una reflexión particular es el relacionado con la titularidad o propiedad del expediente clínico. De acuerdo con el numeral 5.4 de la NOM-004, los expedientes clínicos “son propiedad de la institución o del prestador de servicios médicos que los genera”. Al respecto, esta posición es problemática, y debe cambiarse para transitar hacia una que contenga un enfoque de derechos humanos más apropiada, en tanto la propiedad (y titularidad) del expediente debe ser de la persona que recibe el servicio de salud, no sólo la información en sí misma, sino del objeto como tal.⁶ Por esta razón, la Comisión en futuras decisiones debería profundizar sobre este aspecto, y no abstenerse, como en la Recomendación General 29.

101

Sobre el particular, resulta pertinente hacer mención de lo sostenido por la Segunda Sala de la Suprema Corte de Justicia de la Nación (SCJN) en el amparo en revisión 632/2014, en el que entre otros puntos refirió que los numerales 5.4 a 5.7 de la NOM-004 “deben interpretarse en un sentido amplio”, de forma que la persona usuaria tenga la posibilidad de allegarse, cuando así lo solicite, de “cualquier constancia que obre dentro de su expediente, incluso de que éste sea proporcionado en su integridad” (AR 632/2014: 14).

En conexión con lo anterior, la propia NOM-004 prevé que los expedientes clínicos, “por tratarse de documentos elaborados en interés y beneficio del paciente, deberán ser conservados por un periodo mínimo de 5 años, contados a partir de la fecha del último acto médico” (NOM-004: 5.4). Las discusiones sobre el plazo contemplado deberían estar sujetas a un abordaje mayor, y orientadas en incorporar algunas excepciones procedentes para los fines que sean relevantes.⁷

Un aspecto medular adicional lo constituye el hecho de que si bien existe un deber específico de integrar el expediente clínico de cada paciente, esa obligación no implica necesariamente que éste sea electrónico. En este aspecto, la Comisión debió solicitar que se reformara la NOM-004, para que la obligación de empezar a diseñar expedientes electrónicos quedara plasmada. Tal avance facilitaría la conservación de datos personales,

⁶ El INAI en el criterio 317/17 determinó que la titularidad de los datos personales contenidos en expediente clínico es del paciente y no de hospitales o médicos.

⁷ Por ejemplo, en casos en los que la información del expediente en cuestión sea relevante para una investigación científica, así como en casos de violaciones de derechos humanos especialmente graves, como serían las prácticas sistemáticas de esterilizaciones forzadas o en abusos sexuales en contextos de revisiones ginecológicas.

ALEJANDRO DÍAZ PÉREZ / RITA ASTRID MUCIÑO CORRO

la disminución de la posibilidad pérdidas, robos, extravíos, acumulación de papelería y facilidad de almacenamiento, en contraste con las vías tradicionales de instrumentación del expediente clínico (Moreddu, 2017).

102 Asimismo, la implementación del expediente clínico electrónico, como instrumento de protección y garantía del derecho a la información, también implicaría una reestructuración profunda de la Norma Oficial Mexicana NOM-024-SSA3-2012, “Sistemas de información de registro electrónico para la salud. Intercambio de información en salud”, que establece los objetivos funcionales y funcionalidades que deberán observar los productos de sistemas de expediente clínico electrónico para garantizar la interoperabilidad, procesamiento, interpretación, confidencialidad, seguridad y uso de estándares y catálogos de la información de los registros electrónicos en salud.

Finalmente, la sofisticación de los medios de ingreso de los datos contenidos en un expediente clínico electrónico que se dirijan a disminuir la vulnerabilidad de la información, como la utilización de la firma electrónica avanzada por parte del personal médico autorizado que brinda la atención médica, son un tema central de progresiva inclusión.

Derecho a la información en materia sexual y reproductiva

La vulneración al derecho a la información en materia sexual y reproductiva es una constante que afecta principalmente a mujeres y niñas. La prevalencia de factores que restringen el goce efectivo del mismo genera consecuencias que les impiden a aquéllas actuar con autonomía, al igual que tomar las decisiones que mejor correspondan a su proyecto de vida.

Por tal motivo, cobra especial relevancia el conocimiento sobre los datos inherentes al estado de salud durante el proceso del embarazo, así como en las etapas de alumbramiento y posteriores, toda vez que se trata de determinaciones sobre salud sexual y reproductiva, así como sobre la vida de las mujeres y el producto de la gestación.

Dicha situación ha dado lugar a numerosas recomendaciones emitidas por la CNDH, e incluso motivó las recomendaciones generales 4/2002 “Derivada de las prácticas administrativas que constituyen violaciones a los derechos humanos de los miembros de las comunidades indígenas respecto de la obtención de consentimiento libre e informado para la adopción de métodos de planificación familiar”, y 31/2017 “Sobre la violencia

obstétrica en el sistema nacional de salud”,⁸ en las que constató que el personal de salud, al obtener el consentimiento sobre los métodos de planificación familiar, incurre en una serie de acciones u omisiones, transgresoras de los derechos humanos de las personas usuarias.

De esta manera, es posible afirmar que la CNDH cuenta con la evidencia suficiente para sostener que en la práctica médica es recurrente el incumplimiento de los estándares relacionados con este derecho. No obstante lo anterior, fue omisa en pronunciarse al respecto.

La Recomendación General objeto de estudio representaba una excelente oportunidad para visibilizar las barreras que las mujeres enfrentan al acceder a la información en el contexto de la atención a la salud, particularmente durante la atención del embarazo, del parto y del puerperio, así como para establecer medidas idóneas, considerando que este tipo de actos, más allá de ser resultado de la precaria dinámica organizacional en los hospitales, tienen por origen la discriminación.

Si bien en el mencionado documento se hace referencia a la importancia que una correcta integración revierte para las mujeres víctimas de violaciones a los derechos sexuales y reproductivos, la CNDH sólo realiza una mención superficial, y deja de lado una lectura más profunda que considerara los enfoques de género e intercultural.

No pasa desapercibido el hecho de que la inobservancia de los estándares trae consigo una afectación adicional tratándose de personas provenientes de grupos de atención prioritaria, tales como personas mayores, migrantes, etcétera; sin embargo, de la revisión de los 96 casos analizados por la CNDH en su Recomendación General se identificó que en 61 de ellos las personas afectadas son mujeres, de las cuales

- El 15.8% es indígena.
- El 15.8% era menor de edad.
- El 68.2% estaba embarazada.⁹

En este tenor, la Comisión Interamericana de Derechos Humanos (en adelante la CIDH), en su informe sobre “Acceso a la información en mate-

⁸ Los casos que se registraron en la Recomendación General 31/2017 datan desde 2015, por lo que el hecho de que se haya emitido con posterioridad a la Recomendación General 29/2017 no exime a la CNDH de haber integrado en esta última un apartado para analizar la vulneración al acceso a la información en material sexual y reproductiva.

⁹ Para obtener el porcentaje se consideró el número de mujeres que fueron víctimas en los 61 casos, lo cual suma un total de 63. Esa información fue sistematizada de la revisión de las recomendaciones emitidas por la CNDH, que puede consultarse en: <http://www.cndh.org.mx/Recomendaciones>.



ALEJANDRO DÍAZ PÉREZ / RITA ASTRID MUCIÑO CORRO

ria reproductiva desde una perspectiva de derechos humanos”, reconoció que las mujeres latinoamericanas enfrentan obstáculos que les impiden ejercer plenamente al multicitado derecho. Asimismo, indicó que los Estados deben asegurar el acceso a la información, así como: *a)* el consentimiento informado; *b)* la protección de la confidencialidad; *c)* la obligación de entregar información oportuna, completa, accesible, fidedigna y oficio-
sa; *d)* el acceso a la historia médica, y *e)* la obligación de producción de estadísticas confiables (CIDH, 2011: 42).

104

El primer elemento implica brindar con oportunidad y de manera ofi-
ciosa la información necesaria, cerciorarse de que la persona usuaria com-
prendió cuáles son sus opciones y consecuencias de las mismas, y verificar
que no existan vicios en el consentimiento.

De acuerdo con lo establecido por la CNDH en la Recomendación General 4/2002, por lo general la obtención del consentimiento de mujeres indígenas sucede en un escenario en el que no se atiende ninguno de estos aspectos. Sobre el particular, señala la falta de pertinencia cultural de los formatos mediante los cuales se busca recabar la firma, que además de encontrarse redactados sólo en español —idioma que dominan de manera escasa o nula— (CNDH, 2002: 11) en muchas ocasiones se encuentra firmado como persona testigo la o el profesional de salud, circunstancia que pone en duda si en efecto se respetó la autonomía de la persona usuaria.

Con relación a este punto, la Comisión, en la Recomendación General 31/2017, manifestó que de los 28 expedientes en los que se acreditó que hubo violencia obstétrica, en nueve se configuró, al haberse violado el derecho a la información y al libre consentimiento (CNDH, 2017b: 99).

El segundo elemento exige el respeto del secreto profesional, en virtud del cual el personal de salud no puede ser criminalizado por abstenerse de revelar información de la o el paciente.

La confidencialidad asegura que la persona pueda manifestar con la confianza suficiente los datos necesarios para emitir un diagnóstico adecuado. Este componente revierte especial importancia tratándose de las y los adolescentes, a quienes, de acuerdo con el Comité DESC, se les debe respetar su confidencialidad y su vida privada (Comité DESC, 2000: 23).

En cuanto al tercer inciso, la CNDH ha conocido de casos en los que la falta de oportunidad, accesibilidad, veracidad y oficiosidad se han configurado a través de conductas que van desde la negativa de brindar información sobre el estado de salud de la persona internada, hasta la esterilización forzada de la mujer.

Por lo que se refiere al acceso a la información y a la historia médica, la SCJN ha señalado que las autoridades deben facilitar a la o el paciente, copias completas del expediente clínico, y no limitarse a entregar sólo un resumen de este último (AR 632/2014: 14).

Por último, respecto del acceso a la información en relación con la obligación de producción de estadísticas confiables, es preciso señalar que se trata de un deber que se refuerza tratándose de personas en situación de vulnerabilidad, ya que es una forma de identificar las manifestaciones de la desigualdad, discriminación y violencia de que pueden ser víctimas. Al respecto, la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (Belem do Pará) conmina al Estado a contar con estadísticas e indicadores para medir el impacto de la violencia, al igual que la efectividad de las medidas adoptadas para su erradicación (artículo 8o.).

105



En este sentido, se valora positivamente el tratamiento que la CNDH comenzó a darle a la violencia ejercida contra la mujer durante la atención médica recibida en el embarazo, a la que denominó “violencia obstétrica”, toda vez que de esta manera es posible dimensionar la frecuencia y detectar la forma en como ocurre; todo lo cual servirá en el diseño de políticas públicas orientadas a mejorar los servicios de salud.

IV. REFLEXIONES FINALES

El expediente clínico constituye una herramienta fundamental para la persona usuaria, ya que representa un medio para satisfacer diversas necesidades de la o el paciente. Por un lado, es un componente esencial para asegurar el acceso a los servicios de salud de manera oportuna y efectiva, y por el otro, sirve para evidenciar la acción u omisión cometidas por el personal de salud, cuestión que resulta relevante cuando el asunto trasciende al ámbito de lo legal.

En este contexto, la Recomendación General 29 de la CNDH se torna en un importante referente, al basarse para su conformación, en la amplia evidencia empírica disponible, y que se posiciona como único en su tipo, en órganos de derechos humanos en México, y con toda probabilidad en el mundo; también sirve como punto de partida para avanzar en las discusiones contemporáneas sobre el derecho a la información en materia de salud.

No obstante lo anterior, existen varios elementos que dicha recomendación dejó en el olvido, y que deberían retomarse en posteriores decisiones de la Comisión sobre este temática.

ALEJANDRO DÍAZ PÉREZ / RITA ASTRID MUCIÑO CORRO

Estos aspectos específicos parten desde la inclusión de marcos normativos, como la Ley General de Transparencia y Acceso a la Información Pública, y/o la Ley Federal de Transparencia y Acceso a la Información Pública; el desarrollo de las obligaciones existentes sobre el derecho a la información en materia de salud, cuando se trata de protección frente a terceros o particulares (deber de proteger), la modificación del enfoque de titularidad y propiedad del expediente clínico, los periodos temporales de su conservación, hasta la obligación de implementar expedientes electrónicos, a través de una profunda reforma de las normas oficiales, y la generación de mecanismos que se dirijan a disminuir la vulnerabilidad de la información.

106

●
○
● Con la introducción de estos múltiples elementos al debate podrían visibilizarse de mejor forma aquellas cuestiones que son especialmente problemáticas para el acceso y tratamiento de los datos personales contenidos en los expedientes clínicos, y que en consecuencia pueda ser mejor garantizado el derecho a la información en materia de salud.

Finalmente, la CNDH, como organismo protector de los derechos humanos, no puede dejar al margen a las personas pertenecientes a los grupos de atención prioritaria. Es indispensable que al abordar la situación jurídica y contextual de un derecho humano en aras de emitir una recomendación general profundice en los agravios que el incumplimiento de las obligaciones estatales trae para las y los integrantes de estos grupos, sin soslayar la manera en que la interacción de las diferentes condiciones dificulta aún más el ejercicio pleno del derecho a la información.

V. FUENTES CONSULTADAS

COMISIÓN INTERAMERICANA DE DERECHOS HUMANOS (CIDH), 2011, “Acceso a la información en materia reproductiva desde una perspectiva de derechos humanos”.

COMISIÓN NACIONAL DE LOS DERECHOS HUMANOS (CNDH), 2002, Recomendación General 4/2002 derivada de las prácticas administrativas que constituyen violaciones a los derechos humanos de los miembros de las comunidades indígenas respecto de la obtención de consentimiento libre e informado para la adopción de métodos de planificación familiar.

COMISIÓN NACIONAL DE LOS DERECHOS HUMANOS (CNDH), 2017a, Recomendación General 29/2017 sobre el expediente clínico como parte del derecho a la información en servicios de salud.

COMISIÓN NACIONAL DE LOS DERECHOS HUMANOS (CNDH), 2017b, Recomendación General 31/2017 sobre violencia obstétrica en el sistema nacional de salud.

COMITÉ DE DERECHOS ECONÓMICOS, SOCIALES Y CULTURALES DE LAS NACIONES UNIDAS (COMITÉ DESC), 2000, Observación General No. 14, sobre “El derecho al disfrute del más alto nivel posible de salud”.

INMUJERES, 2010, *Población usuaria de servicios de salud*, disponible en: 107
<http://estadistica.inmujeres.gob.mx/myhpdf/93.pdf>.

MOREDDU GILABERT, Mariana, 2017, *Regulación jurídica del expediente clínico electrónico*, México, Tirant lo Blanch. ●

ROLDÁN XOPA, José, 2014, “Acceso al expediente médico”, *Derecho a saber: balance y perspectivas cívicas*, sección V. ○ ●

Marco jurídico

Amparo en Revisión 632/2014, 2014, Unanimidad de votos. Ponente: ministro Alberto Pérez Dayán. Secretaria: Georgina Laso de la Vega Romero.

Caso Albán Cornejo y otros vs. Ecuador, 2007, Corte IDH.

Caso Rodríguez Vera y otros vs. Colombia, 2014, Corte IDH.

INAI, criterio 317/17, 24 de septiembre de 2017.

NOM-004-SSA3-2012, Del Expediente Clínico, México.

Principios de París, Principios relativos al estatuto y funcionamiento de las instituciones nacionales de protección y promoción de los derechos humanos.

Reglamento Interno de la Comisión Nacional de los Derechos Humanos.

RESEÑAS BIBLIOGRÁFICAS



LOS LÍMITES DE LA PRIVACIDAD



Óscar ZAVALA GAMBOA*

Sin lugar a dudas, el derecho a la privacidad históricamente ligado a la protección de datos personales se encuentra frente a grandes predicamentos, particularmente ante al desarrollo tecnológico e industrial que se está viviendo. Basta observar los efectos de la denominada *Industria 4.0* o *Cuarta Revolución Industrial*, para advertir que los escenarios son cada vez más complejos, y la privacidad en ámbitos como redes sociales, operaciones financieras, prestación de servicios (nacional o internacional), entre muchos otros más, encuentran obstáculos que hasta hace algunos años hubieran sido impensables, y que permiten cuestionar si verdaderamente el marco jurídico se encuentra listo para afrontar estas novedades.

Así, el desarrollo tecnológico vinculado con lo que algunos consideran como el derecho humano a la comunicación aparece como uno de los grandes temas de la agenda internacional contemporánea, y como ejemplo tenemos a la Unión Internacional de Telecomunicaciones, organismo especializado de la Organización de las Naciones Unidas que promueve el análisis, y sobre todo la conscientización de la importancia que tiene este tema en las sociedades y el interés —tanto del sector público como el privado— por que se discutan y posicionen avances y retos en esta materia.

Por lo anterior, la obra que se reseña del destacado sociólogo norteamericano Amitai Etzioni es una lectura obligada para los interesados en el derecho a la privacidad y la protección de datos personales; sin embargo, considero que tiene una especial relevancia entre los abogados estudiosos de estos temas, ya que la visión sociológica permite identificar nuevas aristas

* Licenciado y maestro en derecho por la Facultad de Derecho, UNAM. Actualmente es secretario de acuerdos y ponencia en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y profesor en la Facultad de Derecho (UNAM) y en la Escuela Libre de Derecho. Correo: ozavalagamboa@derecho.unam.mx.

ÓSCAR ZAVALA GAMBOA

en temas complejos que han sido poco abordados desde el ámbito jurídico, y que muestran un panorama en el que el derecho parece desfasado frente a situaciones actuales, cada vez más presentes de lo que se pueden imaginar.

112 En ese sentido, parece oportuno retomar las palabras del profesor José Ramón Agustina, importante jurista que tiene la encomienda de prologar la obra en comentario. El profesor Agustina comienza señalando que en la obra de Etzioni se analizan los problemas de la privacidad desde una “perspectiva ortodoxa”. Se entiende por ésta a un cambio en el paradigma que resulta “perturbador”, cuestión que resume muy bien la visión que se plasma en esta obra, donde se cuestionan desde los elementos más básicos de la noción de privacidad, hasta su aplicación en problemáticas muy específicas, y que podrían situarse en lo que Ronald Dworkin denominaría como “casos difíciles”.

La obra de Etzioni parte de una premisa fundamental: identificar y aceptar que la noción de privacidad se encuentra en graves predicamentos y en un asedio inigualable. Por ello, el autor se compromete a demostrar que los defensores radicales de la privacidad no sólo han incurrido en excesos retóricos, sino que en su consideración esos excesos han tenido consecuencias significativas y perjudiciales, que son detalladas y analizadas a lo largo de todo el libro. Para tal efecto, el autor no se limita a analizar la cuestión conceptual, sino que va más allá, al plantear escenarios complejos en los que busca sostener la tesis central.

La selección de casos es más que atinada, y permite al lector, confrontar lo que históricamente se ha conocido como derecho a la privacidad —tal vez desde los postulados de Samuel Warren y Louis Brandeis—, con problemáticas actuales, como pruebas de VIH, actos relacionados con delitos sexuales, intervención de comunicaciones, sistemas biométricos y el uso de expedientes médicos, situaciones de actualidad y gran relevancia que llevan a cuestionar si realmente hay un derecho a la privacidad y cuáles deberían ser sus retos y sus limitaciones.

En ese sentido, el autor plantea que los verdaderos retos son identificar cómo puede servirse mejor el bien común en cuestión sin socavar innecesariamente la privacidad, cuáles son los perjuicios concretos que conlleva privilegiar la privacidad, y qué recursos específicos de política pública pueden implementarse para minimizar la reducción de la privacidad que conllevaría el tratamiento de esos perjuicios. Por último, cuestiona cómo se deberían abordar las cuestiones morales, legales y sociales planteadas por los recursos sugeridos.

Como se observa, el profesor Etzioni, de entrada plantea las limitaciones propias de la privacidad como punto de partida; pero la gran ventaja de

esta obra es que el autor sí propone un método de estudio para determinar si la relación entre privacidad y el bien común (entendido como publicidad de la información) es desequilibrada, y entonces qué puede hacerse para corregir ese desequilibrio.

Finalmente, el autor busca construir la idea de un *concepto contemporáneo de privacidad*, en el que se establezcan sus características, pero también sus limitaciones, lo que permita identificar cuáles son sus ámbitos de aplicación y los casos en los que deberá ceder ante el bien común referido.

Sin lugar a dudas, la obra de Amitai Etzioni resulta novedosa y actual (a pesar del tiempo que ha pasado desde que fue escrita y luego traducida), por lo que invito al lector a adentrarse en esta postura diferente, que indudablemente le permitirá cuestionarse sobre los alcances y limitaciones del derecho a la privacidad.

Para concluir, se retomarán las palabras del jurista Miguel Carbonell, y que parecen especialmente importantes, a propósito de la obra que se reseña:

Uno de los signos de las democracias contemporáneas es la separación entre actividades públicas y privadas de los individuos. Si esa separación no existiera se correría el riesgo de caer en alguno de los dos extremos siguientes: o bien se pulverizarían varios de los derechos fundamentales más importantes dentro de la lógica del Estado constitucional (como el derecho a la inviolabilidad del domicilio, la libertad de creencias, la libertad ideológica, la libertad de procreación, etcétera), o bien —en el otro extremo— se diluirían varios de los sistemas de control que actualmente existen para verificar la actuación de las autoridades (las reglas de comportamiento que rigen en el ámbito público son distintas de las que existen en el ámbito privado, y para los funcionarios públicos se crea todo un sistema de mecanismos de verificación que solamente se puede mantener para el caso en que la distinción entre público y privado sea clara) (Carbonell, 2006: 450).

FICHA BIBLIOGRÁFICA DEL LIBRO RESEÑADO

ETZIONI, Amitai, 2012, *Los límites de la privacidad*, Montevideo-Buenos Aires, Editorial B. de F.

OTRA FUENTE

CARBONELL, Miguel, 2006, *Los derechos fundamentales en México*, México, Porrúa.

