



Compilado sobre transparencia,
privacidad y la era digital
del INFO CDMX

REPÚBLICA DE DATOS IA, TRANSPARENCIA Y DERECHOS EN LA NUEVA DEMOCRACIA

Julio César Bonilla Gutiérrez
Mateo Mansilla-Moya
Laura Lizette Enríquez Rodríguez

COORDINADORES

02

U N A M



FACULTAD DE DERECHO

República de Datos IA, transparencia y derechos en la nueva democracia

JULIO CÉSAR BONILLA GUTIÉRREZ
MATEO MANSILLA-MOYA
LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ

Coordinadores





Copyright © 2025 INFO CDMX

Título

República de Datos IA, transparencia y derechos en la nueva democracia

© ***Coordinadores***

Julio César Bonilla Gutiérrez

Mateo Mansilla-Moya

Laura Lizette Enríquez Rodríguez

Compilado sobre Transparencia, Privacidad y la Era Digital del INFO CDMX

Editora

Patricia Daniela Lucio Espino

ISBN: 978-607-642-225-0

UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE DERECHO

Ciudad Universitaria

Coyoacán, 04510

Ciudad de México

www.derecho.unam.mx

La presente obra ha sido dictaminada y aprobada para su publicación, de acuerdo con el sistema de revisión por pares doble ciego, por el Comité Editorial del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México 2025.

Esta obra es de libre acceso por lo que se permite la reproducción parcial o total de su contenido, de sus características de diseño editorial por cualquier forma o medio analógico o digital, permanente o temporal, así como su comunicación pública y distribución, siempre y cuando se le reconozca a cada uno de los autores su derecho de paternidad.

Diseño de interiores y portada UNAM, 2025.

**Comité Editorial del
Instituto de Transparencia,
Acceso a la Información
Pública, Protección de
Datos Personales y
Rendición de Cuentas de la
Ciudad de México 2025**

Mtra. Laura Lizette Enríquez Rodríguez

COMISIONADA PRESIDENTA DEL INFO CDMX

Dr. Julio César Bonilla Gutiérrez

COMISIONADO CIUDADANO DEL INFO CDMX

Dra. Sonia Venegas Álvarez

ESPECIALISTA EXTERNA

Dra. Patricia Daniela Lucio Espino

ESPECIALISTA EXTERNA

Mtro. Juan Gómez Pérez

ESPECIALISTA EXTERNO

Coordinadora del Comité

Lcda. Nora Angelica Damian Santiago

DIRECTORA DE VINCULACIÓN Y
PROYECCIÓN ESTRATÉGICA DEL INFO CDMX

Secretaria Técnica del Comité

Lcda. Georgina Mena López

DIRECTORA DE COMUNICACIÓN
SOCIAL DEL INFO CDMX



Compilado sobre transparencia,
privacidad y la era digital
del INFO CDMX

**Pleno del Instituto de
Transparencia, Acceso a la
Información Pública,
Protección de Datos
Personales y Rendición de
Cuentas de la Ciudad de México**

Laura Lizette Enríquez Rodríguez

COMISIONADA PRESIDENTA
DEL INFO CDMX

Julio César Bonilla Gutiérrez

COMISIONADO CIUDADANO
DEL INFO CDMX

María del Carmen Nava Polina

COMISIONADA CIUDADANA
DEL INFO CDMX



Compilado sobre transparencia,
privacidad y la era digital
del INFO CDMX

Universidad Nacional Autónoma de México

Leonardo Lomelí Vanegas
RECTOR

Patricia Dolores Dávila Aranda
SECRETARIA GENERAL

Facultad de Derecho

Sonia Venegas Álvarez
DIRECTORA

Sarah Mis Palma León
SECRETARIA GENERAL

Coordinación Editorial de la Facultad de Derecho

Patricia Daniela Lucio Espino

COORDINADORA EDITORIAL Y EDITORA

Alan David Barraza Guerrero

Ana María Ramírez Sánchez

COEDITORES Y VALIDACIÓN DE CONTENIDOS

María Concepción Cárdenas Ostria

Cintha Gutiérrez Ruiz

CORRECCIÓN DE ESTILO

Michelle Sánchez Cabello

Ricardo Pérez Rodríguez

DISEÑO EDITORIAL

Jonathan Salvador Bastida Ávila

PROTECCIÓN A LA PROPIEDAD INTELECTUAL

Jennifer Valeria Galicia Bastida

ASISTENTE ADMINISTRATIVO

Mariana Areli Santos Osnaya

Mariana Basilio Añorve

Miguel Hernández Morales

Alicia Monserrat Velázquez Arias

Ximena Guadalupe Viccon Hernández

SERVICIO SOCIAL Y PRÁCTICAS PROFESIONALES

ÍNDICE

PRÓLOGO	15
<i>Dr. Julio César Bonilla Gutiérrez</i>	

CAPÍTULO I

AVANCES Y RETOS DE LA UTILIZACIÓN DE LA INTELIGENCIA ARTIFICIAL EN LA FISCALIZACIÓN SUPERIOR EN EL ÁMBITO DE LA CIUDAD DE MÉXICO

Edwin Meráz Ángeles

I.1. Introducción	19
I.2. Construyendo agenda. Alineación a los objetivos estratégicos	21
I.3. Revisión total y nueva modalidad de muestreo	25
I.4. Estrategia	26
I.5. Hitos	27
I.6. Políticas adoptadas	28
I.7. Riesgos	28
I.8. Conclusión	29
Referencias	29

CAPÍTULO II

ENTRE ALGORITMOS Y DERECHOS: PERSPECTIVAS JURÍDICAS Y POLÍTICAS PARA UNA DEMOCRACIA DIGITAL

Julio César Bonilla Gutiérrez

II.1. Introducción	30
II.2. IA, derechos digitales, transparencia y democracia	31
II.3. Impacto de la tecnología en la democracia.	34
II.3.1. Algunas propuestas prácticas para México	35
II.4. Conclusión	37
Referencias	38

CAPÍTULO III

INTELIGENCIA ARTIFICIAL Y DERECHOS DIGITALES

Adrián Alcalá Méndez

III.1. Introducción	39
III.2. Inteligencia artificial y derechos digitales	40
III.3. Conclusiones	46
Referencias	48

CAPÍTULO IV

INTELIGENCIA ARTIFICIAL Y NEURODERECHOS

Gisela María Pérez Fuentes

IV.1. Introducción	50
IV.2. Sistema de inteligencia artificial	51
IV.2.1. Características del sistema de inteligencia artificial	52
IV.2.2. Progresividad de la inteligencia artificial (<i>machine learning</i> y <i>deep learning</i>)	52
IV.3. De los derechos digitales a los neuroderechos	53
IV.3.1. Significado de los neuroderechos	55
IV.3.2. Protección internacional sobre la ética de la IA	56
IV.4. Conclusiones	57
Referencias	58

CAPÍTULO V

LA INFORMACIÓN PÚBLICA: COMPONENTE DE ACCESO Y EJERCICIO DE LOS DERECHOS
FUNDAMENTALES*Ana Lía de Fátima García García*

V.1. Introducción	59
V.2. Subjetividad sobre el concepto de información y mecanismos de acceso a la información pública	60
V.3. La participación ciudadana y la disponibilidad de la información pública	62
V.4. Conclusión	63
Referencias	63

CAPÍTULO VI

LA TRANSPARENCIA Y EL PODER JUDICIAL

Juan Carlos Abreu y Abreu

VI.1. Preámbulo	64
VI.2. Génesis y evolución de la noción de transparencia	65
VI.3. Taxonomía de la transparencia	66
VI.4. Dimensiones de la transparencia	67
VI.5. La transparencia en el entorno judicial	67
VI.6. Conclusiones	68
Referencias	68

CAPÍTULO VII

INTERPRETACIÓN A LA LEY INTERAMERICANA SOBRE
GESTIÓN DOCUMENTAL: UNA ÓPTICA EN LA DIRECCIÓN DE RECURSOS HUMANOS

Federico Hernández Pacheco

VII.1. Introducción	70
VII.2. Ley Interamericana sobre Gestión Documental y la dirección de los recursos humanos: interpretación	72
VII.3. Conclusiones	79
Referencias	80
Bibliografía complementaria	81

CAPÍTULO VIII

LA PROTECCIÓN DE LOS DATOS PERSONALES DE NIÑEZ Y
ADOLESCENCIA EN EL MUNDO DIGITAL

Aristides Rodrigo Guerrero García

VIII.1. Niñez e internet: sobreexposición y riesgos	82
VIII.2. La actividad internacional en torno a la privacidad de la niñez	84
VIII.3. Estado actual de protección en México	87
VIII.4. Conclusiones	90
Referencias	91

CAPÍTULO IX

INFO CDMX: VANGUARDIA EN LA PROTECCIÓN DE DATOS PERSONALES

Laura Lizette Enríquez Rodríguez

IX.1. Introducción	94
IX.2. Actividad cuasijurisdiccional	95
IX.3. Vigilancia del cumplimiento de principios y disposiciones en materia de protección de datos personales.	96
IX.4. Otras acciones	99
IX.5. Conclusiones	101
Referencias	102

CAPÍTULO X

LAS CINCO GENERACIONES DE LAS NORMAS DE PROTECCIÓN DE DATOS Y EL DERECHO A LA
AUTODETERMINACIÓN INFORMATIVA EN LA JURISPRUDENCIA DE LA CORTE IDH*Oscar Raúl Puccinelli Parucci*

X.1. Introducción. Las cinco generaciones de normas de protección de datos .	103
X.2. El reconocimiento jurisprudencial del derecho a la autodeterminación informativa en el Caso CAJAR de la Corte IDH	109
X.3. Conclusiones	116
Referencias	117
Bibliografía complementaria.	122

CAPÍTULO XI

REVISTA *ABOGACÍA*: DIVULGACIÓN JURÍDICA, DEMOCRACIA Y DERECHOS HUMANOS*Mateo Mansilla-Moya**Ivana Paredes Calderón*

XI.1. Reflexiones preliminares	123
XI.2. Derecho al acceso a la información y revistas de divulgación jurídica . . .	125
XI.3. Revista <i>Abogacía</i> y acceso a la información	128
XI.4. Notas para continuar con la reflexión	129
Referencias	130

CAPÍTULO XII

EL CONOCIMIENTO COMO PRESUPUESTO DE LA LIBERTAD: UN BREVE ANÁLISIS

Diego Bernal Toriello

XII.1. Preámbulo	131
XII.2. El conocimiento	132
XII.3. La libertad	133
XII.4. La relación entre el conocimiento y la libertad	135
XII.5. Importancia del derecho a conocer	136
XII.6. Conclusión	137
Referencias	137

CAPÍTULO XIII

LA PARTICIPACIÓN CIUDADANA ES LA CLAVE FRENTE A LA CRISIS DE CONFIANZA
Y LEGITIMIDAD EN LOS TRIBUNALES MEXICANOS*Fátima Gamboa*

XIII.1. Preámbulo	139
XIII.2. En medio de una crisis de legitimidad y confianza.	140
XIII.3. ¿Cómo mejoramos la participación ciudadana?	141
XIII.4. Nuestra propuesta, un modelo de justicia abierta feminista.	142
Referencias	144

CAPÍTULO XIV

ACCESO A LA ENERGÍA ELÉCTRICA E INTERNET COMO CONDICIÓN *SINE QUA NON*
PARA LA GARANTÍA DE LOS DERECHOS DIGITALES*Andrés Acosta Padilla*

XIV.1. Introducción	145
XIV.2. Acceso a la energía eléctrica en México	145
XIV.3. Acceso a internet y derechos digitales	149
XIV.4. Conclusiones	152
Referencias	152

PRÓLOGO

Nos encontramos frente a una revolución surgida con el uso de las nuevas tecnologías y el desarrollo de la Inteligencia Artificial (IA). Éstas colocan a las sociedades del siglo XXI frente a uno de los mayores desafíos a causa del nivel de sus implicaciones y, al mismo tiempo, también les abre paso a las más grandes oportunidades de nuestra historia reciente: garantizar el ejercicio de los derechos humanos en un equilibrio entre libertad, poder y tecnología.

Tenemos una conversación urgente en esta materia. Estamos llamados a responder a preguntas que marcan la frontera civilizatoria en el contexto actual: ¿cómo garantizar que la inteligencia artificial sirva como auxiliar de las personas y no como herramienta que las sustituya?, ¿cómo controlamos la economía del dato dentro de un marco de derechos humanos? y ¿cómo garantizamos la dignidad humana en la era digital?

Estas son sólo algunas de las múltiples y muy importantes preguntas que debemos hacernos, pero también son impostergables. Dejó de ser un tema del futuro, ahora es una realidad del presente, en la que vivimos, convivimos y nos desarrollamos. Se trata de un diálogo en el cual debemos adentrarnos ahora, con responsabilidad, compromiso y visión.

Por eso, este libro se sitúa en el corazón de ese diálogo. Sus contenidos reflejan la experiencia, compromiso, preocupación y propuestas de sus autoras y autores, quienes desde diversas perspectivas abordan al más alto nivel cada uno de los temas. Se trata de una serie de textos que invitan a repensar nuestras instituciones, nuestras leyes, nuestras prácticas, configuradas en términos digitales.

En principio, la comprensión del origen y la evolución de las normas de protección de datos ocupa un espacio relevante, pues nos permite, a partir de tal revisión, proyectar sus posibles alcances. Así, no deja de ser relevante volver a la formulación alemana del “derecho a la autodeterminación informativa”, hasta estudiar los últimos escaños de estos contenidos que no hacen sino recordarnos que el derecho no es estático, sino dinámico.

También se abordan perspectivas del derecho a la protección de datos personales con un enfoque centrado en niñas, niños y adolescentes, el cual es uno de los grupos que hoy en día se encuentran en el centro de la discusión sobre el uso de la IA. La niñez vive y es parte, como comunidad nativa, de un mundo hiperconectado, digital, en el que su identidad se construye, en muchas ocasiones, fuera de su comprensión. Es por ello por lo que proteger su privacidad no es sólo tarea del derecho, sino una obligación ética y social.

La inteligencia artificial, otro de los grandes ejes que nos reúne, se analiza en varios capítulos de esta obra, los cuales muestran que ésta es el ejemplo del máximo alcance tecnológico hasta el momento. Dos caras de un mismo progreso: de un lado, sus aplicaciones prometen servir a la humanidad, optimizando procesos, acercando la justicia, detectando corrupción, mejorando los servicios públicos; del otro, representa riesgos inéditos para los derechos humanos, para la privacidad, para la igualdad, para la democracia. Esta realidad digital inclusive vislumbra un nuevo umbral que nos hace pensar en neuroderechos.

Pero debemos ser firmes y no cesar en nuestro entusiasmo innovador. No se trata de rechazar la tecnología, tampoco de idealizarla. No obstante, tampoco podemos pensarla en términos neutrales. Nuestro trabajo ha de consistir en diseñar una gobernanza democrática de ella. Una que garantice que no sean cajas negras inaccesibles, sino herramientas auditables, esto es, que las decisiones automatizadas no sustituyan ni determinen el sentido del juicio humano, sino que lo fortalezcan. Que la tecnología amplíe derechos y libertades es nuestra encomienda.

En esa labor la transparencia y el acceso a la información enfrentan un momento crucial y muestran su máximo valor. Su ejercicio es lo que da legitimidad a las instituciones. Una justicia abierta, transparente, cercana, no es sólo una aspiración, sino una condición indispensable para construir la confianza pública y garantizar que cada decisión se encuentre en el marco de la ley y los principios democráticos que la sostienen.

Por lo anterior, esta obra busca que se reflexione, con agudeza, pensamiento crítico y responsabilidad, sobre el papel de la información pública como componente esencial de la era digital. No hay democracia sin información, no hay libertad si el conocimiento es privilegio de unos cuantos, no hay transparencia sin participación ciudadana.

Abordamos con ese compromiso una serie de temas que dan muestra de la realidad que nos rodea, dando cuenta de la crisis de confianza en los tribunales, el conocimiento como presupuesto de la libertad, y el análisis de organismos como INFO CDMX, con los cuales se subraya un tema esencial: las instituciones, por sólidas que sean, sólo encuentran sentido en tanto son instrumentos vivos de la democracia. Y es que la legitimidad no se hereda, se construye y renueva con cada acto de apertura, con cada esfuerzo por integrar a la ciudadanía, con cada decisión que pone en el centro a la persona.

Cada capítulo de esta obra es una aportación al mismo compromiso con una democracia digital incluyente, protectora de derechos y promotora de innovación. Ninguno de estos temas puede abordarse en solitario. Hay una fuerte interrelación entre ellos. Acceso a la información, datos personales, inteligencia artificial, transparencia, participación ciudadana, acceso universal, democracia: todo está conectado. Cada decisión en un ámbito repercute en el otro y de ese entrelazamiento depende la calidad de nuestras democracias en el futuro inmediato.

No encontraremos soluciones definitivas –ningún texto serio podría hacerlo–, pero sí rutas, preguntas, propuestas. Es un llamado a trabajar en conjunto en el diseño de un futuro en el que la tecnología no sustituya la política, en el que la justicia sea un elemento definitorio, en el que el dato no anule a la persona, en el que el algoritmo esté siempre bajo el control de los principios éticos y democráticos.

Este libro es un paso en ese camino a la construcción de nuestra sociedad digital: un llamado a imaginar, con responsabilidad y esperanza, un mundo donde la inteligencia artificial y las nuevas tecnologías estén al servicio de la sociedad.

Que estos diálogos nos animen a no temer al cambio, a asumir, con convicción democrática, el reto de moldear una era digital que nunca olvide que el centro de toda ley, de toda política, de toda tecnología, debe ser siempre la dignidad humana.

Dr. Julio César Bonilla Gutiérrez

Comisionado Ciudadano del INFO CDMX y Académico de la UNAM

CAPÍTULO I

Avances y retos de la utilización de la inteligencia artificial en la fiscalización superior en el ámbito de la Ciudad de México

Edwin Meráz Ángeles¹

SUMARIO: I.1. Introducción; I.2. Construyendo agenda. Alineación a los objetivos estratégicos; I.3. Revisión total y nueva modalidad de muestreo; I.4. Estrategia; I.5. Hitos; I.6. Políticas adoptadas; I.7. Riesgos; I.8. Conclusión.

PALABRAS CLAVE: Fiscalización superior; inteligencia artificial, rendición de cuentas, cuenta pública.

I.1. INTRODUCCIÓN

Estamos atestiguando la democratización de herramientas tecnológicas con capacidades asombrosas para el análisis de información y la generación de contenido, algunas de ellas inclusive de acceso gratuito.

En este sentido, si “los tiempos difíciles crean hombres fuertes; los hombres fuertes crean tiempos fáciles; los tiempos fáciles crean hombres débiles; y los hombres débiles crean tiempos difíciles” (OpenAI, 2025),² se anticipa que la inteligencia artificial (IA) contribuirá a tiempos fáciles que permitan mejorar la gestión de los asuntos de interés general, sin pérdida de resiliencia y fortaleza.

La fiscalización superior, entendida como la facultad del H. Congreso local, que ejerce a través de la Auditoría Superior de la Ciudad de México (ASCM), para revisar, evaluar y pronunciarse respecto de la aplicación de los recursos públicos (ingreso y gasto) y operaciones concluidas (LFSCDMX, 2018, artículo 2o.) enfrenta la gran oportunidad de allegarse de este tipo de herramientas para la creación de valor público, a la vez de fortalecer y empoderar a las personas, tanto servidores públicos como ciudadanos, y a los propios entes auditados. No estamos hablando de un futuro deseable y lejano, sino de una realidad presente que tiene implicaciones económicas,

¹ Auditor Superior de la Ciudad de México.

² “Hard times create strong men. Strong men create good times. Good times create weak men. Weak men create hard times”. Frase popular atribuida a Michael Hopf y solicitada a ChatGPT.

sociales y políticas (consolidación del régimen democrático mediante la rendición de cuentas), así como jurídico-administrativas (certeza del estado de la administración pública, atención de faltas administrativas, combate a la corrupción, etc.).

La fiscalización debe aprovechar los avances tecnológicos para mantenerse relevante y efectiva. ¿Qué sentido tendría una revisión tradicional, prácticamente en papel, en un contexto digital? Desaprovechar los beneficios tecnológicos tendría costos administrativos, políticos y económicos significativos para la Ciudad de México.

Ahora bien, por un momento imaginemos el uso del siguiente *prompt*:³

ASISTENTE DE IA: Con base en la información y documentación contenidas en la Cuenta Pública de la Ciudad de México del ejercicio fiscal 20XX, así como en información complementaria de fuentes públicas, asúmete como el órgano técnico responsable de su fiscalización y lleva a cabo la auditoría del gasto público; presenta los resultados por unidad responsable y rubro de gasto, y muestra las faltas administrativas recurrentes.

Sin detenernos en su claridad, relevancia o pertinencia, este *prompt* nos ejemplifica lo que pretendemos comunicar, a saber, que es un hecho notorio que la IA se constituirá como una herramienta generadora de ventajas importantes para la función de fiscalización superior. La institucionalización de esta herramienta no es cuestión de sí o no, sino de “ya nos tardamos”.

En las siguientes líneas analizaremos, en términos generales, lo que constituye la agenda que se ha fijado la ASCM para implementar el uso de la IA en el cumplimiento de su función revisora, incluyendo los objetivos, metas, políticas, así como las acciones que permiten responder los siguientes planteamientos desde la perspectiva de la fiscalización superior: ¿cuáles son las condiciones actuales y qué retos se enfrentan en materia de fiscalización?, ¿inteligencia artificial, para qué?, ¿estamos listos para iniciar?, ¿cuál será la estrategia y líneas de acción, incluyendo responsables, tareas e hitos?, ¿qué políticas deben establecerse en la ASCM para el uso de IA? y ¿qué riesgos deben gestionarse? De igual forma, buscaremos señalar hasta dónde hemos llegado con relación al diseño y programación.

³ “En el contexto de la inteligencia artificial, especialmente en modelos de lenguaje como ChatGPT, un *prompt* es el texto o instrucción que se le proporciona al modelo para generar una respuesta. Es la entrada que el usuario ofrece para que el modelo pueda generar una salida relevante o adecuada” (ChatGPT, Prompt, 2025).

I.2. CONSTRUYENDO AGENDA. ALINEACIÓN A LOS OBJETIVOS ESTRATÉGICOS

En mayo de 2021, fecha que marcó el inicio de la anterior administración de la Ciudad de México, la ASCM empuñó sus esfuerzos en repensarse para mejorar e innovar, mediante la implementación de un proceso de planeación estratégica que orientara su actuar con un enfoque a resultados. Además de fijar la misión y la visión institucionales, se determinó un resultado al que se debía contribuir y los correspondientes objetivos estratégicos, las estrategias y acciones.

Así, la utilización de la IA, como parte de las acciones, contribuirá a las estrategias relativas a ampliar:

[El] universo de auditorías [y] modernizar la infraestructura informática para eficientar el proceso de revisión [para] reducir la brecha entre el presupuesto ejercido y el auditado (objetivo estratégico) [a efecto de lograr una aportación a la buena administración (resultado). (ASCM, 2021, p. 4).

Imagen 1



Adaptado de ASCM, 2021.

a) Condiciones actuales y sus retos

A la fecha de elaboración de este texto (2024), la ASCM se encuentra en proceso de revisión del Informe de la Cuenta Pública de la Ciudad de México para el ejercicio fiscal de 2023, lo que se traduce en 202 auditorías, que comprenden, a su vez, el análisis del control interno del total de entes.⁴ De los ocho tipos de auditoría que aplica la

⁴ Además de la función de fiscalización superior propiamente dicha, la ASCM ejerce atribuciones complementarias, como la revisión trimestral del avance de la implementación de la normatividad en materia de armonización contable a 52 entes obligados en la Ciudad de México. Ello se traduce en 208 revisiones adicionales a las auditorías referidas, en las que interviene personal tanto administrativo como de auditoría.

ASCM, las auditorías de cumplimiento, financieras, de desempeño, de tecnologías de la información y comunicaciones (TIC) y de obra pública requieren:⁵

1. Análisis de grandes volúmenes de datos: El personal auditor revisa documentación con grandes cantidades de datos financieros y de cumplimiento normativo, con el propósito de identificar transacciones sospechosas, duplicidades, alteraciones en patrones de gasto o incumplimientos normativos.
2. Exhaustiva revisión documental: El personal auditor revisa y analiza contratos, políticas, regulaciones y otros documentos legales para identificar términos no conformes con la norma e incluso cláusulas problemáticas en términos de la regulación correspondiente.
3. Limitaciones para la optimización del muestreo: Por diversas circunstancias, los procesos de muestreo enfrentan el riesgo de no identificar las áreas de mayor riesgo y seleccionar muestras menos representativas. En este sentido, el personal auditor invierte tiempo y recursos en realizar el análisis predictivo para determinar qué áreas (y su muestra) tienen más probabilidades de presentar problemas de cumplimiento.
4. Gestión estructurada de los papeles de trabajo: La redacción y compilación de información de hallazgos, riesgos y demás elementos que conforman los papeles de trabajo de los auditores requiere un seguimiento puntual y meticuloso e, incluso, la puesta en operación de controles para garantizar la integridad de los expedientes de auditoría.

Con relación a las tareas señaladas con anterioridad y en términos de retos, podemos decir, por un lado, que persiste un uso intensivo de papel. A pesar de avances importantes en el uso de plataformas electrónicas para la comunicación, el almacenamiento y procesamiento de la información al interior de la ASCM, así como el flujo de información entre la auditoría y los entes auditados, continúa, en determinados tramos, igual que desde la época virreinal, mediante el uso de papel (oficios diversos, requerimientos, atenciones, solventaciones, incluyendo medios probatorios), lo que implica además traslados físicos con horas-persona, al igual que consumo de combustibles fósiles y de bienes materiales. Por ello, la fiscalización superior debe plantearse disminuir su huella de carbono.

⁵ En este ciclo de fiscalización se ejecutan “80 auditorías de cumplimiento, 63 financieras, 1 financiera y de cumplimiento, 30 de desempeño, 2 auditorías con enfoque en TIC, y 26 de obra pública. A su vez, no se consideró la aplicación de tres tipos de auditorías: de desempeño con enfoque ambiental, auditorías forenses ni auditorías especiales” (ASCM, 2023, p. 8).

Aunado a lo anterior, la fiscalización superior se enfrenta a un reto mayúsculo con relación a la Ciudad de México en sí misma, su tamaño con respecto a los siguientes conceptos:

1. Ingresos anuales de 297.4 miles de millones de pesos (mmdp) (49.4% de recursos propios); (SAF, 2024, p. 32).
2. Un presupuesto ejercido de prácticamente 290 mmdp;
3. 52 entes evaluables en materia de contabilidad gubernamental;
4. 109 entes evaluables en materia de control interno; y
5. 109 entes auditados.⁶

El tamaño sí importa, la fiscalización superior debe ampliar su cobertura, a efecto de contribuir en mayor medida a la transparencia y rendición de cuentas en la capital del país y, por consecuencia, con el fortalecimiento del régimen democrático local.

Otro gran reto deriva de los nuevos enfoques para revisar y evaluar la efectividad del gasto público. Históricamente, la fiscalización de los recursos públicos se ha centrado en enfoques contables, presupuestales, económicos y jurídicos. Recientemente, se ha adoptado un enfoque de evaluación de desempeño, que analiza el cumplimiento de metas y objetivos gubernamentales. Empero, la Reforma Constitucional de 2011 en materia de Derechos Humanos (DDHH) significó no sólo un cambio de paradigma en torno al marco jurídico en la materia, sino también en cuanto a la eficacia de los mismos. En este sentido, si bien es cierto que los DDHH son transversales a las acciones de gobierno, que existen instancias cuyo objeto público se centra en aquellos de diversas formas, también lo es que se carece de una metodología para fiscalizar el vínculo gasto público-eficacia de los derechos humanos. Por tanto, la fiscalización superior debe adoptar en lo futuro un enfoque en los DDHH en cuanto a su eficacia.

b) Inteligencia artificial, ¿para qué?

La inteligencia artificial (IA) es un campo de la informática que se enfoca en crear sistemas y máquinas capaces de realizar tareas que normalmente requieren inteligencia humana. Estas tareas incluyen el aprendizaje, el razonamiento, la percepción y la toma de decisiones. La IA puede abarcar desde algoritmos simples hasta redes neuronales complejas que imitan el funcionamiento del cerebro humano. (ChatGPT, concepto de IA, 2025)

⁶ A saber: 2 órganos de gobierno (más 1 autónomo sectorizado), 16 alcaldías, 20 dependencias, 46 entidades paraestatales, 15 organismos desconcentrados y 9 órganos autónomos.

La IA contribuye con el personal auditor. Para la ASCM la inteligencia artificial tendrá un carácter instrumental en el sentido de que se trata de una herramienta que debe abonar a la fiscalización en auxilio de las personas auditoras para automatizar tareas y procesos, no se pretende, de manera alguna, sustituir al capital humano, sino que las personas responsables de la auditoría tengan a su disposición una herramienta para la aplicación de técnicas de auditoría que permita, en una primera etapa, agilizar, complementar e incrementar la calidad de su trabajo y expandir la frontera del ingreso y gasto auditados. Posteriormente, la información generada permitirá atender (detectar, aminorar e inclusive predecir) faltas administrativas en función de su frecuencia y, eventualmente, un combate a la corrupción más próximo.

Imagen 2



Generada a través de Adobe Firefly, 2025.

En este sentido, el objetivo general de incorporar la IA consiste en transformar para mejorar, aprovechando desde la función de fiscalización superior las ventajas de las nuevas tecnologías, con objeto de incorporar herramientas innovadoras en la aplicación de las técnicas de auditoría y contribuir con ello a la buena administración.

En particular y con relación a los destinatarios de la fiscalización superior:

- a) H. Congreso de la Ciudad de México: Como principal destinatario, el Congreso requiere que su órgano técnico le proporcione bases para el mejor entendimiento y certeza del resultado anual de la cuenta pública y, en un futuro,

cuando el presupuesto basado en resultados tenga un estadio más avanzado, elementos para la asignación anual de recursos vía presupuesto de egresos. Asimismo, la ASCM tiene la obligación de instrumentar las medidas necesarias para prevenir recurrencias en las recomendaciones, de lo cual la información que se rinde a la soberanía debe tener un mayor alcance (LFSCDMX).

- b) Entes auditados: Con un enfoque preventivo, la ASCM proporcionará información integral para la toma de decisiones internas y la implementación de mejoras en la gestión. Al respecto, la IA deberá contribuir a identificar ventanas de oportunidad para la mejora gubernamental, así como la detección de faltas administrativas.
- c) Ciudadanía: Empoderar al ciudadano y a la sociedad civil con información de mayor cobertura y calidad; es decir, se pretende proporcionar elementos para el ciudadano que estudia, investiga, analiza, concluye, exige resultados y, de ser el caso, denuncia desviaciones, contribuyendo así a la transparencia y rendición de cuentas. La ASCM debe asumirse como un garante de las expectativas civiles con relación a los resultados de la fiscalización superior.

Cabe destacar que este esfuerzo de transformación para la mejora se complementa con otras acciones que ya están en ejecución en la ASCM, tales como: 1) la institucionalización del sistema informático para la evaluación del control interno; 2) la implementación de auditorías focalizadas;⁷ y 3) ejecución de auditorías de desempeño con enfoque en derechos humanos.

I.3. REVISIÓN TOTAL Y NUEVA MODALIDAD DE MUESTREO

Ante la posibilidad de procesamiento robusto de cantidades de información medibles en terabytes, el volumen de información a procesar no es una limitante, lo que permitirá a la ASCM ampliar la capacidad de revisión hasta llegar al 100% del objeto de revisión de que se trate, sustituyendo el muestreo estadísticamente representativo previsto por la norma interna vigente a la fecha. (ASCM, 2024)

⁷ La focalización del proceso de revisión y análisis de la información de los sujetos de fiscalización inició a partir de la fiscalización de la Cuenta Pública 2022, con el fin de incrementar la posibilidad de detectar problemas y proponer soluciones particulares. Consiste en identificar áreas de alto riesgo en la etapa de planeación de las auditorías y concentrarse en ellas en la etapa de ejecución. Así, las personas auditoras profundizan en el análisis de la información, mejoran la comprensión de las deficiencias o problemas e identifican soluciones más efectivas.

a) *¿Listos para iniciar?*

Con independencia de la fortaleza institucional para contar con todo tipo de información y documentación necesarias para la revisión de la cuenta pública, es de destacar que una ventaja importante de la transparencia y sentido de responsabilidad de la rendición de cuentas en el ámbito público de la Ciudad de México radica en que su actividad gubernamental está ampliamente documentada. La totalidad de *data*, información y documentación que se requiere para el ejercicio fiscalizador no presenta limitantes en cuanto a su disponibilidad.

Por otra parte, hacia el interior de la ASCM, la convicción de aceptar el cambio a través de la innovación y uso de nuevas tecnologías es patente a nivel directivo y operativo. La capacidad institucional relativa a recursos materiales y capital humano deberá ser evaluada paso a paso.

I.4. ESTRATEGIA

Los trabajos relativos a la incorporación de la IA a los trabajos de auditoría iniciaron entre octubre y noviembre del 2023. Los esfuerzos se centraron, en esta primera etapa, en el método deductivo, de manera que, una vez determinados en general los requerimientos de una revisión, se procediera a la programación correspondiente para incorporar la IA al proceso fiscalizador. El entramado jurídico, vasto y complejo –con aspectos contables, presupuestarios, normativos y financieros–, impidió tener avance alguno; por ello, se decidió cambiar el modelo y el método.

En lugar de un desarrollo rígido inicial, se optó por un modelo de *design as you go*, que permitiera un alto grado de flexibilidad y adaptación a las necesidades de las personas auditoras como usuarias; el diseño pasó a control de personal auditor de manera exclusiva, apoyado, desde luego y como un solo equipo, por el área de tecnologías de la información. Asimismo, de manera inductiva y siguiendo a Alan Turing con el tema enigma, se decidió partir de requerimientos de revisión y resultados ya conocidos generados en auditorías tradicionales previas para entrenar algoritmos de *machine learning*, fijar metas más concretas, así como centrar los requerimientos y alcances del proyecto, estableciendo así un vínculo más estrecho entre herramienta y usuario final.

La magnitud del proyecto de IA con relación a la capacidad con que se cuenta hace necesario ir paso a paso y focalizar el esfuerzo en un tipo de revisión, considerando que la ASCM puede llevar a cabo hasta ocho tipos de auditoría.⁸ Se eligió la auditoría de cumplimiento en licitaciones públicas para la compra de bienes. El objetivo específico consiste en que, para efectos de la Cuenta Pública 2024 de la Ciudad

⁸ “[...] financiera, de obra pública, de desempeño, desempeño con enfoque ambiental, especial, de cumplimiento, de tecnologías de la información y comunicaciones, así como forense” (ASCM, 2025, p. 18).

de México, misma que está en curso de ejecución, el 100% de gasto por compras de bienes licitadas sea auditable bajo este nuevo esquema en sustitución de un muestreo que tradicionalmente ha rondado el 20% del gasto.

I.5. HITOS

Antes de llevar a cabo la programación para auditar propiamente dicha, fue necesario enfrentar circunstancias que no se habían visualizado en un inicio. Por ejemplo, la documentación que se recibe de los entes auditados en la ASCM, en atención a requerimientos de ésta, puede no ser legible, no debidamente clasificada o requerir procesos de validación ante terceras instancias. Derivado de lo anterior fue preciso que los algoritmos de *machine learning* pudieran:

1. Asumir lo que la ASCM requiere en términos de aproximadamente 50 documentos (en el entendido de auditoría de cumplimiento de licitaciones públicas para la compra de bienes);
2. Identificar la calidad de los documentos y, de ser necesario, mejorarlos para su posterior procesamiento (corregir color, distorsiones de texto, etc.);
3. Identificar y clasificar los documentos en función de su naturaleza y vinculación con un requerimiento, extrayendo la información sustancial que corresponda (fechas, números de folio o contrato, destinataria, emisora, etc.);
4. De ser necesario, autenticar de manera automática el documento ante las autoridades competentes;
5. Una vez alimentado de información y documentación, procesadas éstas y definidos y programados los criterios de evaluación, el sistema estará en posibilidades de evaluar finalmente el grado de cumplimiento o incumplimiento, así como de emitir las observaciones y recomendaciones que correspondan, para su incorporación a los informes institucionales correspondientes.

Conviene detenernos un poco en este punto. Un algoritmo de *machine learning* requiere del procesamiento de miles de documentos, entre más, mejor. Habida cuenta de que estamos en presencia de actos de autoridad que, políticamente son responsabilidad de la ASCM y técnicamente lo son de las personas auditoras, se requiere el mayor grado de certeza de los resultados de la IA, por lo que hasta en tanto no se tenga un grado más que razonable de certeza el proyecto no entrará a etapa productiva.

A septiembre del 2024, el porcentaje de avance del proyecto es del 70%, avance que incluye pruebas de funcionalidad; se espera que para diciembre de 2024 el sistema esté en etapa productiva.

I.6. POLÍTICAS ADOPTADAS

Si bien a la fecha de elaboración del presente capítulo el desarrollo de políticas, valores específicos y reglas institucionales para el uso de la IA en la fiscalización están en proceso de integración, se tienen previstas las siguientes:

1. El uso del sistema institucional es obligatorio, pero el uso de cualquier plataforma de IA no se restringe a criterio de la persona auditora usuaria.
2. La retroalimentación de la persona usuaria es bien recibida para la mejora permanente.
3. El uso de la IA debe encajar en términos de sus resultados en el Código de Ética de la ASCM. La utilización para crear sesgos en los resultados o falsear está prohibido.
4. La protección de datos personales es prioritaria sobre cualquier necesidad de procesamiento.
5. Cualquier plataforma debe garantizar la protección de datos personales y la seguridad de la información, en términos de la normatividad aplicable.
6. Todos los resultados del uso de IA están sujetos a la interpretación o supervisión por parte de personal de la ASCM.

I.7. RIESGOS

Los riesgos a gestionar son los siguientes:

1. Confiabilidad en los resultados generados por la IA;
2. Protección de datos personales;
3. Seguridad ante ciberataques;
4. Resistencia al cambio;
5. Curva de aprendizaje sobre todo en aspectos éticos del uso de la IA;
6. Dependencia institucional a plataformas extranjeras;
7. Desconfianza pública en la fiscalización superior en general y en el uso de IA en particular.

I.8. CONCLUSIÓN

La implementación de la inteligencia artificial en la fiscalización superior representa un avance decisivo para optimizar los procesos de auditoría en la ASCM. Este órgano superior de fiscalización ha asumido el reto de integrar estas tecnologías no sólo para aumentar la eficiencia y cobertura de sus auditorías, sino también para mejorar la calidad de la rendición de cuentas y promover la transparencia en la gestión pública.

A pesar de los desafíos que esto conlleva, como la gestión de riesgos asociados a la ciberseguridad, la protección de datos y la curva de aprendizaje institucional, los beneficios potenciales en términos de detección de irregularidades, reducción de la carga administrativa y mejora en la toma de decisiones son incuestionables. Esta transformación no sólo fortalecerá las capacidades técnicas de la ASCM, sino que también contribuirá al fortalecimiento del régimen democrático local, haciendo más accesible y comprensible la fiscalización para la ciudadanía.

REFERENCIAS

- Auditoría Superior de la Ciudad de México (ASCM). (2021). *Planeación estratégica*. <https://ascm.gob.mx/QR/Docs/PE-ASCM-271021.pdf>
- ASCM. (2023). Programa General de Auditoría. Cuenta Pública Ciudad de México 2023. <https://ascm.gob.mx/Pdfs/PGA2023.pdf>
- ASCM. (2025). *Manual del proceso general de fiscalización*. ASCM, Coordinación General Técnica de Auditoría. https://ascm.gob.mx/Transparencia/Pdfs/Art121/I/OAS_MA_02_I.pdf
- Firefly. (2025). *Prompt: auditores públicos e inteligencia artificial*. <https://www.firefly.ai/>
- Ley de Fiscalización Superior de la Ciudad de México (LFSCDMX). (última reforma: 27 de noviembre de 2018). *Gaceta Oficial de la Ciudad de México (GOCM)*. https://data.consejeria.cdmx.gob.mx/images/leyes/leyes/LEY_DE_FISCALIZACION_SUPERIOR_DE_LA_CDMX_2.pdf
- OpenAI. (2025). ChatGPT (versión GPT-4o) [Modelo de lenguaje]. <https://openai.com/es-ES/>
- Secretaría de Administración y Finanzas (SAF). (2024). *Informe de la Cuenta Pública 2023. Tomo I. Resultados generales*. SAF. https://servidoresx3.finanzas.cdmx.gob.mx/egresos/cp2023_24/

CAPÍTULO II

Entre algoritmos y derechos: perspectivas jurídicas y políticas para una democracia digital

Julio César Bonilla Gutiérrez¹

SUMARIO: II.1. Introducción; II.2. IA, derechos digitales, transparencia y democracia; II.3. Impacto de la tecnología en la democracia; II.3.1. Algunas propuestas prácticas para México; II.4. Conclusión.

PALABRAS CLAVE: Inteligencia artificial (IA), derechos digitales, transparencia, democracia.

II.1. INTRODUCCIÓN

En el tejido de nuestra existencia contemporánea, donde la tecnología borda patrones complejos en el tapiz de la vida diaria, la inteligencia artificial (IA) no sólo se revela como una fuerza de innovación, sino también como una esfera de influencia crítica para los derechos digitales que hemos ido imaginando y construyendo, así como para la estructura de nuestra democracia.

Al paso acelerado de los avances tecnológicos, se le suma la urgencia de navegar y moldear estos impresionantes desarrollos con un compromiso firme hacia la transparencia, el acceso a la información, la protección de los datos personales, la privacidad, la intimidad y autodeterminación informativa de las personas, así como con la rendición de cuentas. En ese sentido, el presente ejercicio reflexivo pretende ser un recorrido proactivo por el panorama de la inteligencia artificial y los derechos digitales, enfocándose en cómo estos componentes son vitales para cimentar una democracia más sólida y transparente.

Así, el propósito de este diálogo escrito es múltiple. Primero, operar y servir como una herramienta de consulta que recoge y valora las perspectivas críticas y propositi-

¹ Comisionado Ciudadano del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX). Coordinador del Grupo de Transparencia Judicial de la Red de Transparencia y Acceso a la Información (RTA). Doctor en Derecho con mención honorífica por la División de Estudios de Posgrado de la Facultad de Derecho de la Universidad Nacional Autónoma de México (UNAM). Realizó una estancia posdoctoral en la Universidad de Salamanca. Miembro del Sistema Nacional de Investigadores (SIN) y Académico de la UNAM.

vas, tanto en lo legal como en lo político, con el objeto de fungir como un espacio de encuentro para voces expertas que buscan delinear los contornos de los desafíos actuales y trazar rutas hacia soluciones innovadoras que refuercen los pilares de nuestra convivencia democrática.

Segundo, este trabajo persigue cultivar una cultura de justicia y legalidad; en un escenario dominado por disrupciones tecnológicas, en el cual es esencial mantener un equilibrio donde el progreso tecnológico camine de la mano con la ética y la legalidad. Al explorar la interacción entre la inteligencia artificial y los marcos legales desde un lente como éste, aspiramos a ser un catalizador para la formulación y el fortalecimiento de normativas que resguarden la integridad digital de las personas.

En tal virtud, el presente texto promueve un diálogo democrático sobre cuestiones vitales que afectan las libertades y los derechos humanos, así como las instituciones encargadas de su protección. Este diálogo es crucial para asegurar que la adopción de tecnologías disruptivas, como la inteligencia artificial, sea continuamente examinada, y que su evolución se alinee con los principios democráticos fundamentales. Asimismo, esta conversación busca empoderar a las personas, equipándolas con conocimientos útiles y necesarios para entender y ejercer sus derechos en un mundo cada vez más gobernado por el código digital.

II.2. IA, DERECHOS DIGITALES, TRANSPARENCIA Y DEMOCRACIA

En el corazón de la modernidad tecnológica, las inteligencias artificiales que hemos desarrollado se nos presentan como una amalgama de algoritmos y sistemas capaces de ejecutar tareas que, históricamente, requerían la intervención humana; o bien, dicho de un modo técnico, como un conjunto de *software* y *hardware* inteligente capaz de realizar tareas a las que subyace “la elucidación del proceso de aprendizaje humano, la cuantificación del proceso de pensamiento humano, la explicación del comportamiento humano y la comprensión de lo que hace posible la inteligencia” (Lee y Qiufan, 2021, p. XI). Concebida así, la IA representa nuestro último paso como humanidad en el viaje para entendernos a nosotros mismos.

Dichas tareas abarcan desde el reconocimiento de patrones y la toma de decisiones hasta la interpretación y generación de lenguaje natural. No obstante, el término “inteligencia” no debe confundirse con la comprensión humana; la IA *no entiende* en el sentido convencional e, incluso, emocional, que solemos atribuirle al término entendimiento, sino que procesa información y produce resultados basados en los datos que recibe.

Ahora bien, en lo tocante a los derechos digitales, es preciso decir que, en la actualidad, se habla de “la aparición de esta nueva gama de derechos directamente relacionados con la sociedad de la información”, los cuales, para algunos autores,

configuran lo que denominan una cuarta generación u ola de derechos humanos que, a su vez, conciben como el resultado de nuevas reivindicaciones de la ciudadanía derivadas de las profundas transformaciones tecnológicas que hemos alcanzado (Riofrío Martínez-Villalba, 2014, pp. 16-17). Y, cuyas implicaciones, en realidad, debidamente consideradas, claramente trascienden al terreno de lo político en muchos sentidos. Ello, porque dichas implicaciones ya tienen, desde ahora, y previsiblemente pueden cobrar aún mayor relevancia en relación con la distribución, el ejercicio y las consecuencias del poder al interior de las sociedades y comunidades políticas (Hay, 2002, pp. 168-193). Esto, en razón de su casi omnipresente existencia.

Lo anterior, sobre todo, si consideramos que, tanto el internet como el espacio digital, más allá de “ser fuente de acumulación de poder económico y político”, deben ser pensados como bienes colectivos y, en tal virtud, deben ser regulados y resguardados (Morales, 2019, pp. 47-50). Asumir lo anterior, evidentemente, implica concebir que la actividad de las personas usuarias en el espacio digital debe tener y contar con la debida y oportuna intervención de los Estados para garantizar a todas ellas, no sólo el acceso democrático al referido espacio digital, sino también la libertad de expresión y sus derechos correlativos, su seguridad personal e integridad, el derecho al acceso a la información que respete los principios de transparencia, no discriminación, pluralismo, veracidad, así como el derecho a la intimidad y privacidad de las personas.

En otras palabras, puesto de un modo sencillo, los derechos digitales son la extensión o proyección de las libertades y los derechos fundamentales al entorno digital e incluyen tanto los referidos derechos como aquellos que, progresivamente y a partir de estos primeros, debamos y podamos imaginar al resultar necesarios en razón de los vertiginosos cambios que a diario experimentamos, y cuyos alcances futuros aún no conocemos o sospechamos. Estos derechos y libertades, en todo caso, ya son y, sin duda, seguirán siendo fundamentales para asegurar que las tecnologías, como las IA, se desarrollen y apliquen de maneras que respeten la dignidad y la autonomía humanas.

Para tales efectos, es preciso comprender la relevancia que tiene la *transparencia* en el contexto digital, la cual se refiere a la claridad con la que las instituciones y las tecnologías operan de cara a las personas usuarias de las muy diversas plataformas existentes. Al respecto, es claro, implica una apertura que permite a las personas entender y evaluar cómo se toman las decisiones que les afectan, especialmente aquellas mediadas por algoritmos. Lo anterior, a pesar de que, en realidad, tan sólo por dar un ejemplo, aún en la presencia de la referida y necesaria transparencia, pareciera poco práctico esperar que las y los usuarios comprendamos las explicaciones de uso de datos de cada compañía cada vez que se nos pregunta si consentimos la recolección de nuestros datos. Además, porque, si bien la transparencia, la responsabilidad y la confidencialidad de datos son claramente principios cuya aplicación es deseable y cuya incorporación ha sido hecha en diversa normativa nacional e internacional, en los hechos es difícil limitar el propósito de cada pieza de datos recopilados, porque la

IA es un ejercicio extenso y, por ello, es inviable enumerar todos los usos y propósitos futuros o posibles para cada pieza de datos recopilados cuando comienza la recolección (Lee y Qiufan, 2021, p. 396).²

En este contexto, la protección de datos personales se ha convertido en un aspecto crítico de los derechos digitales. Ello, porque los sistemas de IA pueden procesar enormes cantidades de datos personales para aprender y tomar decisiones. En esta medida, es claro que la manera en que estos datos se recopilan, almacenan, usan y comparten, plantea serias preguntas sobre la privacidad y la seguridad.

En tal sentido, la rendición de cuentas en el uso de la IA es fundamental para garantizar que cualquier acción tomada, por o con el apoyo de sistemas automáticos, pueda ser rastreada y justificada. Esto es crucial en la prevención de abusos y en la garantía de que se puedan identificar y corregir errores de manera efectiva. La rendición de cuentas está intrínsecamente ligada a la transparencia, ya que sin una visión clara de cómo operan los sistemas de IA, no se puede asegurar una responsabilidad efectiva de los desarrolladores y organizaciones que emplean estas tecnologías. Aseguramiento que, al pasar por los deberes del Estado y sus instituciones, también lo hace, sin duda, por el acceso a la información pública como libertad y derecho humano fundamental para toda democracia sustantiva.

En mérito de todo lo hasta aquí expresado, los conceptos de inteligencia artificial, derechos digitales, transparencia y acceso a la información pública están profundamente interconectados entre sí. Por ejemplo, una IA que se utiliza en el sector público debe ser transparente y debidamente informada en cuanto a sus alcances de cara a las personas, para que las mismas entiendan cómo se toman las decisiones que les afectan y garantizar que se adopten sin sesgos y en concordancia con estándares éticos (Boobier, 2022, p. 202). Simultáneamente, es claro, debe respetar los derechos digitales, asegurando que la privacidad y la protección de datos personales no se vean comprometidas.

Así, han quedado explicitados no sólo los términos clave, sino también su interrelación, respecto de la cual debe subrayarse la importancia de un equilibrio entre el avance tecnológico y la protección de los derechos humanos fundamentales en la sociedad digital. Esta comprensión es esencial para forjar políticas y prácticas que apoyen una democracia verdaderamente robusta y transparente en la era digital.

² En específico, la mención de que, por ejemplo, cuando Gmail, inicialmente, guardaba todos nuestros correos electrónicos era para ayudarnos a buscar y encontrar cualquiera de ellos con mayor facilidad. Pero, más tarde, cuando desarrolló la nueva función de autocompletado, necesitaba entrenar con los datos antiguos y así lo hizo. Ello, al tratarse de un proceso extenso y aditivo que se va construyendo y evoluciona con el tiempo y con base en los desarrollos previos.

II.3. IMPACTO DE LA TECNOLOGÍA EN LA DEMOCRACIA

La integración de la inteligencia artificial en los procesos democráticos ha generado y representa un terreno fértil, tanto para oportunidades expansivas que sirvan al arraigo y consolidación de una cultura democrática en la sociedad como para el surgimiento de desafíos significativos. La IA puede potenciar la democracia al mejorar la eficiencia de los servicios públicos, personalizar la interacción entre ciudadanos y gobierno, así como facilitar procesos electorales más seguros (Boobier, 2022, pp. xix-xxvi). Por ejemplo, sistemas automatizados pueden ayudar a verificar identidades de manera más rápida y segura durante las elecciones, reduciendo las posibilidades de fraude electoral y aumentando la transparencia del proceso en su conjunto.

Sin embargo, estas tecnologías también presentan desafíos a los principios democráticos fundamentales, como la igualdad, la equidad, la transparencia y la rendición de cuentas. Un desafío prominente es el riesgo de sesgo en los algoritmos de IA, que pueden perpetuar o incluso exacerbar desigualdades existentes si no se diseñan o entrenan adecuadamente. Además, el efecto de *caja negra* de algunos sistemas de IA puede obstaculizar la transparencia, ya que los procesos de toma de decisiones automatizados que este tipo de tecnologías son capaces de adoptar, no siempre son interpretables o, siquiera, entendibles por los humanos.

Un ejemplo ilustrativo de la influencia de la tecnología en la transparencia es el uso de algoritmos en la asignación de recursos gubernamentales. En teoría, estos sistemas podrían optimizar la distribución de recursos para maximizar la utilidad pública; sin embargo, sin los controles adecuados también podrían ocultar decisiones injustas detrás de la fachada de neutralidad tecnológica (Boobier, 2022, pp. 17-30). Otro caso es el de las *fake news* o falsas noticias y campañas de desinformación amplificadas por plataformas de redes sociales, que utilizan algoritmos de IA para maximizar el involucramiento del público usuario, sin consideración alguna respecto de la veracidad de las cosas que se difunden de este modo. Esto, claramente, afecta la calidad de la información que reciben las personas y, por ende, la integridad de los procesos democráticos, tanto electorales como no electorales, es decir, al diálogo público. Ello, claro, en una comprensión instrumental de la democracia que, por supuesto, por mucho trasciende las cuestiones mera y formalmente electorales para concebir la existencia y el papel de toda institución integrante del aparato estatal, como medios para llevar a cabo las inclusiones democráticas que les corresponde realizar frente a las personas en su específico ámbito de competencia.

El despliegue de la IA en contextos democráticos presenta desafíos legales significativos, especialmente en torno a la protección de datos personales y privacidad. Las diversas regulaciones existentes, nacionales y regionales, proporcionan un marco para abordar algunos de estos desafíos. Sin embargo, la rapidez con que evoluciona la tecnología a menudo supera la capacidad de las leyes actuales para mantener el ritmo y actualizarse frente a tales avances. Además, la IA plantea cuestiones éticas profundas,

como la determinación de quién es responsable cuando un algoritmo causa daño. Estas cuestiones requieren un diálogo continuo entre tecnólogos, legisladores y sociedad civil en su conjunto, para asegurar que la tecnología sea utilizada y empleada en los hechos, de manera que respete los derechos humanos y, a su vez, fortalezca tanto a las instituciones como a las prácticas democráticas.

Paralelamente, la IA ofrece oportunidades sin precedentes para mejorar la participación ciudadana y la rendición de cuentas en la gestión pública. Las herramientas de IA pueden ser utilizadas para personalizar la comunicación entre gobiernos y ciudadanos, ofreciendo a estos últimos una mayor capacidad para seguir y entender las acciones de sus representantes. Además, tecnologías de procesamiento de lenguaje natural podrían permitir a los ciudadanos acceder y analizar grandes volúmenes de documentos públicos rápidamente, facilitando una participación más informada y efectiva en los asuntos públicos.

En tal inteligencia, el presente trabajo busca ser una llamada a la acción para que expertos, juristas y políticos aporten sus perspectivas sobre cómo la IA puede servir mejor a los principios democráticos. Es crucial que estas voces plurales y, a veces divergentes, participen en la configuración de las políticas que guiarán el desarrollo de la tecnología en la esfera pública. La contribución de una amplia gama de expertos asegurará que las políticas no sólo sean tecnológicamente factibles, sino también socialmente justas y orientadas hacia el fortalecimiento de la democracia.

Imaginemos, por ejemplo, foros y paneles, que incluyan tanto a tecnólogos como a miembros del público, en los que se puedan explicar y explorar las implicaciones de la IA en términos accesibles. Talleres prácticos, en los que las y los ciudadanos puedan interactuar con tecnologías de IA y ver de primera mano cómo podrían impactar su vida diaria y su participación cívica, también son esenciales. Estas iniciativas pueden ayudar a desmitificar la tecnología y fomentar un entendimiento más profundo y crítico de su papel en la sociedad.

II.3.1. ALGUNAS PROPUESTAS PRÁCTICAS PARA MÉXICO

La integración de la tecnología en la práctica democrática en México es un desafío y una oportunidad crucial en la era digital. Algo imperativo es proceder sin demora a la implementación de plataformas digitales de participación ciudadana más allá de la mera gestión de trámites y solicitud de información. Estas plataformas deben ser diseñadas para facilitar la participación directa de las personas en los procesos legislativos y de toma de decisiones gubernamentales. Las plataformas pueden incluir foros de discusión, encuestas en línea y votaciones electrónicas sobre temas específicos, permitiendo así una mayor inclusión y representatividad en la toma de decisiones políticas que, en el agregado, abonan a la legitimidad democrática. Además, estas

herramientas pueden fortalecer la transparencia y la confianza en el sistema democrático al permitir a los ciudadanos acceder y contribuir a los debates públicos y políticos de manera directa y en tiempo real.

Otra recomendación clave es la promoción de la educación digital y la capacitación tanto para ciudadanos como para servidores públicos. La alfabetización digital es esencial para garantizar que todas las personas puedan participar plenamente en la democracia digital. Esto implica no sólo enseñar a utilizar herramientas tecnológicas, sino también comprender su impacto en la sustancia democrática y cómo pueden ser utilizadas para mejorar la transparencia y la eficiencia en la administración pública y en todas las instituciones que conforman al aparato del Estado. Los programas de capacitación deben incluir módulos sobre ciberseguridad, privacidad de datos y ética digital, asegurando que, tanto los ciudadanos como los servidores públicos, cuenten con las herramientas necesarias y estén equipados para navegar en el entorno digital de manera segura y responsable.

La transparencia y el acceso a la información son pilares fundamentales para una democracia efectiva. Es crucial desarrollar y fortalecer sistemas que permitan el acceso abierto a datos gubernamentales y decisiones políticas. La implementación de tecnologías como *blockchain* puede ser una solución efectiva para aumentar la transparencia y la confianza pública, al permitir la verificación de la información y la trazabilidad de las decisiones, asegurando que los registros no puedan ser alterados una vez que han sido creados. Esto puede ser particularmente útil en la gestión de contratos gubernamentales, presupuestos y procesos electorales, proporcionando una capa adicional de seguridad y confianza.

Por otro lado, el fomento de la participación inclusiva es esencial para asegurar que todos los ciudadanos tengan la oportunidad de participar activamente en los procesos democráticos. Esto implica diseñar aplicaciones y plataformas accesibles para personas con discapacidades, comunidades rurales, indígenas y otros grupos vulnerables. La accesibilidad debe ser una consideración central en el diseño de cualquier herramienta digital, asegurando que las barreras tecnológicas no excluyan a ningún segmento de la población. Además, esto es lógico, se deben implementar programas de divulgación y educación específicos para estos grupos, proporcionando el apoyo necesario para que puedan utilizar las herramientas digitales de manera efectiva.

Asimismo, fortalecer la legislación y las políticas públicas en torno a la inteligencia artificial y los derechos digitales es crucial para asegurar que el desarrollo y uso de estas tecnologías se realice de manera ética y responsable. Desarrollar un marco regulatorio claro y específico para la implementación y el uso de la inteligencia artificial en diferentes sectores es una prioridad innegable. Este marco debe abordar cuestiones éticas, de privacidad y de responsabilidad, asegurando que las tecnologías de IA se utilicen de manera justa, equitativa y transparente. Las normativas deberán incluir directrices claras sobre la recopilación y el uso de datos, la transparencia en los algoritmos y la rendición de cuentas de los desarrolladores y usuarios de IA.

La protección de los derechos digitales es otra área que debemos atender. Es necesario fortalecer las leyes existentes y crear nuevas normativas que protejan los derechos digitales de los ciudadanos, incluyendo la protección de datos personales, la privacidad en línea y la libertad de expresión en el entorno digital. Esto implica desarrollar políticas de privacidad robustas, implementar medidas de seguridad para la protección de datos y asegurar que las plataformas digitales cumplan con los estándares de protección de datos. Además, se deben establecer mecanismos claros para que los ciudadanos puedan ejercer sus derechos digitales y buscar reparación en caso de violaciones.

Fomentar la investigación y el desarrollo en inteligencia artificial es esencial para mantener a México a la vanguardia de la innovación tecnológica. El gobierno debe apoyar la investigación y el desarrollo de tecnologías de IA a través de subsidios, incentivos fiscales y colaboración entre el sector público y privado. Esto debe ir acompañado de directrices claras sobre el uso ético y responsable de estas tecnologías. La inversión en investigación y desarrollo no sólo fomentará la innovación, sino que también ayudará a crear empleos y fortalecer la economía digital de México. Además, es importante promover la colaboración internacional en investigación de IA, participando en proyectos y consorcios globales que puedan beneficiar a México.

II.4. CONCLUSIÓN

La convergencia entre inteligencia artificial y derechos digitales en el marco de una democracia digital presenta tanto retos como oportunidades significativas. Este trabajo ha explorado cómo la tecnología puede ser una herramienta poderosa para fortalecer la transparencia, la participación ciudadana y la protección de derechos fundamentales. Al adoptar plataformas digitales de participación ciudadana, promover la educación y la capacitación digital, y desarrollar marcos regulatorios claros y éticos para la inteligencia artificial, podemos avanzar hacia una democracia más inclusiva, transparente y eficiente.

La implementación de tecnologías como *blockchain* para la transparencia y la votación electrónica segura son pasos cruciales para garantizar la integridad y la confianza en los procesos democráticos. Además, la protección de los derechos digitales y la privacidad constituyen pilares esenciales para asegurar que el desarrollo tecnológico respete y promueva la dignidad y la autonomía humanas.

En este viaje hacia una democracia digital, mejor y posible, es vital fomentar la investigación y la colaboración tanto a nivel nacional como internacional. Sólo mediante un esfuerzo conjunto entre ciudadanos, gobiernos y sectores privados podemos enfrentar los desafíos y aprovechar las oportunidades que la inteligencia artificial y las tecnologías digitales nos ofrecen.

Este es un momento de transformación y esperanza. Con visión, compromiso y acción, en México habremos de encontrar el camino hacia un futuro en el que la tecnología y la democracia se entrelacen para crear una sociedad más justa, equitativa informada y participativa.

REFERENCIAS

- Boobier, T. (2022). *AI and the future of the public sector. The creation of public sector 4.0*. John Wiley & Sons.
- Hay, C. (2002). *Political analysis. A critical introduction*. Palgrave Macmillan; Red Globe Press.
- Lee, K. F. y Qiufan, C. (2021). *AI 2041. Ten visions for our future*. Crown Currency; Penguin Random House.
- Morales, S. (2019). Derechos digitales y regulación de internet. Aspectos claves de la apropiación de tecnologías digitales. En A. L. Rivoir y M. J. Morales (Eds.). *Tecnologías digitales. Miradas críticas de la apropiación en América Latina*. CLACSO.
- Riofrío Martínez-Villalba, J. C. (2014). La Cuarta Ola de Derechos Humanos: los derechos digitales. *Revista Latinoamericana de Derechos Humanos*, Semestre I, 25(1). <https://ssrn.com/abstract=2515038>

CAPÍTULO III

Inteligencia artificial y derechos digitales

Adrián Alcalá Méndez¹

SUMARIO: III.1. Introducción; III.2. Inteligencia artificial y derechos digitales; III.3. Conclusiones.

PALABRAS CLAVE: Inteligencia artificial, datos personales, datos masivos (*big data*), tecnologías de la información y comunicación, derecho a la protección de datos personales, aprendizaje automático (*machine learning*), aprendizaje profundo (*deep learning*).

III.1. INTRODUCCIÓN

El reconocimiento constitucional del derecho fundamental a la protección de los datos personales ocurrió mediante la Reforma del 1 de junio de 2009, que añadió un segundo párrafo al artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), y que estableció esencialmente: “Toda persona tiene derecho a la protección de sus datos personales, así como a su acceso, rectificación y cancelación, y a manifestar su oposición” (DOF, 2009).

A partir de esa fecha, el desarrollo de las tecnologías de la información y comunicación ha crecido exponencialmente, evolucionando de manera acelerada y modificando las interacciones y relaciones entre personas en distintas partes del mundo, así como los dispositivos electrónicos.

Entre las tecnologías más avanzadas, se puede destacar el uso de la *inteligencia artificial* (IA), que se define como el empleo de algoritmos para crear sistemas informáticos y dispositivos capaces de aprender y resolver situaciones ante condiciones específicas. En esencia, estos sistemas buscan imitar el razonamiento humano a través del análisis masivo de información, que a menudo incluye datos personales.

En este contexto, la IA puede parecer un concepto sacado de la ciencia ficción, ya que numerosos programas de televisión y películas han mostrado las maravillas que la

¹ Licenciado en Derecho, Maestro en Amparo y Doctorante en Derecho. Fue Comisionado del extinto INAI (2022-2027), siendo el último Presidente. Fue Consejero Propietario del Instituto de Transparencia y Acceso a la Información Pública del Estado de Baja California y el primer Consejero Presidente en 2011. De 2014 a 2020 fue Secretario de Acceso a la Información en el entonces mismo Instituto Nacional. Ha sido conferencista, panelista y articulista sobre derecho de acceso a la información y protección de datos personales.

imaginación humana puede crear mediante el uso y aplicación de la tecnología. Sin embargo, la inteligencia artificial no es algo ajeno a nuestra vida cotidiana. De hecho, está más presente que nunca en diversas áreas de la vida diaria, muchas veces sin que las personas se den cuenta o reflexionen sobre ello. Ejemplos de su uso incluyen los correctores ortográficos en herramientas de procesamiento de texto, las aplicaciones de asistencia en los dispositivos móviles que funcionan mediante comandos de voz, las recomendaciones de canciones o películas basadas en un análisis de gustos y preferencias o el cálculo de rutas de transporte utilizando sistemas de posicionamiento global.

Es relevante destacar que el orden jurídico nacional no incluye preceptos normativos específicos para regular la protección de los datos personales utilizados en el desarrollo y aplicación de la inteligencia artificial. No obstante, las leyes existentes en la materia contemplan principios, deberes y obligaciones suficientemente generales que pueden aplicarse a las personas físicas y jurídicas, tanto públicas como privadas, responsables del tratamiento de información personal.

III.2. INTELIGENCIA ARTIFICIAL Y DERECHOS DIGITALES

La evolución y penetración de la inteligencia artificial han fortalecido diversos sectores productivos, económicos e industriales, propiciando la automatización de procesos y facilitando el análisis de información a gran escala. Esto ha impulsado significativamente el comercio electrónico y la prestación de servicios digitales.

Sin embargo, junto con los innumerables beneficios que el desarrollo tecnológico ha aportado a la sociedad, también surgen dudas e incertidumbres sobre el funcionamiento de las tecnologías basadas en IA y el tratamiento de los datos personales que recopilan y utilizan, ante el posible mal uso de esta información.

Por tal motivo, para entender con claridad el escenario del orden jurídico actual en la materia, resulta indispensable, en principio, definir la *inteligencia artificial* como “una rama de las ciencias computacionales encargada de estudiar modelos de cómputo capaces de realizar actividades propias de los seres humanos en base a dos de sus características primordiales: el razonamiento y la conducta” (López Takeyas, 2007, p. 1). Es importante mencionar que no existe una definición particular de IA, lo cual ha llevado a diversos autores a desarrollar su contenido desde múltiples puntos de vista, dependiendo en gran medida de su área de conocimiento. Por ejemplo:

Marvin Minsky (1956): “Es la ciencia de hacer que las máquinas hagan cosas que requerirían inteligencia si las hubiera hecho un humano”.

Alan Turing (1950): “[Es una] disciplina científica y tecnológica cuyo objetivo es crear procesos de la mente y su conexión con el cuerpo a través de la metáfora computacional”. (INAI, 2022, p. 12)

Empero, para efectos de este trabajo, resulta ilustrativo el concepto esbozado por la Red Iberoamericana de Protección de Datos (RIPD) en las *Recomendaciones generales para el tratamiento de datos en la inteligencia artificial*, a saber:

[En] su concepción amplia, se trata de un término “sombrija” que incluye una variedad de técnicas computacionales y de procesos enfocados a mejorar la capacidad de las máquinas para realizar muchas actividades, los que comprenden desde modelos algorítmicos, pasando por los sistemas de *machine learning*, hasta llegar a las técnicas de *deep learning* [...]. (RIPD, 2019b, p. 6)

En este sentido, es pertinente señalar que en el campo de la inteligencia artificial se contemplan dos tipos de actividades, a través de las cuales los ordenadores llevan a cabo las funciones para las que son programados: por un lado, el aprendizaje automatizado (*machine learning*), que puede entenderse como una rama específica de la inteligencia artificial que dota a los sistemas informáticos de la capacidad de aprender por sí mismos y mejorar automáticamente sin necesitar programación adicional (UCSP, s.f.); y, por otro, el aprendizaje profundo (*deep learning*), que consiste en redes neuronales que intentan simular el comportamiento del cerebro humano mediante una combinación de entradas de datos que permite aprender de grandes cantidades de información. Este enfoque, a través de diversas capas, ayuda a optimizar y refinar la precisión de las predicciones (Holdsworth y Scapicchio, s.f.).

De esta manera, mientras la inteligencia artificial ofrece muchos beneficios a diversos sectores industriales (académicos, económicos y tecnológicos), también genera expectativas sobre su funcionamiento e impacto en los derechos y libertades de las personas usuarias de estas tecnologías. Esto es así porque la IA se basa en la obtención, procesamiento e interpretación de grandes cantidades de información y datos masivos (*big data*), entre los cuales, incuestionablemente, se encuentran los datos personales.

Por tal motivo, amplios sectores de la población mundial han expresado su preocupación acerca de que los desarrolladores de esta tecnología y, más aún, quienes la utilizan en su beneficio, respeten y se apeguen al marco jurídico que garantiza el derecho fundamental a la protección de los datos personales.

En esa tesitura, en los Estados Unidos Mexicanos, los artículos 6o., apartado A, fracción II, y 16, párrafo segundo de la CPEUM establecen, fundamentalmente, que la información relativa a la vida privada y los datos personales será protegida según los términos que fijen las leyes, y que toda persona tiene derecho a la protección de sus datos personales, así como a solicitar su acceso, rectificación, cancelación y a manifestar su oposición.

Con base en lo anterior, el 5 de julio de 2010, se publicó en el *Diario Oficial de la Federación* la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), cuyo artículo 1o. establece que su objetivo es “regular el tratamiento legítimo, controlado e informado [de los datos personales, garantizando así] la priva-

cidad y el derecho a la autodeterminación informativa de las personas” (LFPDPPP, 2010). De igual manera, el 21 de diciembre de 2011 se publicó en el mismo medio oficial el Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP), con el propósito de detallar las disposiciones contenidas en la ley federal.

Posteriormente, con el objetivo de establecer un organismo constitucional autónomo responsable de salvaguardar los derechos fundamentales de acceso a la información y a la protección de los datos personales, el 7 de febrero de 2014 se publicó el Decreto por el que se Reforman y Adicionan diversas Disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en Materia de Transparencia (DOF, 2014). Este decreto dio origen al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y sentó las bases constitucionales para la emisión de la legislación en la materia.

De este modo, la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPESO) fue publicada el 26 de enero de 2017 (DOF), con el siguiente objetivo:

[...] establecer las bases, principios y procedimientos para garantizar el derecho de toda persona a la protección de sus datos personales en posesión de sujetos obligados”. [Estos incluyen a] cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, en los ámbitos federal, estatal y municipal. (LGPDPESO, 2017, art. 1o.)

Asimismo, los diversos Lineamientos Generales de Protección de Datos Personales para el Sector Público se publicaron en el DOF el 26 de enero de 2018, con el propósito de desarrollar las disposiciones de la ley general en la materia, exclusivamente en el ámbito federal.

Es necesario precisar que el marco normativo mexicano en materia de protección de datos personales se clasifica en dos grandes sectores: el público y el privado, atendiendo la naturaleza jurídica de la persona que tiene el poder de decisión sobre los datos personales, es decir, la persona responsable del tratamiento. Esto se debe a que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales tiene competencia exclusiva para conocer de los asuntos concernientes a las personas físicas y jurídicas de carácter privado, incluyendo a los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en los ámbitos federal, estatal y municipal. En el sector público, existe una competencia diferenciada entre el organismo garante federal y los 32 organismos garantes de las entidades federativas, los cuales tienen a su cargo las cuestiones vinculadas a los sujetos obligados de carácter estatal y municipal en su respectivo ámbito territorial.

De conformidad con las leyes en la materia, el marco normativo es aplicable a cualquier tratamiento de datos personales, ya sea en soportes físicos o electrónicos, sin importar cómo hayan sido creados ni el tipo de soporte, almacenamiento u organización. Esto se debe a que la información concerniente a una persona física identificada o identificable puede expresarse en forma numérica, alfabética, gráfica, alfanumérica, fotográfica, acústica o cualquier otro formato.

En este contexto, el derecho fundamental a la protección de los datos personales se basa en el cumplimiento de obligaciones derivadas de los principios –licitud, información, consentimiento, finalidad, calidad, proporcionalidad, lealtad y responsabilidad– y deberes –confidencialidad y seguridad– que rigen el tratamiento, así como en la posibilidad de ejercer ante los responsables los derechos de acceso, rectificación, cancelación, oposición y, en el sector público, también el derecho a la portabilidad. Al respecto, a continuación, se expondrá brevemente en qué consisten cada uno de ellos para pronta referencia:

- *Principio de licitud:* Los responsables están obligados a que el tratamiento se realice conforme a la legislación mexicana y el derecho internacional. En el sector público, esto también implica que el tratamiento debe restringirse a las facultades que la normatividad aplicable le confiere al responsable.
- *Principio de información:* Obliga a los responsables a comunicar a las personas titulares los datos que se recaban de ellas y con qué fines, así como proporcionar la información sobre la existencia y características principales del tratamiento a través del aviso de privacidad. Este aviso es un documento físico, electrónico o en cualquier otro formato, generado por el responsable y puesto a disposición de las personas titulares desde el momento en que se recaban los datos personales o de forma previa al tratamiento.
- *Principio de consentimiento:* Los responsables deben obtener una manifestación de voluntad de las personas titulares para llevar a cabo el tratamiento. Ésta debe ser libre (sin error, mala fe, violencia o dolo), específica (referida a finalidades concretas y determinadas que justifican el tratamiento) e informada (cuando las personas titulares conocen el aviso de privacidad previo al tratamiento al que serán sometidos los datos personales).
- *Principio de finalidad:* El tratamiento de los datos personales debe limitarse al cumplimiento de los fines establecidos en el aviso de privacidad, los cuales deben especificar de manera clara y, sin lugar a confusión, para qué serán tratados los datos personales. En el sector público, las finalidades deben estar relacionadas con las atribuciones que la normatividad otorga a los sujetos obligados.
- *Principio de calidad:* Los responsables deben adoptar las medidas necesarias para que los datos personales sean exactos, completos, correctos y actualizados en relación con los fines para los cuales fueron recabados. Así, cuando los datos

personales dejen de ser necesarios para el cumplimiento de las finalidades señaladas en el aviso de privacidad y las disposiciones legales aplicables, deberán ser cancelados, previo periodo de bloqueo.

- *Principio de proporcionalidad:* Los responsables están obligados a tratar únicamente los datos personales que sean estrictamente necesarios, relevantes y adecuados en relación con las finalidades para las que se hayan obtenido. Para ello, se deben realizar esfuerzos razonables para que los datos personales sean los mínimos necesarios, atendiendo a la finalidad del tratamiento que se llevará a cabo.
- *Principio de lealtad:* La obtención y tratamiento de datos personales no deberá realizarse a través de medios engañosos o fraudulentos. Los responsables están obligados a privilegiar la protección de los intereses de las personas titulares y la expectativa razonable de privacidad, la cual consiste en la confianza que deposita cualquier persona en otra respecto de que los datos personales entregados serán tratados en los términos acordados por las partes involucradas.
- *Principio de responsabilidad:* Los responsables deben velar y responder por el tratamiento de los datos personales bajo su custodia o posesión, o por aquellos que hayan comunicado a sus encargados. Pueden emplear estándares, mejores prácticas internacionales, esquemas de autorregulación o cualquier otro mecanismo. En el sector público, los sujetos obligados deben implementar mecanismos para acreditar el cumplimiento de los principios, deberes y obligaciones previstas en la ley de la materia y rendir cuentas sobre el tratamiento de los datos personales en su posesión.
- *Deber de confidencialidad:* Los responsables deben establecer controles para garantizar que toda persona que intervenga en cualquier fase del tratamiento guarde confidencialidad respecto de los datos personales a los que tenga acceso con motivo de sus actividades, incluso después de concluir su relación con el responsable o la persona titular. Esto para evitar la difusión indiscriminada de los datos personales sometidos a tratamiento.
- *Deber de seguridad:* Los responsables deberán establecer y mantener medidas de seguridad administrativas, físicas y técnicas que permitan proteger los datos personales contra daño, pérdida, alteración, destrucción o su uso, acceso o tratamiento no autorizado, sin importar el tipo de sistema en el que se encuentran o la clase de tratamiento que se lleve a cabo.

La verdadera aplicación práctica del derecho fundamental a la protección de datos personales se efectúa a través de los denominados derechos ARCOP –acceso, rectificación, cancelación, oposición y portabilidad–, los cuales permiten a las personas titulares materializar el ejercicio de su autodeterminación informativa, mediante el acceso, rectificación, cancelación, oposición y, en algunos casos, portabilidad de sus datos personales.

- *Acceso:* Las personas titulares podrán acceder a sus datos personales en poder del responsable y conocer las condiciones y generalidades de su tratamiento. Para ello, se debe poner a disposición de las personas titulares los datos personales requeridos, previa acreditación de su identidad, en el lugar donde se encuentren, o bien, entregarlos mediante copias simples, certificadas, medios magnéticos, ópticos o cualquier otra tecnología.
- *Rectificación:* Las personas titulares pueden solicitar la rectificación de sus datos personales en cualquier momento cuando no estén actualizados, sean incompletos o inexactos. Para ello, la persona solicitante debe precisar los datos personales a corregir y la modificación necesaria, acompañando los documentos que sustentan la procedencia de la rectificación.
- *Cancelación:* La cancelación de los datos personales brinda a las personas titulares la posibilidad de solicitar la eliminación de dichos datos de los archivos, registros, expedientes y sistemas del responsable. Esto no implica que la cancelación sea inmediata, sino que el responsable debe cesar el tratamiento de los datos personales, a partir de un periodo de bloqueo previo a su supresión.
- *Oposición:* Las personas titulares pueden manifestar su oposición al tratamiento de sus datos personales cuando exista una causa legítima y su situación así lo requiera, para evitar que se genere una afectación, o cuando se necesite expresar que no se efectúe el tratamiento respecto de finalidades concretas.
- *Portabilidad:* De acuerdo con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados, cuando el tratamiento de datos personales se realice de manera electrónica en un formato estructurado y comúnmente utilizado, las personas titulares podrán requerir al responsable una copia de los mismos en un formato que les permita seguir utilizándolos. Además, las personas titulares pueden solicitar la transmisión de sus datos personales y cualquier otra información almacenada en un sistema de tratamiento automatizado a otro, en un formato electrónico comúnmente utilizado, sin impedimentos por parte del responsable, siempre y cuando el tratamiento se base en el consentimiento o en un contrato.

Es importante resaltar que, si bien la legislación mexicana no contiene disposiciones expresas y específicas para regular el tratamiento de datos personales mediante sistemas basados en inteligencia artificial, las obligaciones derivadas de los principios y deberes antes mencionados, así como el ejercicio de derechos ARCOP, pueden ser igualmente aplicables en la medida en que el tratamiento realizado por dicha tecnología involucre la recopilación, utilización, análisis o almacenamiento de información de carácter personal.

Sobre este particular, es importante destacar que el RLFPDPP dispone que los responsables deberán informar a las personas titulares cuando se lleve a cabo el tratamiento de datos personales como parte de un proceso de toma de decisiones:

[...] sin que intervenga la valoración de una persona física. [De esta manera, las personas titulares pueden] ejercer su derecho de acceso para conocer los datos personales que se emplearon para la toma de decisión [respectiva, así como] el derecho de rectificación cuando consideren que alguno de los datos utilizados es inexacto o incompleto, [con el fin de] solicitar la reconsideración de [dicha] decisión. (RLFPDPP, 2011, art. 112)

Por su parte, la LGPDPPSO brinda a las personas titulares la posibilidad de solicitar la oposición al tratamiento o exigir su cese cuando:

[Los] datos personales sean objeto de un tratamiento automatizado [que genere] efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades. [Esto incluye] evaluaciones sin intervención humana de determinados aspectos personales del mismo, así como el análisis o predicción de su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento. (LGPDPPSO, 2017, art. 47, fracc. II.)

III.3. CONCLUSIONES

Con base en lo analizado en este capítulo, se puede afirmar, con cierto grado de certeza, que la inteligencia artificial y sus múltiples aplicaciones en la vida cotidiana de las personas, así como en empresas e instancias gubernamentales, ha traído consigo beneficios y avances tecnológicos que tienden a simplificar actividades. Sin embargo, también presentan serios desafíos para la protección de los derechos humanos y, en particular, para la protección de los datos personales. A medida que las capacidades de los sistemas tecnológicos para recopilar, analizar y procesar una mayor cantidad de información personal aumentan, también se incrementan las posibilidades de ocasionar afectaciones a las personas titulares en su esfera jurídica de derechos.

Es esencial generar conciencia, tanto en los desarrolladores como en quienes contraten o adquieran *software*, productos y servicios basados en sistemas de IA, para que se utilicen estas tecnologías en estricto apego a los principios, deberes y obligaciones previstos por la normatividad aplicable en materia de protección de datos personales, siempre que se requiera de este tipo de información para su funcionamiento. Esto es imperativo para garantizar el efectivo ejercicio de los derechos fundamentales tutelados por el orden jurídico nacional e internacional.

Al respecto, no debe perderse de vista que los avances tecnológicos están, de manera inevitable, mucho más avanzados que el orden jurídico vigente, lo cual ocasiona un desfase de la legislación respecto de las conductas que pretende regular. Por tal motivo, considerando la protección de los intereses de las personas titulares, así como la necesidad de tratar datos personales para diferentes actividades lícitas y legítimas, la Red Iberoamericana de Protección de Datos estimó pertinente emitir algunas reglas para el tratamiento de datos personales. Estas reglas buscan evitar cualquier arbitrariedad que pueda vulnerar los derechos de las personas titulares y no pretenden, de modo alguno, oponerse a la realización de dicho tratamiento.

De esta manera se emitieron las Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial (2019b), con el propósito de presentar sugerencias preventivas a quienes desarrollan productos con IA, orientándolos para que desde su diseño se consideren las exigencias normativas sobre el tratamiento de datos personales. Estas recomendaciones incluyen los siguientes conceptos:

- Cumplir las normas locales sobre el tratamiento de datos personales.
- Efectuar estudios de impacto de privacidad.
- Incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto.
- Materializar el principio de responsabilidad demostrada.
- Diseñar esquemas apropiados de gobernanza sobre tratamiento de datos personales en las organizaciones que desarrollan productos de inteligencia artificial.
- Adoptar medidas para garantizar los principios sobre tratamiento de datos personales en los proyectos de inteligencia artificial.
- Respetar los derechos de las personas titulares de los datos e implementar mecanismos efectivos para el ejercicio de estos.
- Asegurar la calidad de los datos.
- Utilizar herramientas de anonimato.
- Incrementar la confianza y la transparencia con los titulares de los datos personales. (RIPD, 2019b, pp. 15-24)

De forma paralela, en 2019, la RIPD también emitió las Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial (2019a), que consisten en directrices complementarias y más detalladas de las recomendaciones antes citadas, abordando cada uno de los principios contemplados en los Estándares de Protección de Datos Personales para los Estados Iberoamericanos aprobados en 2017 –legitimación, licitud, lealtad, transparencia, finalidad, proporcionalidad, calidad, responsabilidad, seguridad y confidencialidad– (RIPD, 2017, p. 17).

Finalmente, no se omite destacar que, en ámbito nacional y en ejercicio de sus funciones preventivas para la protección del derecho fundamental a la protección de los datos personales, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales ha emitido las Recomendaciones para el Tratamiento de Datos Personales Derivado del Uso de la Inteligencia Artificial (2022). Estas recomendaciones buscan:

[...] difundir el conocimiento sobre la relación de la IA con la protección de los datos personales, promoviendo [así] el uso ético y adecuado de la información [de carácter] personal [mediante] las diferentes tecnologías [que se valen de] la IA para su funcionamiento [...] [Asimismo, promueven] el cumplimiento [...] del deber de seguridad [por parte de los] responsables de los sectores público y privado que desarrollan productos o servicios [con este tipo de sistemas]. (INAI, 2022, p. 9)

REFERENCIAS

- Acuerdo mediante el cual se Aprueban los Lineamientos Generales de Protección de Datos Personales para el Sector Público. (26 enero de 2018). *Diario Oficial de la Federación (DOF)*. https://dof.gob.mx/nota_detalle.php?codigo=5511540&fecha=26/01/2018#gsc.tab=0
- Acuerdo mediante el cual se Aprueba la Adición de un Título Décimo Primero a los Lineamientos Generales de Protección de Datos Personales para el Sector Público y la Modificación y Adición de una Fracción XXV al Artículo 25 y una Fracción XIII al Artículo 42 del Estatuto Orgánico del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales. (25 de febrero de 2022). *Diario Oficial de la Federación (DOF)*. https://dof.gob.mx/nota_detalle.php?codigo=5643872&fecha=25/02/2022#gsc.tab=0
- Constitución Política de los Estados Unidos Mexicanos (CPEUM). (última reforma: 15 de octubre de 2025). <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>.
- Decreto por el que se Adiciona un Segundo Párrafo, Recorriéndose los Subsecuentes en su Orden, al Artículo 16 de la Constitución Política de los Estados Unidos Mexicanos. (1 de junio de 2009). *Diario Oficial de la Federación (DOF)*. https://dof.gob.mx/nota_detalle.php?codigo=5092143&fecha=01/06/2009#gsc.tab=0
- Decreto por el que se Reforman y Adicionan diversas Disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en Materia de Transparencia. (7 de febrero de 2014). *Diario Oficial de la Federación (DOF)*. https://www.diputados.gob.mx/LeyesBiblio/ref/dof/CPEUM_ref_215_07feb14.pdf

- Holdsworth, J. y Scapicchio, M. (s.f.). *¿Qué es el deep learning?* En IBM, Think. <https://www.ibm.com/mx-es/topics/deep-learning>
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2022). *Recomendaciones para el Tratamiento de Datos Personales Derivado del Uso de la Inteligencia Artificial*. INAI. <https://home.inai.org.mx/wp-content/documentos/DocumentosSectorPublico/RecomendacionesPDP-IA.pdf>.
- Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) (abrogada) (publicada: 5 de julio de 2010). https://www.diputados.gob.mx/LeyesBiblio/abro/lfpdppp_2010/LFPDPPP_2010_abro.pdf
- Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) (abrogada) (publicada: 26 de enero de 2017). https://www.diputados.gob.mx/LeyesBiblio/abro/lgpdppso_2017/LGPDPPSO_2017_abro.pdf
- López Takeyas, B. (16 de enero de 2007). “Introducción a la inteligencia artificial”. En Instituto Tecnológico de Nuevo Laredo. <https://nlaredo.tecnm.mx/takeyas/Articulos/Inteligencia%20Artificial/ARTICULO%20Introduccion%20a%20la%20Inteligencia%20Artificial.pdf>
- Red Iberoamericana de Protección de Datos (RIPD). (2017). *Estándares de Protección de Datos Personales para los Estados Iberoamericanos*. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
- RIPD. (2019a). *Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial*. <https://www.redipd.org/sites/default/files/2020-02/guia-orientaciones-espec%C3%ADficaproteccion-datos-ia.pdf>
- RIPD. (2019b). *Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial*. <https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf>
- Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (RLFPDPPP). (21 de diciembre de 2011). *Diario Oficial de la Federación (DOF)*. https://www.diputados.gob.mx/LeyesBiblio/regley/Reg_LFPDPPP.pdf
- Universidad Católica San Pablo (UCSP). (s.f.). *Machine learning vs. inteligencia artificial: principales diferencias*. <https://postgrado.ucsp.edu.pe/articulos/machine-learning-inteligencia-artificial-diferencias/>

CAPÍTULO IV

Inteligencia artificial y neuroderechos

Gisela María Pérez Fuentes¹

SUMARIO: IV.1. Introducción; IV.2. Sistema de inteligencia artificial; IV.2.1. Características del sistema de inteligencia artificial; IV.2.2. Progresividad de la inteligencia artificial (*machine learning* y *deep learning*); IV.3. De los derechos digitales a los neuroderechos; IV.3.1. Significado de los neuroderechos; IV.3.2. Protección internacional sobre la ética de la IA; IV.4. Conclusiones.

PALABRAS CLAVE: Inteligencia artificial, *machine learning*, *deep learning*, derechos digitales, neuroderechos, neurotecnología, bioética.

IV.1. INTRODUCCIÓN

El término inteligencia artificial (IA) fue acuñado por Alan Turing en la década de 1950, mediante el desarrollo del Test de Turing, según el cual, si se desarrollaba un programa informático para conversar con humanos y estos creían estar conversando con otros humanos, se afirmaba que tal programa había superado el test de inteligencia. (Casadesús Ripoll, 2022, p. 3)

La primacía de prestación de servicios que implica la robótica y la inteligencia artificial ha puesto en peligro una serie de derechos fundamentales vinculados directamente con la persona humana, cuestionando la identidad, intimidad y calidad cognoscitiva de algunos sujetos sobre otros con menos recursos.

La inteligencia artificial significa el aprendizaje a través de algoritmos que se denominan neutrales, pero son ¿realmente parciales? Al reproducir los procesos cognitivos humanos, en los datos personales que acumulan, aparecen: fuente de quien los almacena, manipulación, la existencia de responsabilidad y ética en el tratamiento de estos datos que significa el respeto a los derechos humanos. Por ello, la hipótesis de esta pequeña aportación reflexiva está basada en que los adelantos tecnológicos deben respetar los derechos fundamentales, por lo que la prestación de la IA no puede poner

¹ Profesora-Investigadora de tiempo completo en la Universidad Juárez Autónoma de Tabasco. Es líder del Cuerpo Académico “Estudios de Derecho Civil”. Perteneció al Sistema Nacional de Investigadoras e Investigadores, Nivel III, del Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAH-CYT). Es miembro regular de la Academia Mexicana de Ciencias desde el año 2014.

en peligro a la persona humana a partir del ejercicio invasivo que puede provocar la tecnología. En el desarrollo de este capítulo explicamos algunos casos que, sin embargo, han traspasado estos límites, así como la advertencia de científicos y juristas ante esta realidad.

IV.2. SISTEMA DE INTELIGENCIA ARTIFICIAL

La IA significa el aprendizaje a través de algoritmos específicos, mediante los cuales se reproducen actividades cognitivas humanas, en los que se desarrollan percepción, creatividad, comprensión de lenguaje, los cuales en algunas circunstancias conllevan sesgos de quien los elabora.

La IA es la capacidad de las máquinas para usar algoritmos, aprender de los datos y utilizar lo aprendido en la toma de decisiones, pudiendo analizar grandes volúmenes de información en el mismo momento (Rouhiainen, 2018, pp. 10-12). Las tecnologías de la IA son la base de muchas herramientas para internet, en una primera etapa, por ejemplo, motores de búsqueda o sistemas para la construcción de portales web.

Se reconoce que muchos de los cambios de decisiones en nuestras vidas están regidos por algoritmos de la IA, tales como la publicidad, mercadotecnia, sanidad, seguros, el sistema judicial, y qué decir del sistema bancario.

En el Reglamento del Parlamento Europeo por el que se establece la Ley de Inteligencia Artificial (aprobado por dicho Parlamento y el Consejo de la Unión Europea, el 13 de junio de 2024), se define al sistema de IA como el *software* que se desarrolla empleando una o varias de las técnicas y estrategias de aprendizaje automático (lógica y conocimiento).

En la IA aparece la robótica como ciencia que estudia el diseño y construcción de máquinas capaces de desempeñar tareas del ser humano mediante procesos mecánicos y programados, consistentes en el diseño de sistemas, manipulación, sistemas de controles, sensores y fuentes de energía, por lo que la IA no puede existir sin interdisciplinariedad, desde un matemático e ingeniero hasta el jurista, atravesando por la medicina, la biología y el arte, por lo que es imprescindible la existencia de responsabilidad y ética en estos procesos de adelantos tecnológicos que permitirán evitar la violación de los derechos fundamentales.

IV.2.1. CARACTERÍSTICAS DEL SISTEMA DE INTELIGENCIA ARTIFICIAL

La autonomía y la imprevisibilidad de los sistemas son consideradas como características propias de la IA y las capacidades más disruptivas para el actual marco legislativo, que no está preparado para cubrir los daños causados por el avance tecnológico.

En el ámbito de la IA se utilizan algoritmos para recibir y analizar datos de entrada para predecir los valores de salida, a medida que se introducen nuevos datos estos algoritmos aprenden y optimizan sus operaciones desarrollando así la IA [...]. (Gómez Rodríguez, 2022, p. 98)

IV.2.2. PROGRESIVIDAD DE LA INTELIGENCIA ARTIFICIAL

(*MACHINE LEARNING Y DEEP LEARNING*)

En la medida que a un tipo de máquina se le puede dotar de capacidades de adaptación y aprendizaje, entraña cierto grado de imprevisibilidad en su comportamiento. Existe entonces una autonomía, que significa una cadena causal que va desde la captación de datos mediante sus sensores, tomando una decisión que no requiere la intervención de un agente externo ni en particular la de un agente humano, pero en la autonomía filosófica esto significa establecer sus propias normas, lo cual no puede darse.

Así, se considera que existen la inteligencia artificial débil (*narrow*) y la inteligencia artificial fuerte (*general IA*). En la actualidad, la denominada IA débil ha alcanzado un elevado grado de desarrollo y efectividad de tratamiento de datos, hasta llegar a *big data* y el desarrollo del aprendizaje automático que se conoce como *machine learning*, por ejemplo, desde los programas de procesamiento de imágenes y reconocimiento facial, hasta programas de procesamiento de datos con finalidades específicas (detección de posibles fraudes en transacciones económicas o publicidad).

Se reconoce como *machine learning* a la habilidad para aprender sin que haya sido explícitamente programada con anterioridad, pero para que un algoritmo aprenda de la experiencia y evolución tiene que contar con patrones que puedan almacenar una determinada cantidad de datos.

La IA se centra en el uso de datos y algoritmos para imitar la forma en que los humanos aprenden, mejorando gradualmente su precisión. Esta recopilación de información se ha denominado *minería de datos* (*data mining*), consistente en el proceso de analizar los datos recopilados identificando patrones para así extraer información. (Casadesús Ripoll, 2022, p. 8)

Los datos personales en gran escala son el nuevo petróleo de la economía, como el insumo para el desarrollo de la tecnología y sus aplicaciones: analítica de datos, inteligencia artificial, el internet de las cosas o la tecnología de cadena de bloques.

En cambio, el *deep learning* es el aprendizaje profundo como forma de *machine learning*, utilizada en estructuras de redes neuronales (datos neuronales) basada a grandes rasgos en el cerebro humano, que aprende mediante el ensayo y las respuestas.

Se basa en la creación artificial de redes neuronales y en la imitación de la capacidad de autoaprendizaje del cerebro humano. El *deep learning*, también denominado *aprendizaje profundo*, ha obtenido resultados relevantes en la comprensión del lenguaje natural y en el análisis de las emociones. Los últimos avances en IA están basados en el aprendizaje profundo, un método de aprendizaje automático que emplea redes neuronales artificiales. (Gómez Rodríguez, 2022, p. 107) [énfasis añadido]

IV.3. DE LOS DERECHOS DIGITALES A LOS NEURODERECHOS

Se advierte el interés y la voluntad de diferentes organismos por definir los derechos digitales, es el caso en el derecho comparado de la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital, publicada en el *Diario Oficial de la Unión Europea* el 23 de enero de 2023, misma que fue proclamada conjuntamente por el Parlamento Europeo, el Consejo y la Comisión, luego de haber sido propuesta por la Comisión a las otras instituciones el 26 de enero de 2022.

En la Carta de los Derechos Digitales (2021) del Gobierno de España, los derechos ante la inteligencia artificial no sólo deben perseguir el bien común y el principio desarrollado en la bioética de no maleficencia, sino que además se establecerán condiciones de transparencia y gobernanza para que exista comprensibilidad en los avances de la IA cuando aparecen los tratamientos propios que mejoran la vida humana. Por su parte, en México, se expidió la Carta de Derechos de la Persona en el Entorno Digital, mediante un Código de Buenas Prácticas. (INAI, 2021)

La IA es interdisciplinaria, en ella se desarrollan la ciencia y la ingeniería, y se exploran y desarrollan métodos que permiten interconectar el sistema nervioso con dispositivos técnicos. Se entiende por *neurotecnología* cualquier tecnología que registre información procedente de la actividad cerebral o interfiera con ella y, por ello, la importancia de la ética y también del derecho.

En el 2013, se aprobó en Estados Unidos de América, por iniciativa del Dr. Rafael Yuste, el proyecto conocido como BRAIN (investigación del cerebro a través del avance de neurotecnologías innovadoras). Este proyecto tenía como base fundamental

un sistema en el que se establecía la comunicación directa entre el cerebro y una máquina, y en el cual la actividad eléctrica que se produce cuando las neuronas se activan para comunicarse entre sí se procesa y decodifica en comandos que se envían a un dispositivo para llevar a cabo una acción deseada. Este sistema se conoce como interfaz cerebro-computadora. (Yuste *et al.*, 2021, pp. 157-161)

Estas tecnologías, al combinarse con la IA, podrían usarse para descifrar y manipular procesos mentales y aumentar cognitivamente a las personas, conectándolas a interfaces cerebro-computadora.

[Los avances] tecnológicos significan que estamos en el camino hacia un mundo en el que será posible decodificar los procesos mentales de las personas y manipular directamente los mecanismos cerebrales subyacentes a sus intenciones, emociones y decisiones; donde los individuos pudieran comunicarse con otros simplemente pensando; y donde poderosos sistemas computacionales vinculados directamente al cerebro de las personas ayudan en sus interacciones con el mundo, de manera que sus capacidades físicas y mentales mejoran enormemente.

[Estos] avances podrían revolucionar el tratamiento de muchas enfermedades, desde lesiones cerebrales y parálisis hasta epilepsia y esquizofrenia, y transformar la experiencia humana para mejor. Pero la tecnología también podría exacerbar las desigualdades sociales y ofrecer a las corporaciones, los piratas informáticos, los gobiernos o cualquier otra persona, nuevas formas de explotar y manipular a las personas. [En esta realidad] hasta se podrían alterar profundamente algunas características humanas [...]. (Yuste *et al.*, 2017)

Características como la privacidad mental (abogados, profesores o alumnos, cuando estudian derecho de obligaciones se les enseña que el consentimiento es la manifestación de voluntad, pero la reserva mental no provoca efectos jurídicos, sin embargo, a partir de estos avances tecnológicos sí se provocarían nuevos efectos).

El proyecto de investigación, no obstante, causó una preocupación en diversos investigadores, como el propio Yuste y un grupo de aproximadamente 25 personas vinculadas a la neurociencia, inteligencia artificial y bioética, de varios países y con gran desarrollo, tanto en Europa, China, Japón, Australia, Canadá e Israel, que buscaban visibilizar en la Declaración de Derechos Humanos, la protección de los derechos neuronales.²

² “El Grupo Morningside está formado por neurocientíficos, neurotecnólogos, [médicos, especialistas en ética] e ingenieros de inteligencia artificial. Incluye representantes de Google y Kernel (una nueva empresa de neurotecnología en Los Ángeles, California); de proyectos cerebrales internacionales; y de instituciones académicas y de investigación en Estados Unidos, Canadá, Europa, Israel, China, Japón y Australia. [Se reunieron] en un taller patrocinado por la Fundación Nacional de Ciencias de EEUU en la Universidad de Columbia, Nueva York, en mayo de 2017 para discutir la ética de las neurotecnologías y la inteligencia [artificial]” (Yuste *et al.*, 2017).

¿Qué significan entonces los neuroderechos y cómo lograr su protección? El grupo encabezado por el Dr. Rafael Yuste, plantea que la información de los cerebros debe ser protegida, evitando que el desarrollo científico entre en la explotación con fines de lucro. (Salazar Solís *et al.*, 2020, pp. 123-125)

El Dr. Yuste hace dos planteamientos: primero, que sean los médicos los que determinen el principio de beneficencia, propio de la bioética, y esto es un poco complejo, porque en el mejor de los casos puede existir una inclinación a la etapa paternalista de la medicina, ya superada por el necesario consentimiento informado de los pacientes o cualquier persona que se somete a un experimento; segundo, precisamente la protección de los neuroderechos enunciados por científicos, no por abogados. Expliquemos esta realidad científica: no estamos refiriéndonos a la investigación neurológica y sus efectos, no exactamente al actuar por sí solos de los robots.

Así que la neurotecnología se considera como cualquier tecnología que registre información de la actividad cerebral. Si se combina con la inteligencia artificial, tiene el potencial de alterar la sociedad, por lo que en el trabajo de investigación BRAIN se propone el desarrollo de un código deontológico que proteja de manera internacional los denominados cinco neuroderechos, los cuales responden más a las ideas de los científicos en general, que a las propias de los abogados y juristas. (Salazar Solís *et al.*, 2020, pp.126-127)

IV.3.1. SIGNIFICADO DE LOS NEURODERECHOS

Rafael Yuste y Sara Goering, integrantes del experimento, sostienen que “la IA y las interfaces cerebro-computadora deben respetar la privacidad, la agencia e identidad y la igualdad de las personas”. (Yuste *et al.*, 2017)

Los *neuroderechos* se pueden definir como el intento para crear un nuevo marco jurídico internacional de derechos humanos, destinados específicamente a proteger el cerebro y su actividad a medida que se produzcan avances en neurotecnología y, en este contexto, se han identificado y definido cuatro neuroderechos:

1. *Derecho a la privacidad mental*: Implica una protección de datos cerebrales, involucra la seguridad frente a terceros, de contenidos conscientes o subconscientes. La privacidad tal y como la conocemos (el derecho a estar solo) desaparece, porque alguien a través de estos experimentos puede llegar hasta esa parte íntima de las ideas y sentimientos. En la protección de este derecho, los científicos no deben llegar a conocer por estímulos tu subconsciente sin previa autorización, pues de saberlo pueden programar acciones condicionadas y no propias.

2. *Derecho a la identidad*: Deben desarrollarse límites para prohibir que la tecnología interrumpa el sentido de uno mismo; cuando la neurotecnología conecta a las personas con las redes digitales podría alterar el sentido del *yo*, de quién es, sin su expreso consentimiento, lo que se ha denominado *hackeo* o manipulación cerebral.
3. *Derecho al acceso equitativo a la aumentación cognitiva*: La finalidad de este reconocimiento es establecer directrices a nivel internacional y nacional, que se encarguen de regular el desarrollo y las aplicaciones de las neurotecnologías.
4. *Derecho a la protección de sesgo en los procesos automatizados de toma de decisiones*:

El concepto de *sesgo cognitivo* fue introducido por los psicólogos israelíes Kahneman y Tversky en 1972. Consiste en una interpretación errónea sistemática de la información disponible, que ejerce influencia en la manera de procesar los pensamientos, emitir juicios y tomar decisiones. (Braininvestigations, 2020) [énfasis añadido]

Convirtiéndose en un error sistemático en el pensamiento que ocurre cuando las personas procesan información.

IV.3.2. PROTECCIÓN INTERNACIONAL SOBRE LA ÉTICA DE LA IA

El 25 de noviembre de 2021, la UNESCO emitió el Primer Acuerdo Mundial sobre la Ética de la Inteligencia Artificial, en los siguientes términos:

Este marco ético define valores y principios comunes que guiarán y garantizarán un desarrollo saludable de esta tecnología, en la que todos los individuos pueden acceder a sus registros de datos personales o incluso borrarlos y prohíbe explícitamente el uso de sistemas de IA para la calificación social y la vigilancia masiva. (ONU, 2021)

El Acuerdo pone de manifiesto lo siguiente:

- Marco ético.
- Valores y principios de los países en el uso, desarrollo e implementación de la IA.
- Un desarrollo saludable de la IA. (UNESCO, 2022)

IV.4. CONCLUSIONES

El reconocimiento constitucional con alcance general de los neuroderechos puede servir como un medio para conceptualizar las violaciones de los derechos humanos que podrían causar el uso o el abuso de la neurotecnología, para proteger la autonomía individual y la privacidad mental.

Se debe establecer una distinción entre datos personales y datos neuronales. El dato personal es el que se ha registrado, a través de medios telemáticos, de una persona, la cual la hace identificada o de posible identificación (identificable).

El dato neuronal, en cambio, se identifica por un dato cerebral o neurodato, como una información obtenida de la actividad de las neuronas que contienen una representación de la actividad cerebral. Se refiere a la información obtenida, directa o indirectamente, a través de los patrones de actividades de las neuronas, cuyo acceso está dado por neurotecnología avanzada, incluyendo sistemas de registros cerebrales, tanto invasivos como no invasivos. Estos datos contienen una representación de la actividad psíquica, de forma consciente como subconsciente, y que corresponden al más íntimo aspecto de la privacidad mental.

Los algoritmos que se utilizan para orientar la publicidad, calcular las primas de seguros o encontrar socios potenciales, serán considerablemente más poderosos si se basan en información neuronal; por ejemplo, patrones de actividad de las neuronas asociadas con ciertos estados de atención. Y los dispositivos neuronales conectados a internet abren la posibilidad de que individuos u organizaciones (*hackers*, corporaciones o agencias gubernamentales) rastreen o incluso manipulen la experiencia mental de las personas.

En resumen, la privacidad mental protege a los individuos del uso de los datos obtenidos durante la medición de su actividad cerebral sin su consentimiento y prohíbe expresamente cualquier transacción comercial.

Es importante que en México se apliquen los principios aprobados en 2021 por la UNESCO, de forma que sean supervisados por leyes generales y especializadas. En un primer momento han sido tomados en consideración por el INAI a través de la Carta de Derechos de la Persona en el Entorno Digital (INAI, 2021), en la cual destacan:

- El uso de sistemas de IA no debe ir más allá de lo necesario para alcanzar un objetivo legítimo.
- Los daños no deseados; riesgos de seguridad y vulnerabilidades a los ataques deberían ser evitados.
- La privacidad debe protegerse y promoverse a lo largo de todo el ciclo de vida de la IA.
- El despliegue ético de los sistemas de IA depende de su transparencia y otros principios, como la privacidad, la seguridad y la protección.

REFERENCIAS

- Casadesús Ripoll, P. (2022). *La responsabilidad civil por el uso discriminatorio de los datos personales a través de la inteligencia artificial*. Editorial Comares.
- Carta de Derechos Digitales. (14 de julio de 2021). https://www.eapn.es/ARCHIVO/documentos/documentos/1701273506_carta_derechos_digitales_redes_2021.pdf
- Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital. (23 de enero de 2023). *Diario Oficial de la Unión Europea (DOUE)*. [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123\(01\)&qid=1684248405089](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123(01)&qid=1684248405089)
- Gómez Rodríguez, J. M. (enero-junio de 2022). Inteligencia artificial y neuroderechos. Retos y perspectivas. *Cuestiones Constitucionales. Revista Mexicana de Derecho Constitucional*, 1(46). <https://revistas.juridicas.unam.mx/index.php/cuestiones-constitucionales/article/view/17049/17593>
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2021). *Carta de Derechos de la Persona en el Entorno Digital. Código de Buenas Prácticas*. INAI. https://www.idaip.org.mx/archivos/transparencia/ruoch/BIBLIOTECA%20DIGITAL/Carta_DDigitales.pdf
- Kreimer, R. (5 de diciembre de 2021). *Las distorsiones cognitivas* [Video]. YouTube. <https://www.youtube.com/watch?v=oIoOtmxwmR8>
- Organización de las Naciones Unidas (ONU). (25 de noviembre de 2021). Primer Acuerdo Mundial sobre la Ética de la Inteligencia Artificial. <https://news.un.org/es/story/2021/11/1500522>
- Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO). (2022). *Recomendación sobre la Ética de la Inteligencia Artificial*. https://unesdoc.unesco.org/ark:/48223/pf0000381137_spa
- ¿Qué es el sesgo cognitivo y por qué es importante en los negocios? (24 de enero de 2020). En *Braininvestigations. The Mind Decoding Company*. <https://www.braininvestigations.com/neurociencia/sesgo-cognitivo-negocios/>
- Reglamento del Parlamento Europeo y del Consejo 2024/1689. (13 de junio de 2024). https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=OJ:L_202401689
- Rouhiainen, L. (2018). *Inteligencia artificial. 101 cosas que debes saber hoy sobre nuestro futuro*. Alienta Editorial.
- Salazar Solís, L. A., Zuluaga Ocampo, L., Martínez Mancilla, Y., y Madrigal Castro A. (2020). *Inteligencia artificial en Latinoamérica*. Fundación Konrad Adenauer.
- Yuste, R., Goering *et al.* (2017). Four ethical priorities for neurotechnologies and AI. *Nature*, 551(7679). <https://doi.org/10.1038/551159a>
- Yuste, R., Genser, J. y Herrmann, S. (2021). It's time for neuro-rights: New human rights for the age of neurotechnology. *Horizons. Journal of International Relations and Sustainable Development*, (18).

CAPÍTULO V

La información pública: componente de acceso y ejercicio de los derechos fundamentales

Ana Lía de Fátima García García¹

SUMARIO: V.1. Introducción; V.2. Subjetividad sobre el concepto de información y mecanismos de acceso a la información pública; V.3. La participación ciudadana y la disponibilidad de la información pública; V.4. Conclusión.

PALABRAS CLAVE: Acceso y ejercicio de los derechos fundamentales, componentes y mecanismos de acceso a la información pública, derechos fundamentales, información pública.

V.1. INTRODUCCIÓN

La información pública representa un componente esencial para la democracia, la legitimidad y la confianza de la ciudadanía sobre las acciones diarias de aquellos que ostentan el poder público; además, constituye el bastón para el acceso a otros derechos fundamentales, como la salud, la educación, la vivienda, la alimentación, la seguridad y la justicia.

Entre las virtudes del acceso a la información destaca como instrumento y herramienta del saber para la construcción del conocimiento, que permite a las personas tomar decisiones basadas en criterios, fundamentos e incluso desde una óptica científica y humanista, y con ello posibilita a éstas un desarrollo integral, humanista y con certeza jurídica.

El ejercicio de los derechos fundamentales, como el acceso a la información pública, implica de primera instancia la participación ciudadana que apoya, en el saber del quehacer público, la toma de decisiones informadas, fomento y acceso a otros derechos, transparencia y rendición de cuentas sobre el uso y aprovechamiento de cada uno de los recursos públicos que posee nuestra Nación, administrados por los entes públicos del Estado Mexicano.

¹ Maestra en Administración Pública y Administración de Empresas. Directora General de Fundación IMSS. Desde el IMJUVE e INDESOL, desarrolló políticas públicas en materia de juventud y salud. Como Secretaria Ejecutiva del INFO CDMX, coordinó la transición de las reformas a la Ley del Instituto.

Este capítulo explorará la importancia de la información pública como un componente esencial para el acceso y el ejercicio de los derechos fundamentales, examinando su rol en la democracia, los marcos legales que lo sustentan, y los desafíos que tienen las instituciones para construir una cultura de la información pública.

V.2. SUBJETIVIDAD SOBRE EL CONCEPTO DE INFORMACIÓN Y MECANISMOS DE ACCESO A LA INFORMACIÓN PÚBLICA

“La información es un conjunto de datos con significado que estructura el pensamiento de los seres vivos, especialmente, del ser humano [...]” (Solís-Macías, 2017, p. 2); por lo tanto, este conjunto de datos y significados son herencia de la cultura que sí se crea, sí se transforma y sí se transmite mediante la intersubjetividad.

Esta última idea representa uno más de los retos, puesto que cada persona puede tener expectativas diversas sobre la información que desea obtener, cuando le es concedida puede ampliar sus inquietudes como un indicador de conocimiento, si sucede esto se habrá logrado el primer objetivo del derecho fundamental que nos ocupa.

Sin embargo, la intersubjetividad de los significados implica un reto, puesto que se puede oponer los resultados contra la expectativa, que también pueden llevar a confusiones, malestares e inconformidades que deriven en malentendidos, sobreentendidos o incluso con la impresión denegada.

En el caso de la información pública, esta tiene otros alcances establecidos en diversos instrumentos normativos, como en el artículo 6o. de la Constitución Política de los Estados Unidos Mexicanos, la Ley General de Transparencia y Acceso a la Información Pública y la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

A nivel internacional, existen varios tratados y convenios que reconocen el derecho al acceso a la información pública como un componente fundamental de los derechos humanos. La Declaración Universal de Derechos Humanos (artículo 19) y el Pacto Internacional de Derechos Civiles y Políticos (artículo 19) establecen el derecho a la libertad de expresión, que incluye el derecho a buscar, recibir y difundir información.

De acuerdo con el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX, 2024), la información pública es todo aquel documento, es decir, soporte físico de cualquier tipo (escrito, impreso, sonoro, visual o electrónico), en el que se plasme cualquier información gubernamental en posesión de las autoridades públicas locales obligadas.

En este sentido, la información pública debe ser el conjunto de datos, caracteres, signos y significados que se derivan de la praxis pública, que contienen en su conjunto información del interés del pueblo; ésta debe estar dispuesta y completa, sin embargo, cuando por algo puede no estar, existen mecanismos conocidos como *solicitudes de acceso a la información pública*, que pueden ser demandadas a diversas fuentes.

La información pública debe tener la capacidad de transmitir valores que permitan agregar valor social para el bien común, a través de un lenguaje claro, preciso y eficaz; de ahí que las ambigüedades deben ser objeto de revisión, escrutinio y detección de áreas de oportunidad, con el fin de facilitar su entendimiento y comprensión en las poblaciones, mismas que poseen vulnerabilidades físicas, sociales, culturales y/o económicas, por ello, la posibilidad de brindar, adquirir y poseer la información pública es fundamental; ésta debe ser accesible, plural e inclusiva, en caso contrario, deberán realizarse los ajustes necesarios y razonables para lograrlo.

Para atender y poner a disposición de la información pública a las diferentes poblaciones, el INFO CDMX, a lo largo de sus 18 años de historia, ha creado –acertadamente y de manera paralela a la evolución de las tecnologías– los mecanismos que permitan a las poblaciones acceder y poseer información con valor público; cada una ha representado una oportunidad, pero también un reto para este fin. Entre los mecanismos que posee e implementa el INFO CDMX se encuentran los siguientes:

- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, y demás normativa vigente y aplicable: Éstas fundamentan, brindan orden jurídico y delimitan las atribuciones y funciones de la institución garante.
- Plataforma Nacional de Transparencia: Herramienta tecnológica a través de la cual se pueden elaborar solicitudes de información pública, proteger los datos personales y presentar recursos de revisión.
- INFOMEX: Herramienta tecnológica que permite el acceso a la información pública de las autoridades obligadas de la Ciudad de México.
- Biblioteca Digital: En este espacio se puede acceder a publicaciones en materia de acceso a la información pública, transparencia, rendición de cuentas y protección de datos personales.
- TEL-INFO: Servicio telefónico especializado para la orientación relativa a los derechos fundamentales de los que es garante el INFO CDMX, y vínculo que permite la realización de solicitudes de información y seguimientos.

V.3. LA PARTICIPACIÓN CIUDADANA Y LA DISPONIBILIDAD DE LA INFORMACIÓN PÚBLICA

Las actividades fundamentales para el acceso de la información pública implican por lo menos dos dimensiones: por un lado, aquellas acciones que se realicen desde la ciudadanía para acceder a datos que puedan ser útiles para resolver o mejorar su calidad de vida, entorno y/o desarrollo; y, por otro, aquellas acciones y mecanismos que pongan las instituciones públicas al servicio de la ciudadanía, lo que implica obligadamente una sinergia o relaciones entre dos esferas sociales, dependerá de la comunicación efectiva, clara y precisa para su entendimiento sobre los objetivos planteados y basados en la normativa, la cual debe considerarse como un elemento perfectible.

Durante los 18 años de existencia del INFO CDMX, son conocidas su evolución y estrategias que han hecho en materia de promoción y difusión: campañas publicitarias, ferias de la transparencia en lugares públicos estratégicos y activaciones educativas. Sin embargo, surge una inquietud, ¿por qué entonces muchas personas carecen de los conocimientos para acceder a su derecho fundamental de acceso a la información pública?

En este sentido, debe considerarse que la población va creciendo y el acceso a la información en general evoluciona vertiginosamente; claro ejemplo son las redes sociales, que podrían ser o representar la principal fuente de ésta, pero debe estar en claro que el acceso a uso de las tecnologías es desigual por condiciones como la edad, la disposición de los dispositivos o tecnologías de la información y la comunicación (TIC) y el costo de los servicios.

Podemos poner a consideración nuevas estrategias de promoción y difusión sobre los derechos fundamentales y sus diferentes posibilidades de acceso; el ejercicio será a voluntad y necesidad de cada persona, pero siempre dispuestas.

Por ello, deben pensarse desde la simplificación de los procedimientos, esto implica procesos sencillos y accesibles, para el entendimiento de por lo menos la mayoría de las poblaciones; continuidad y modernización de los contenidos y actividades educativas con mecanismos de evaluación, que permitan la detección de áreas de oportunidad, así como la supervisión y revisión anticipada de las respuestas a las solicitudes de información que son generadas por las instituciones públicas; no se trata de responder, sino de brindar el mayor interés para crear una cultura que brinde confianza, certidumbre y reconocimiento al quehacer público.

El fomento debe estar enfocado en reconocer las similitudes y diferencias de las poblaciones, es decir, deben realizarse con apego a la equidad e igualdad social de personas con diferentes vulnerabilidades y disposición de recursos económicos y tecnológicos.

La cultura sí se transforma y sí se crea, así que es un compromiso compartido evolucionar en materia de estos derechos, para facilitar el desarrollo integral, sostenible y accesible de nuestras poblaciones que brinden valor y bien común.

Los derechos fundamentales no son retóricos, deben ser sustantivos, con impactos importantes para cada persona que habita o transita en la espectacular Ciudad de México, lo que se logra gracias a sus mecanismos perfectibles y contextualizados a las realidades propias de la cultura mexicana y capitalina.

V.4. CONCLUSIÓN

Sin la participación ciudadana no se podrá lograr un desarrollo óptimo, requiere de la corresponsabilidad de todas las esferas sociales, incluidas las familias, las instituciones públicas y privadas, al igual que las instancias obligadas y el garante de acceso a la información pública, las cuales deberán crear una cultura de confianza través de la comunicación clara, directa y eficiente en constante progreso.

El acceso a la información pública es, por lo tanto, un componente esencial para el ejercicio de los derechos fundamentales y la consolidación de la confianza ciudadana traducida en una democracia robusta, integral y transparente, con miras a dotar de oportunidades a las poblaciones en favor del bien común.

REFERENCIAS

Constitución Política de los Estados Unidos Mexicanos (CPEUM). (última reforma: 15 de octubre de 2025). <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>.

Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México. (INFO CDMX, 2024). <https://www.infocdmx.org.mx/>

Solís-Macías, V. M. (2017). La información y sus transformaciones: ¿qué significa el término información? En P. Hernández Salazar (Coord.). *Significados e interpretaciones de la información desde el usuario*. (pp. 1-28). UNAM, Instituto de Investigaciones Bibliotecológicas y de la Información. https://www.academia.edu/39312600/la_informaci%C3%B3n_y_sus_transformaciones_¿qu%C3%A9_significa_el_t%C3%A9rmino_informaci%C3%B3n

CAPÍTULO VI

La transparencia y el poder judicial

Juan Carlos Abreu y Abreu¹

SUMARIO: VI.1. Preámbulo; VI.2. Génesis y evolución de la noción de transparencia; VI.3. Taxonomía de la transparencia; VI.4. Dimensiones de la transparencia; VI.5. La transparencia en el entorno judicial; VI.6. Conclusiones.

RESUMEN: Sustantivo o adjetivo, la transparencia es un término que, en los albores del siglo XXI, ha tomado protagonismo y relevancia. En el *Estado de derecho*, específicamente en sistemas democráticos, es considerado elemento toral para alcanzar su teleología, de manera tal que su opacidad o inexistencia se asocia de manera irrefutable a Estados fallidos o sistemas autoritarios.

Su presencia no sólo se construye al ámbito del poder ejecutivo, sino que se identifica en actuaciones del legislativo y en las acciones del judicial. Justamente, en este último, el reto ha resultado significativo, pues encuentra un nicho de oportunidad en la impartición de justicia digital, la que, desde diversas posturas doctrinarias y estudios estadísticos, propicia la disminución de corrupción y acerca a la ciudadanía a ejercer el derecho universal de acceso a la justicia.

PALABRAS CLAVE: Transparencia, transparencia activa, transparencia pasiva, Poder Judicial, justicia digital.

VI.1. PREÁMBULO

La transparencia ha experimentado un conjunto de procesos que combinan relaciones [divergentes y de evidente contraste como:] la opacidad y la publicidad, el secreto y la noticia, los súbditos y ciudadanos, los claroscuros y las luces, el centralismo burocrático y las libertades individuales-colectivas, los privilegios y la igualdad; que dan cuenta de cómo el poder público se diseña e implementa con la intervención de actores, organismos, estrategias, tiempos y objetivos puntuales [...]. (Uvalle Berrones, 2016, p. 200)

¹ Miembro del Claustro Doctoral de la Escuela Judicial del Estado de México. Integrante del Sistema Nacional de Investigadores (SNI). Profesor de la Facultad de Derecho de la Universidad Autónoma del Estado de México (UAEM). ORCID: 0000 0002 1397 2592. Actualmente, Director del Centro de Investigaciones Judiciales del Poder Judicial del Estado de México.

Elementos que han permitido su conformación como política pública. De este modo, hoy en día, la transparencia es una política pública con reconocimiento de instituciones internacionales, como el Banco Mundial, la Organización de las Naciones Unidas, la Organización para el Comercio y el Desarrollo Económico, Transparencia Internacional, entre otras, que ha venido modificando la relación de los ciudadanos con el Estado de manera significativa; eliminando cualquier idea de que se trata de un tópico de moda.

La visión de los Estados modernos como “cajas negras”, “sistemas cerrados” o “ámbitos inaccesibles”, [...] está perdiendo legitimidad desde el momento en que los asuntos colectivos tienen como trasfondo el vigor de los espacios públicos [...] y hacer posible que el poder sea más abierto y responsable ante los ciudadanos. (Uvalle Berrones, 2016, p. 209)

Es decir, la vieja usanza era restringir información en nombre de los llamados “secretos de Estado”; sin embargo, a partir del nuevo milenio; las diversas instituciones de los Estado-Nación “permiten a los ciudadanos acceder a los bancos de información que producen y resguardan, [...] para responder a las nuevas dinámicas de los espacios públicos [...] en la visión de los Estados modernos, constitucionales y democráticos” (Uvalle Berrones, 2016, p. 209). Con lo anterior, se permite dilucidar que:

[...] el valor de la transparencia debe respaldarse en calidad de las instituciones, las cuales [...] son portadoras de los valores de la democracia, diseñando una política pública que con claras reglas de juego para los ciudadanos con el Estado para que la información público-gubernamental sea formalizada y legitimada en el proceso que valida el derecho de acceso a la información. (Uvalle Berrones, 2016, pp. 200-201)

VI.2. GÉNESIS Y EVOLUCIÓN DE LA NOCIÓN DE TRANSPARENCIA

La transparencia, gramaticalmente es un adjetivo calificativo que indica la característica de los cuerpos que permiten el paso de la luz, la palabra fue “exportada” a la semántica política por la necesidad de manifestar un sustantivo que indicara el límite a una de las formas en que se manifiesta el absolutismo. (Simmental Franco, 2017, p. 145)

Resulta un elogio identificar en el México prehispánico a uno de los temas que más se destacaba culturalmente:

la severidad con la que se castigaban los delitos, y el enorme valor que se le daba a la honestidad y al reconocimiento de la palabra, [...]. Es decir, la importancia de la honestidad y de la “transparencia” entre el decir y el hacer, no sólo era consecuencia de ideales sociales, sino de necesidades derivadas de sus propias condiciones de vida. (Simental Franco, 2017, p. 148)

Conforme a diversos sociólogos y antropólogos, desde la Conquista hasta el siglo XX, específicamente la década de los ochenta; México y Latinoamérica en general, vivieron esquemas de opacidad y discrecionalidad en las esferas públicas que enturbiaron la democracia imperante; convirtiéndose la transparencia en un elemento aspiracional. Es hasta los noventa, cuando nació y se fortificó la exigencia de mayor transparencia y mejor rendición de cuentas en todo el orbe.

La democratización en América Latina, Europa del este y varios países de Asia y África fue motivo de que los nuevos gobernantes democráticamente electos y su práctica de gestión pública fueron sometidos a una intensa vigilancia. Pero también en países avanzados y con democracias bien establecidas se revelaron en los últimos años sonados casos de corrupción gubernamental. De allí que los conceptos y procedimientos de transparencia y rendición de cuentas se enfocaran en forma prioritaria y casi exclusiva a la lucha contra la corrupción pública.

La transparencia y la rendición de cuentas “[...] Requieren una participación activa de la ciudadanía y la vigilancia de la sociedad civil organizada y de los medios de comunicación. Requiere, también, la creación de mecanismos institucionales de responsabilidad y control que fortalezcan tanto la participación ciudadana como el gobierno responsable” (Emmerich, 2004, p. 69). En el siglo XXI, la democracia, ciudadanía y transparencia son el trinomio por postular en las sociedades democráticas.

VI.3. TAXONOMÍA DE LA TRANSPARENCIA

Distinguimos dos modalidades de transparencia:

(I) transparencia activa, que “consiste en la difusión periódica y sistematizada de información [relativa al desempeño de las funciones públicas]. Se trata de la obligación impuesta a los órganos del Estado para que, con periodicidad [...] publiquen toda la información que sea necesaria para una evaluación social de su desempeño [...]” (Emmerich, 2004, p. 80). Esta modalidad es con la que poblacionalmente estamos familiarizados; por ejemplo, el Poder Judicial del Estado de México a través de su portal de Internet, los datos e información que difunde y pone al alcance de la ciudadanía es de tipo activa; al permitir la consulta por ejemplo de sentencias en versión pública, de precedentes y de la agenda estadística; y, (II) la transparencia pasiva:

[...] que denota la obligación del Estado para conceder, a los ciudadanos que lo requieran, acceso oportuno a la información que obra en poder de los órganos públicos, salvo que medie razón legalmente establecida e imparcialmente acreditada para justificar la reserva o secreto de determinado tipo de información, [como lo son:] la seguridad nacional, derechos de terceros, procedimientos en trámite cuya revelación anticipada perjudique el cumplimiento de una función pública, entre otros. (Emmerich, 2004, p. 80)

VI.4. DIMENSIONES DE LA TRANSPARENCIA

“La transparencia se caracteriza por tener tres dimensiones que sitúan su complejidad en términos de la acción de gobierno: 1) dimensión técnica [que] concierne al mundo complejo de los procesos que sustentan como operación de gobierno para diseñar y ejecutar las disposiciones que la constitucionalizan y legalizan; en estricto sentido, esta primera dimensión se conforma por el marco normativo constitucional de la transparencia y el acceso a la información; 2) dimensión política [que] refiere al modo en que favorece el diálogo entre los gobernantes y los gobernados con fines de evaluación, entiéndase hoy en día las actividades de rendir o proporcionar informes de actividades de las personas al frente de las instituciones; y, “3) dimensión institucional, que alude a que es parte de las reglas del juego que se definen entre los actores que más influencia tienen para que sea una política pública” (Uvalle Berrones, 2016, p. 212).

Se debe de reconocer de manera satisfactoria que México ha arropado la transparencia en diversas políticas públicas y, de manera concreta, cada institución de los tres ámbitos de poder en el país, cuentan con su sitio o portal de acceso a la transparencia.

VI.5. LA TRANSPARENCIA EN EL ENTORNO JUDICIAL

La transparencia es un tema central en el debate político-académico, y es uno de los rubros que deben atenderse prioritariamente en el ejercicio del poder en cualesquiera de los tres ámbitos de la división de poderes.

Bajo la tesitura clásica de dividir el ejercicio del poder en: impartición de justicia, expedición de leyes y administración pública, queda claro que la transparencia va implícita en el ámbito jurisdiccional. Y que la ética judicial debería exponer permanentemente una conducta transparente. (Simental Franco, 2017, p. 153).

En todo Estado de Derecho contemporáneo, la transparencia es una expresión de la ética. De manera concreta “la transparencia es causa y fin de la ética judicial, que es un componente permanente en la manifestación práctica de la función jurisdiccional” (Simental Franco, 2017, p.144).

Este aspecto, en el Poder Judicial mexicano, cuenta con el Código de Ética y con el Comité de Ética y Prevención de Conflictos de Interés, el cual, busca incrementar el nivel de credibilidad, solvencia moral y ética que deben tener las servidoras y servidores públicos, en especial, jueces, juezas, magistradas y magistrados. Lo anterior conlleva dos acciones muy puntuales y claras para fortalecer la transparencia, la rendición de cuentas, el combate a la corrupción y los actos contrarios a la integridad.

Si no fuese suficiente, en el engranaje de la impartición de justicia, una figura que suma a la transparencia y al combate de la corrupción es la justicia digital, la cual desde el año 2016 se encuentra habilitada, encontrando su auge durante la pandemia sanitaria por Covid-19; el PJ Edomex ha consolidado el principio de economía el cual implica “reducir el litigio en términos tiempo y uso de recursos administrativos para llegar a una solución de la cuestión problemática lo más pronto posible” (Castaño, 2022, p. 69).

Y respecto al aspecto de la Lealtad Procesal, traspolado “[...] al entorno virtual involucra el respeto de las buenas prácticas de seguridad digital y las previsiones necesarias para que la documentación digital allegada al proceso no asocie intrusiones maliciosas o archivos corruptos” (Castaño, 2022, p. 71).

VI.6. CONCLUSIONES

Los Estados modernos como *cajas negras*, *sistemas cerrados* o *ámbitos inaccesibles* están perdiendo legitimidad y propician el activismo ciudadano. La transparencia es el elemento imprescindible en los Estados democráticos y constitucionales, para consolidar el debido actuar de las instituciones. Los Tribunales de Justicia tienen introyectado el concepto de transparencia y sus beneficios, tan es así, que a través de la justicia electrónica o digital se fortalece la credibilidad de la institución en la ciudadanía.

REFERENCIAS

- Castaño, D. (2022). *La Justicia como servicio digital*. Instituto de Ciencia Política Hernán Echavarría Olózaga. <https://icpcolombia.org/wp-content/uploads/2023/03/14.10.22-final-diagramado-Virtual-1.pdf>
- Emmerich, G. E. (segundo semestre, 2004). Transparencia, rendición de cuentas, responsabilidad gubernamental y participación ciudadana. *Revista Polis: Investigación y análisis sociopolítico y psicosocial*, 2(4), 67-90. <https://www.redalyc.org/pdf/726/72620404.pdf>

- Simental Franco, V. A. (enero-junio, 2017), Transparencia y ética judicial. *Revista Cuestiones Constitucionales de la Universidad Autónoma del Estado de México*, 36, 143-166. <https://revistas.juridicas.unam.mx/index.php/cuestiones-constitucionales/article/view/10862/12949>
- Uvalle Berrones, R. (enero-abril, 2016) Fundamentos de la transparencia en la sociedad contemporánea. *Revista Mexicana de Ciencias Políticas y Sociales de la Universidad Autónoma del Estado de México*, 61(226), 199-220. <https://www.revistas.unam.mx/index.php/rmcpys/issue/view/4193>

CAPÍTULO VII

Interpretación a la Ley Interamericana sobre Gestión Documental: una óptica en la dirección de recursos humanos

Federico Hernández Pacheco¹

SUMARIO: VII.1. Introducción; VII.2. Ley Interamericana sobre Gestión Documental y la dirección de los recursos humanos: interpretación; VII.3. Conclusiones.

PALABRAS CLAVE: Gestión documental, recursos humanos, archivos, capacitación.

VII.1. INTRODUCCIÓN

Aprobada en el año 2020 por la Asamblea General de la Organización de los Estados Americanos, la Ley Interamericana sobre Acceso a la Información Pública también cuenta con una Ley Modelo Interamericana sobre gestión documental y una Guía para su aplicación. Esta Ley Modelo es relevante y original, ya que contiene todas las funciones del ciclo de los documentos y archivos, en el estricto sentido, sobre su política de gestión, organización, transferencia, acceso, seguridad, conservación, difusión y servicios, gestión electrónica, así como el importante papel de los perfiles y capacitación del personal (OEA, 2020).

Los archivos se entienden como aquellos soportes impresos o digitales que incluyen información de interés público o privado, “[...] son el conjunto de documentos que surgen mediante la creación de información que va a ser de utilidad personal o institucional y se resguardan bajo criterios o normas de selección y organización en espacios físicos o digitales para su correcta utilización” (Hernández Pacheco *et al.*, 2023, p. 11). En ocasiones, requieren controles de seguridad para su correcto acceso, debido a las características de sus contenidos, como son aquellos casos de seguridad nacional o protección de datos personales.

En este contexto, la administración o gestión documental se lleva a cabo mediante procesos o funciones donde intervienen personas con diversas especialidades como

¹ Investigador Titular del Instituto de Investigaciones Bibliotecológicas y de la Información de la Universidad Nacional Autónoma de México (UNAM). Pertenece al Sistema Nacional de Investigadoras e Investigadores, Nivel II, del Consejo Nacional de Humanidades, Ciencias y Tecnologías (CONAHCYT).

son: los creadores de documentos archivísticos, los editores, diseñadores e impresores y, los especialistas en información seleccionan, organizan, conservan y difunden dichos documentos a través de espacios físicos y virtuales (Hernández Pacheco *et al.*, 2023, p. 8). Al respecto, es importante señalar la relevancia del proceso administrativo en el manejo de los documentos y servicios de archivo, mecanismo que proviene del campo de las Ciencias de la Administración que contiene las siguientes funciones: a) planeación; b) organización; c) dirección y; d) control. Lo cual, se traduce en 1) contar con un plan estratégico de programas de trabajo; 2) asignarlo a las personas que cuenten con los recursos y competencias adecuados; 3) mantener una mentalidad de liderazgo para manejar eficientemente equipos de trabajo y lograr un excelente clima organizacional y; 4) el diseño y aplicación constante de esquemas de supervisión o evaluación mediante herramientas e indicadores de resultados. En efecto, la gestión documental va más allá de un aspecto técnico, involucra a todos los niveles de la organización para contar con un sistema eficaz de manejo de la información archivística para la correcta toma de decisiones, investigación, generación de conocimientos y puntual atención ciudadana.

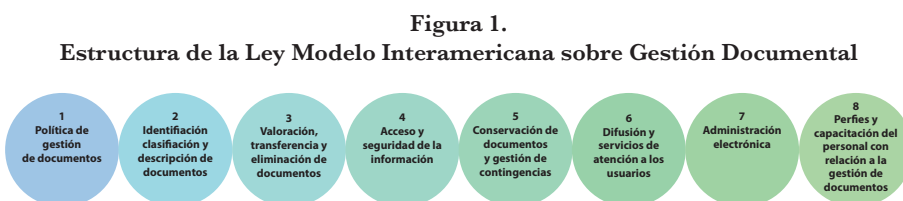
Precisamente la dirección de los recursos humanos se vuelve indispensable al involucrar a las personas en diferentes procedimientos para cumplir con los objetivos, metas, programas de trabajo y resultados. La dirección de los recursos humanos se define como el manejo adecuado de las personas que integran y desempeñan una actividad específica dentro de una institución u organización para su correcto funcionamiento, en donde se integran al trabajo mediante sus habilidades y talentos, perfiles de puestos, conocimientos, competencias, personalidad, aspiraciones, percepciones, etc.; enfocadas hacia el desarrollo organizacional (Chiavenato, I. 2007, p. 1).

Es así como la Ley Modelo Interamericana sobre Gestión Documental (OEA, 2020) contempla 5 capítulos respecto a la clasificación y descripción, seguridad, conservación, difusión y administración electrónica de documentos y archivos; además de 3 capítulos inherentes a la dirección del personal que proponemos interpretar bajo la óptica conceptual y, derivada de la praxis profesional, con el fin de lograr un mayor entendimiento sobre la dimensión y alcance de esta ley que consideramos, cubre de una manera precisa e innovadora todas las fases del ciclo de los documentos y archivos. Al respecto, Artur Kaufmann, autor sobre tópicos de hermenéutica jurídica, señala que el Derecho no solamente se encuentra en las leyes, sino en su interpretación y crítica constructiva para llegar a grandes conclusiones y por consecuencia, facilitar su aplicación. Kaufmann cita a Savigny, quien bien señala que interpretar es ‘reconstruir el pensamiento interno de la ley’ mediante cuatro elementos: 1. Gramatical; 2. Lógico; 3. Histórico y; 4. Sistemático” (Kaufmann, 1992, p. 38).

VII.2. LEY INTERAMERICANA SOBRE GESTIÓN DOCUMENTAL Y LA DIRECCIÓN DE LOS RECURSOS HUMANOS: INTERPRETACIÓN

La presente ley es una importante herramienta para realizar la descripción, clasificación, valoración, difusión, custodia y protección de los documentos que contienen información con el fin de asegurar una política precisa de gestión documental y archivos que se encuentre en armonización con las legislaciones de acceso a la información pública, protección de datos, transparencia y rendición de cuentas, gobierno y datos abiertos, etc.

La estructura de la ley consta de ocho capítulos que se muestran en la siguiente figura:



Fuente: (Hernández Pacheco y Stable Rodríguez, 2024, p. 425).

A continuación, realizaremos nuestra interpretación y comentarios a tres capítulos de esta Ley, que contienen funciones inherentes a la administración organizacional y dirección de recursos humanos:

a) Capítulo 1. Política de Gestión de Documentos

Artículo 2. Implementación de una política de gestión de documentos:

2. n La política de gestión de Documentos y archivos regulará las prácticas realizadas por los responsables de su gestión y por cualquier otra persona que genere o use documentos en el ejercicio de sus actividades, incluyendo: a. El establecimiento de normas y buenas prácticas; b. El diseño de procedimientos y directrices; c. La prestación de servicios relacionados con su gestión y uso [...]. (OEA, 2020)

La normatividad documental es esencial para lograr resultados en el registro, clasificación y recuperación de la información, así como en el intercambio de datos bajo códigos similares previamente establecidos. Además, se recomienda incorporar normas como la ISO 30301:

[...] que contempla los requerimientos y contexto de la organización, así como la estructura organizacional; los flujos de información y los procesos para la toma de decisiones; los valores y las relaciones institucionales; el liderazgo y compromiso; la dirección eficiente de los recursos humanos; la mejora continua; la gestión por competencias; y la comunicación interna y externa permanente para la correcta implementación del Sistema de Administración de Archivos. (Hernández Pacheco *et al.*, 2023, p. 15)

Sobre las buenas prácticas, el denominado *benchmarking*, actividad dentro del campo de las Ciencias de la Administración, ofrece herramientas y listas de cotejo para detectar, documentar y aplicar casos de éxito de otras instituciones u organizaciones nacionales e internacionales.

Los procedimientos son parte de la administración, deberán revisarse constantemente e ir interconectados con el fin de lograr óptimos resultados en productos y servicios. Las directrices son líneas de acción, ejes que van relacionados con los programas de trabajo estratégicos de la organización. Los procedimientos son parte del contenido de normas internacionales como las ISO 9000:2015 sobre Gestión de la Calidad y las directrices se recomiendan para el diseño de planes estratégicos.

El servicio se ha convertido en una parte fundamental de todas las áreas de trabajo, ya sea de organizaciones públicas o privadas, es la fase final de la cadena de un proceso donde se visualizan los resultados, en este caso de gestión documental junto con las personas que brindan los servicios. Por ello, la capacitación continua en materia de atención al público se vuelve imprescindible.

Artículo 3. Nombramiento de una autoridad que lidere la política de gestión:

1. Todo sujeto obligado deberá establecer una unidad o agencia en la que se desarrolle y lidere la política de gestión de Documentos, lo que permitirá garantizar que las decisiones, las acciones y las actividades de la gestión documental se establezcan conforme al marco legal y queden debidamente documentadas.
2. La alta dirección del sujeto obligado debe designar un representante específico quien, al margen de otras responsabilidades, debe ser garante de que la política y el sistema de gestión de documentos se establezca, implemente y mantenga de acuerdo con los requisitos necesarios. (OEA, 2020)

El liderazgo, vinculado a la alta dirección, es imprescindible para el soporte y alcance de los proyectos emprendidos. En efecto, la toma de decisiones fundamentadas en los conocimientos de los líderes será básica en todo momento.

Definitivamente el líder debe ser aquel que asume responsabilidades de forma inteligente, es proactivo y toma los problemas como un desafío personal, además crea y propone soluciones viables con una actitud positiva. Demuestra una

atención especial para encontrar oportunidades y sale a buscarlas constantemente, pero también está siempre preparado para aprovecharlas. Deja además el liderazgo autoritario y logra el liderazgo participativo. (Hernández Pacheco, 2020, p. 351)

Delegar es todo un arte, el líder deberá designar las actividades, pero deberá supervisarlas constantemente, aplicando la base 80/20, es decir, dedicar el 80 por ciento de su tiempo a dirigir a sus colaboradores y el 20 por ciento a planear y organizar trabajo de oficina.

Artículo 4. Procesos de gestión documental:

2. La política de gestión de Documentos deberá implementar la realización periódica, según intervalos acordados en el sujeto obligado, de supervisiones y evaluaciones de todos o parte de los procesos de gestión de documentos como un compromiso de calidad y mejora continua. (OEA, 2020)

La evaluación se convierte en una estrategia de mejora continua para incrementar la calidad de los procesos, productos y servicios. Los mecanismos de evaluación o medición permitirán establecer acciones de mejora al obtener información puntual sobre los resultados esperados en relación con los objetivos y metas establecidos y, de esta forma, diseñar acciones correctivas o preventivas vinculadas a la política de gestión (Nava Carbellido y Jiménez Valadez, 2003, pp. 29-30). La evaluación permitirá revisar procesos, reducir errores y mantener mejoras graduales como lo establece la filosofía de la mejora continua.

b) Capítulo 5. Conservación de Documentos y Gestión de Contingencias

Artículo 23. Evaluación de riesgos:

1. Los sujetos obligados realizarán una evaluación de riesgos para conocer las fortalezas y debilidades en materia de protección de cada uno de los centros de archivo [...].
2. La información recopilada en la evaluación de riesgos se materializará en un mapa de riesgos, que servirá como guía para el seguimiento y establecimiento de rutinas de inspección, como herramienta de actualización obligada que permitirá crear prioridades en la actuación. (OEA, 2020)

Cómo responder a los riesgos es un reto actual según los profesores Gómez Mejía, Balkin y Cardy (2016), que no sólo está relacionado con los recursos materiales como son los documentos de archivo, sino con la atención a las personas que manejan dichos

recursos (p. 11). En efecto, al ocurrir desastres naturales tales como pandemias, terremotos, contaminaciones por agentes químicos, huracanes e inundaciones, o situaciones provocadas por acciones de terrorismo, se deberán contemplar matrices de riesgos que conserven en buen estado los documentos y las áreas donde estos se resguardan, pero sobre todo, se deberán planificar aspectos como los pagos por incapacidades o defunciones, los gastos de subsistencia del personal, la posible contratación de empleados temporales, así como la previsión de la pérdida de talentos, entre otros aspectos.

c) Capítulo 8. Perfiles y Capacitación del Personal con Relación a la Gestión de Documentos

Artículo 30. Alta dirección:

1. La alta dirección del sujeto obligado establecerá la orientación de la política de gestión de Documentos y archivos para:

[...]

b. Imponer al personal la adopción de los requisitos y deberes inherentes a la gestión y custodia de los documentos;

[...]

2. Aunque la alta dirección de un sujeto obligado delegue la responsabilidad de la gestión y custodia de los Documentos en todo el equipo humano de su institución, conservará la responsabilidad última en materia de rendición de cuentas.

3. Si la complejidad del sujeto obligado lo requiriera, la alta dirección de este nombrará un representante en gestión de Documentos y archivos a nivel operativo que debe tener definidos su papel, responsabilidades y competencias. (OEA, 2020)

La organización del trabajo y la dirección es parte del proceso administrativo, y es a lo que se refiere el apartado 1 y el inciso b. Orientar se refiere a guiar el trabajo para la consecución de los objetivos. La adopción de requisitos y deberes significa organizar todas las actividades o labores que se realizan para alcanzar los objetivos propuestos en la política de gestión. Lo que se busca es que todas las partes de la institución unan sus esfuerzos para la obtención de resultados (Hernández Pacheco, 2020, p. 44).

En el apartado número 2 queda claro que la alta dirección asume los compromisos de su equipo de trabajo, en el sentido de que todas las actividades que se organicen y dirijan serán el reflejo del liderazgo y correcta planeación del sujeto obligado.

El apartado número 3 se refiere al perfil que debe reunir la persona que esté al frente de la gestión documental. Para ello, el análisis de puestos y la descripción de perfiles es una técnica utilizada en el ámbito de los recursos humanos y que actualmente establece y señala como importante la Norma Oficial Mexicana 035.

Artículo 31. Mandos intermedios:

1. Los jefes de las unidades de gestión de los sujetos obligados son responsables de garantizar que el personal a su cargo cree, mantenga y custodie los Documentos como parte integrante de su trabajo, de acuerdo con las políticas, procedimientos y normas previamente establecidas.
2. Los mandos intermedios de los sujetos obligados fomentarán y mantendrán reuniones de trabajo interdisciplinarias periódicas entre el personal que crea y custodia Documentos en su ámbito de responsabilidad, los técnicos de la información y los técnicos de archivos del sujeto obligado, con el fin de desarrollar, implementar, revisar y mejorar los sistemas de gestión en su ámbito de actuación, y con el fin de crear, custodiar y tratar Documentos auténticos, íntegros y disponibles. (OEA, 2020)

La dirección y unidad de mando son principios de la administración esenciales para el manejo de personal, aunque en la actualidad las habilidades blandas para fomentar la participación de equipos se han convertido en un aspecto esencial para aquellos que son jefes o encargados de áreas de trabajo, así como las habilidades para mantener un clima laboral adecuado y gestionar los conflictos cotidianos.

Asimismo, brindar información y tomar en cuenta las ideas u opiniones propuestas por los integrantes de la organización a través de reuniones, no solo fomenta un clima laboral estable, sino que brinda la posibilidad de innovar con el fin de lograr la excelencia en las actividades encomendadas.

Artículo 32. Técnicos de archivo:

1. Los técnicos calificados en archivos y gestión documental son los responsables de todos los aspectos relativos al tratamiento archivístico y correcta gestión de documentos del sujeto obligado, incluyendo el diseño, implementación y mantenimiento del sistema de gestión de documentos y sus operaciones.
2. Los técnicos de archivos son un recurso humano transversal y altamente calificado, fundamental para el sujeto obligado en materia de comunicación, concientización, asesoramiento y formación de los equipos humanos en tratamiento archivístico y gestión de los Documentos.
3. Los técnicos de archivos deben trabajar en colaboración con los técnicos de la información y de las comunicaciones en el diseño, implementación y mejora del sistema de gestión, en la arquitectura de la información, en la seguridad de la información y en el acceso y recuperación de esta. (OEA, 2020)

La archivística es una rama de las Ciencias de la Información y Documentación que en algunos países se estudia a nivel posgrado. Existen líneas de investigación en centros e instituciones que realizan investigación científica, lo cual nos asegura que es

un área con un *corpus* de conocimientos sólidos, tanto teóricos como prácticos. Nos parece que la denominación habrá de ser “los profesionales de archivos”, ya que son expertos que llevarán a cabo todas las fases de la cadena documental con una visión experimentada y transdisciplinaria.

Artículo 33. Plan de comunicación:

1. El plan de comunicación garantizará que los procedimientos y beneficios de la gestión de documentos y archivos se comprendan por todo sujeto obligado, clarificando las directrices en materia de gestión de documentos y situando los procedimientos y procesos en un contexto que permita entender las razones de su necesidad.
2. El plan de comunicación articulará procedimientos para que los documentos relativos a la política de gestión de Documentos y archivos del sujeto obligado sean accesibles y lleguen a todos sus integrantes, siendo conveniente un fácil acceso a un paquete de Documentos que informen de responsabilidades y procedimientos estratégicos. (OEA, 2020)

La comunicación organizacional es:

[...] entendida como una dinámica de [canales] de información y puntos de encuentro entre los diferentes departamentos o áreas que componen a la institución, con el objetivo de establecer acuerdos, sinergias y soluciones a problemas comunes [...]. [C]omunicar es hacer llegar a las personas determinados mensajes o ideas con un objetivo claro y en el momento oportuno, además que dichos mensajes sean entendidos por todas las audiencias. Se dice también que es un proceso a través del cual las funciones de dirección, tales como la planeación, organización, ejecución y control son llevadas a cabo efectivamente. (Hernández Pacheco, 2020, p. 219).

Artículo 34. Concienciación del equipo de trabajo:

1. El sujeto obligado debe crear conciencia y mantener a su personal al tanto de:
 - a. La relevancia de cada una de sus actividades individuales y como éstas contribuyen a la consecución de los objetivos del sistema de gestión de Documentos y archivos;
 - b. Los aspectos significativos del sistema de gestión de Documentos y archivos que están asociados a su trabajo y los beneficios en la mejora de su desempeño;
 - c. La importancia del cumplimiento de la política y procedimientos de la gestión de los Documentos y archivos del sujeto obligado y;
 - d. Los riesgos y consecuencias del incumplimiento de los procedimientos establecidos. (OEA, 2020)

La dirección por objetivos, atribuida a Peter Drucker, está relacionada con el desempeño del personal. La dirección por objetivos fomenta la participación de todas y todos los colaboradores a fin de cumplir con los objetivos estratégicos de la organización, mide cada una de las contribuciones y, sobre todo, proporciona las bases para el otorgamiento de incentivos o recompensas (Naranjo-Pérez *et al.*, 2005, p. 59). En efecto, es un sistema que vincula las metas y objetivos con el trabajo de las personas; establece los beneficios de mantener un correcto desempeño y las consecuencias al no cumplir adecuadamente con las tareas asignadas.

Artículo 35. Plan de capacitación continua:

1. El sujeto obligado establecerá entre sus estrategias el diseño de un plan de capacitación continua y designará a un responsable con un nivel jerárquico adecuado para que se ocupe del programa, lo dote de los recursos necesarios y se responsabilice de su diseño y ejecución.
2. La capacitación se destinará a todo aquel personal del sujeto obligado que crea, mantiene o custodia documentos (también a directivos y alta dirección), a contratados externos, a voluntarios y a cualquier otra persona que se encargue de la totalidad o parte de una actividad en la que se creen documentos y se incorporen a los sistemas de gestión de documentos del sujeto obligado, teniendo en cuenta sus funciones y responsabilidades.
3. El análisis de las necesidades de capacitación se sustentará en encuestas periódicas, dirigidas al equipo humano, en evaluaciones de rendimiento del personal y en análisis de puntos débiles, riesgos o lagunas existentes en la gestión de documentos y archivos del sujeto obligado.
4. La capacitación debe ser evaluada y revisada periódicamente mediante: a. La medición de su rendimiento; b. La realización de auditorías; y c. El contraste de los niveles de competencia del personal frente a los objetivos del programa de formación.
5. Los sujetos obligados revisarán periódicamente tanto los contenidos de la capacitación como su orientación, para garantizar su efectividad y adecuación a los cambios que se puedan producir en el contexto (legal, social, administrativo, etc.) en el que se inscribe el sujeto obligado y en el propio sistema interno de gestión de documentos y archivos.
6. Dentro del plan de capacitación se promoverán los ajustes necesarios para alcanzar una mejora continua y se diseñarán mecanismos para que el personal capacitado se beneficie de las mejoras introducidas en las nuevas actividades.
7. Los sujetos obligados evaluarán el nivel de satisfacción de las personas que hayan participado en una actividad de capacitación (por ejemplo, mediante encuestas de satisfacción). (OEA, 2020)

Detectar necesidades de capacitación, elaborar un plan, aplicarlo y evaluarlo son las fases de un programa que habrá de implementarse de forma periódica. Definitivamente la capacitación conecta con el desarrollo continuo de la organización y las actividades que se realicen, el trabajo mejora considerablemente mediante acciones formativas. En efecto, la capacitación:

[...] ya es reconocida como un proceso sistemático, inherente a la estrategia de las instituciones para desarrollar competencias, para que las personas sean más creativas, productivas e innovadoras y así puedan aportar un valor añadido a la institución en conjunto. De esta forma, contribuyen al cumplimiento de objetivos, metas y resultados. (Hernández Pacheco, 2020, p. 233)

Aunque, es necesario planear adecuadamente los programas de capacitación para que logren una conexión con los objetivos estratégicos de nuestra institución, con el fin de asegurar que las inversiones en capacitación tengan un impacto en los resultados. Los especialistas señalan que la planeación de la capacitación utiliza un enfoque sistemático compuesto de cuatro fases: 1) diagnóstico o análisis de necesidades, mediante un análisis de la organización y los puestos de trabajo, así como de las funciones del personal como la selección, planes de carrera, comunicación, evaluación del desempeño, retribución y prevención de riesgos laborales, entre otras funciones; 2) diseño del programa, el cual se sugiere que sea integrado y sistemático, así como que contenga los objetivos, contenidos, métodos y técnicas de enseñanza, el número ideal de alumnos, profesorado competente, espacios y horarios adecuados; 3) aplicación, que es el seguimiento de las acciones de capacitación en relación con su calidad y apoyo permanente de todas las áreas involucradas, principalmente de la alta dirección y; 4) evaluación, que se relaciona tanto con el cambio de hábitos y comportamientos de quienes tomen los cursos y talleres, como con la mejora de productos, servicios y el impacto de los programas formativos en relación con los beneficios obtenidos. (Hernández Pacheco, 2020, pp. 237-274).

VII.3. CONCLUSIONES

La Ley Modelo Interamericana de Gestión Documental (LMIGD) complementa las disposiciones de nuestra legislación de archivos, particularmente de los capítulos que contiene el Título Segundo denominado “De la Gestión Documental y Administración de Archivos” de la Ley General de Archivos, ya que la LMIGD contiene apartados no solo inherentes a la organización, digitalización y preservación de los documentos, sino que contempla varios conceptos y fases del proceso administrativo y de la dirección de los recursos humanos.

En efecto, trata aspectos sobre normatividad, buenas prácticas, procedimientos, directrices, el servicio, el papel del líder, la evaluación y mejora continua, la prevención de riesgos, el diseño de perfiles, las competencias, la comunicación organizacional, la dirección por objetivos y los programas de capacitación o formación continua; todas actividades, funciones y argot vinculado con las Ciencias de la Administración y la Dirección de los Recursos Humanos, disciplinas que se investigan y estudian en las universidades e instituciones más prestigiosas del mundo.

Por lo que en este trabajo nos hemos dado a la tarea de interpretar y comentar exclusivamente apartados de la Ley que abordan esas temáticas, con el fin de lograr un mayor campo de aplicación en aquellas organizaciones que han emprendido proyectos de gestión documental con el fin de cumplir como sujetos obligados, pero también, para lograr un adecuado sistema de información que apoye las actividades sustantivas como son la toma de decisiones y la generación de nuevos conocimientos. Definitivamente, interpretar una ley desde la teoría y la práctica brinda mayores posibilidades de ampliar los beneficios de las disposiciones legales.

REFERENCIAS

- Chiavenato, I. (2007). *Administración de recursos humanos. El capital humano de las organizaciones*. (8a ed.). McGraw-Hill Interamericana.
- Gómez-Mejía, L.R.; Balkin, D.B; y Cardy, R.L. (2016). *Gestión de recursos humanos*. (8a. ed.). Pearson Educación. <https://unamex.vitalsource.com/reader/books/9788490352984/pageid/41>
- Hernández Pacheco, F. (2020). *Dirección de recursos humanos en bibliotecas y otras instituciones*. (2a. ed.). UNAM, Instituto de Investigaciones Jurídicas; Instituto de Investigaciones Bibliotecológicas y de la Información. <https://archivos.juridicas.unam.mx/www/bjv/libros/14/6792/16.pdf>
- Hernández Pacheco, F., Carreón Trujillo, C., Córdova Palomino, M., Reyes Hernández, M. (2023). *Archivos y administración documental. Fundamentos y tendencias*. Porrúa; INFOCDMX.
- Hernández Pacheco, F, y Stable Rodríguez, Y. (2024) “Los archivos en las Américas y la Ley Modelo Interamericana sobre Gestión Documental”. En María Gracia Andía (dir). *Acceso a la información, transparencia y derechos humanos : desde una mirada regional*. Albremática <https://tienda.eldial.com/productos/e-book-acceso-a-la-informacion-transparencia-y-derechos-humanos-desde-una-mirada-regional/>
- Kaufmann, A. (1996). Concepción hermenéutica del método jurídico. En *Persona y Derecho. Revista de fundamentación de las Instituciones Jurídicas y de Derechos Humanos*, (35), 11-36. <https://dadun.unav.edu/entities/publication/21bb385a-57ce-4be9-a89a-14caa8e4cd84>

- Naranjo-Pérez, R., Mesa-Espinosa, M. A. y Solera-Salas, J. (2005). De la administración por objetivos al control estratégico. *Revista Tecnología en Marcha*, 18(1), 57-65, https://revistas.tec.ac.cr/index.php/tec_marcha/article/view/441
- Nava Carbellido, V. M. y Jiménez Valadez, A. R. (2003). *ISO 9000: 2000: estrategias para implantar la norma de calidad para la mejora continua*. Limusa.
- Organización de los Estados Americanos (OEA). (2020). Ley Modelo Interamericana sobre Gestión Documental (LMIGD). https://www.oas.org/es/sla/ddi/docs/acceso_informacion_Propuesta_de_Ley_Modelo_sobre_Gestion_Documental.pdf

BIBLIOGRAFÍA COMPLEMENTARIA

- Kaufmann, A. (1977). Entre iusnaturalismo y positivismo hacia la hermenéutica jurídica. En *Anales de la Cátedra Francisco Suárez*, (17), 351-362.
- Kaufmann, A. y Hassemer, W. (eds.), (1992). *El pensamiento jurídico contemporáneo*. Debate.
- Kaufmann, A. (1994). Jenseits von Naturrecht und Rechtspositivismus. En *Grundprobleme der Rechtsphilosophie*.

CAPÍTULO VIII

La protección de los datos personales de niñez y adolescencia en el mundo digital

Aristides Rodrigo Guerrero García¹

SUMARIO: VIII.1. Niñez e internet: sobreexposición y riesgos; VIII.2. La actividad internacional en torno a la privacidad de la niñez; VIII.3. Estado actual de protección en México; VIII.4. Conclusiones.

PALABRAS clave: Tecnología, derechos, riesgos, seguridad, información, digital.

VIII.1. NIÑEZ E INTERNET: SOBREEXPOSICIÓN Y RIESGOS

En la actualidad, la tecnología digital ha revolucionado la forma de vivir, trabajar, comunicarse e, incluso, aprender. El creciente uso y desarrollo de tecnologías cada vez más elaboradas ha traído consigo un importante avance, pero a la vez, desafíos y riesgos, especialmente para la niñez y adolescencia en la sociedad global interconectada. En este contexto, se manifiesta la impostergable necesidad de abordar y proteger sus derechos, asegurando que las personas menores de edad puedan beneficiarse de las oportunidades que ofrece la era digital de manera segura, ética y equitativa.

En este contexto, y según el Fondo de las Naciones Unidas para la Infancia (UNICEF, por sus siglas en inglés) hasta el 2018, en todo el mundo, 1 de cada 3 personas usuarias de internet era menor de edad y “más de 175,000 niñas y niños se conectaban todos los días por primera vez a internet” (UNICEF, 2018). El acceso a internet resulta entonces para las infancias, un campo de oportunidades, en donde las herramientas tecnológicas permiten el acceso a todo un abanico digital de actividades. (Cervera Navas, 2009, p. 34)²

¹ Ministro de la Suprema Corte de Justicia de la Nación (SCJN). Excomisionado Presidente del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México. Catedrático de la Facultad de Derecho de la Universidad Nacional Autónoma de México (UNAM).

² Internet es utilizado para informarse, comunicarse, buscar contenido educativo e incluso, de ocio digital, todo ello incluye evidentemente nuevos comportamiento y hábitos en los “nativos digitales” que les permiten utilizar de mejor forma las NTICS. Por ello, su inmersión al mundo digital es más profunda, incluso consolida la llamada “generación 2.0”, mientras que, por el contrario, para los inmigrantes

En el caso particular mexicano, y de acuerdo con la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), correspondiente al año 2022, el 63.8% de las niñas y niños en infancia media, es decir, entre 6 y 11 años, contaba con acceso a Internet; de este sector el 50.6% usaba redes sociales; el 45.5% utilizaba plataformas de video; el 49% escuchaba música por Internet; y el 51% jugaba videojuegos en línea. (INEGI e IFT, 2023). Todo ello apunta a que el mundo de la niñez se encuentra cada vez más digitalizado, en donde, desde el aprendizaje hasta la socialización, cuentan con un alto grado de accesibilidad en el entorno digital.

Esta interacción es tan evidente que, incluso, ha sido acuñado el término “nativo digital”, para referirse a:

[...] aquellos niños, adolescentes y jóvenes que nacieron a partir de 1990 en adelante y que poseen una visualización y una capacidad psico-cognitiva diferente, que les permite asimilar con mayor rapidez el uso adecuado y eficaz, aunque no precisamente el óptimo, de las denominadas Nuevas Tecnologías de la Información y Comunicación (NTIC). (IMJUVE, 2017).

Sin embargo, lamentablemente al mismo tiempo, esto también implica una serie de amenazas para su bienestar físico, psicológico y emocional. No es de extrañar, entonces, que Internet se haya consolidado como una herramienta paradójica pues no solo trae oportunidades para las infancias y adolescencias, sino también riesgos importantes en materia de privacidad y protección de datos personales.

En este orden de ideas, y de acuerdo con la Organización para la Cooperación y el Desarrollo Económico (OCDE), los riesgos en línea para las personas menores de edad pueden clasificarse en tres categorías principales: 1. contenido y contacto inapropiado; 2. riesgos relacionados con el consumo y; 3. preocupaciones sobre privacidad y seguridad.

Aunado a esto, el Módulo sobre Ciberacoso (MOCIBA) de 2020, señaló que, en lo que respecta a:

[...] personas de entre 12 a 19 años, el 39.4% recibió mensajes ofensivos, el 26.3% recibió insinuaciones o propuestas sexuales y el 26% críticas por apariencia o clase social, entre otras como publicación de información personal, suplantación de identidad, rastreo de cuentas o sitios web e, incluso, la recepción de contenido sexual. (INEGI, 2020)

digitales, las barreras tecnológicas son evidentemente más pronunciadas. Gran parte de estudios psico-sociales constatan que la niñez ha socializado a través de medios digitales, lo que se traduce tanto en potenciales beneficios como efectos negativos.

Lo anterior, sin dejar de mencionar fenómenos como el *sharenting* implica la sobreexposición de las infancias en redes sociales. Se trata de “[...] un neologismo que reúne en una palabra las ideas de compartir (*share*) y crianza (*parenting*) para describir las prácticas de uso de tales redes, con el fin de acercar a los allegados información sobre [...] menores de edad [...]” (Wierzba, 2023, pp. 130-131). El *oversharing*, es un término acuñado para referirse a la sobreexposición que llevan a cabo padres y madres de sus hijos e hijas, mediante la publicación en redes sociales que realizan aquellos de imágenes o videos de estos últimos. Claros ejemplos de ellos son videos o fotos de festivales escolares, cumpleaños, o de conductas que pueden ser consideradas como simpáticas (Holzer, 2017); y el *morphing*, se refiere a la manipulación digital de imágenes, dotándolas, generalmente, de un carácter sexual o inapropiado; que se han convertido en nuevas amenazas para la privacidad y seguridad de la infancia en línea, y las cuales han generado una conversación importante sobre los riesgos asociados con la vida digital de las y los menores y la necesidad urgente de abordarlos de manera efectiva.

VIII.2. LA ACTIVIDAD INTERNACIONAL EN TORNO A LA PRIVACIDAD DE LA NIÑEZ

La privacidad de la niñez y de la adolescencia se ha convertido en un tema de preocupación a nivel internacional en la era digital. Con el aumento de la conectividad en línea y el uso generalizado de la tecnología por parte de dichas personas, ha surgido la necesidad de abordar los desafíos específicos relacionados con la protección de su privacidad y de sus datos personales en el ámbito global. En respuesta a estas preocupaciones, se ha observado una creciente actividad internacional dirigida a proteger y promover la protección de tales derechos, que abarca desde medidas legislativas hasta colaboraciones entre diferentes países y organizaciones.

Desde 1924, por ejemplo, la Declaración de Ginebra sobre los Derechos del Niño rezaba en su preámbulo “*l’humanité doit donner à l’enfant ce qu’elle a de meilleur* –la humanidad debe dar al niño lo mejor de sí misma–”, incluyendo en su artículo 1o. la obligación de los Estados de establecer condiciones para su normal desarrollo, tanto a nivel material, como espiritual. (DDN, 1924). En 1981, la Convención Americana sobre Derechos Humanos previó que: “Todo niño (*sic*) tiene derecho a las medidas de protección que su condición de menor requiere por parte de su familia, de la sociedad y del Estado” (OEA, 1969, art. 19). No obstante, es necesario señalar que resulta lamentable que, hasta la fecha, en el Sistema Interamericano de Derechos Humanos no exista tratado o convenio específico alguno dirigido a proteger los derechos de las personas menores de 18 años. (González Contró, 2013, p. 646).

La Convención sobre los Derechos del Niño (Conv.DN) de 1989, por su parte, fue firmada y ratificada por México en 1990, de la cual resulta elemental destacar su artículo tercero, que prevé la consideración primordial al interés superior de la

niñez. “En todas las medidas concernientes a los niños que tomen las instituciones públicas o privadas de bienestar social, los tribunales, las autoridades administrativas o los órganos legislativos, una consideración primordial a que se atenderá será el interés superior del niño” (Conv.DN, art. 3.1.). De lo anterior, resulta importante señalar la evidente ausencia de un instrumento internacional vinculante y específico que regule y reconozca expresamente un catálogo de derechos de las personas usuarias de internet, que incluya a las niñas, niños y adolescentes; sin embargo, sí existen ordenamientos de *soft law* que los incluyen, como la *Carta de derechos humanos y principios para internet* o la *Guía de los derechos humanos para los usuarios (sic) de internet*.

La carta provee un importante marco de trabajo con enfoque de derechos humanos en el ambiente *online* para dimensiones de gobernanza de internet local, nacional y global. Lo interesante de este instrumento es que reconoce el mismo catálogo de derechos para personas nativas digitales como para inmigrantes digitales³ entre los que resaltan los siguientes:

[...] la libertad para elegir y utilizar el sistema y software; libertad para protestar en línea; protección de la personalidad virtual; derecho al anonimato y a utilizar cifrado; educación a través y sobre internet; conocimiento libre y dominio público; [además de ello, incluye un décimo segundo apartado denominado] Niños y niñas e internet, [el cual prevé entre otros derechos, los siguientes:] a beneficiarse del internet, al olvido o supresión digital, a la protección contra la explotación y las imágenes de abuso infantil, a ser escuchado y el interés superior del niño. (ONU, 2015, pp. 10-11)

Por otro lado, la Guía es una herramienta orientadora de la práctica y ejercicio de derechos humanos en la red. Es un documento en constante evolución y abierto a actualizaciones. Si bien es cierto que se basa en el Convenio Europeo de Derechos Humanos y del Consejo de Europa, resulta un importante punto de partida por el contenido tan vanguardista y adelantado en materia de derechos digitales y, principalmente, en cuanto a la niñez y a la juventud. Precisamente, incluye un apartado específico sobre este sector, entre los derechos relevantes que prevé son: a la orientación en el uso seguro de internet, al retiro o eliminado de información personal contenida en internet, a contar con información clara sobre comportamientos y contenidos ilegales en internet; e incluso a ejercer recursos efectivos frente a los proveedores de servicios de internet además de las acciones legales previstas por el ordenamiento jurídico (CE, 2014, p. 12).

Asimismo, parte de los esfuerzos internacionales por sumar a los avances en la protección de los derechos digitales de los menores, resulta importante hablar de la labor de la OCDE, a través de la Recomendación de 2012 sobre la Protección de los

³ En contraposición con el término “persona nativa digital”, las “inmigrantes digitales” son aquellas nacidas de manera anterior a 1990, pero que, de manera progresiva, han ido adaptándose al uso de las NTIC.

Niños en Línea. La cual, basa su análisis en tres principios clave: el empoderamiento, la proporcionalidad y la adaptabilidad de las medidas para la efectividad de la protección de los derechos de la niñez en los entornos digitales. La OCDE ha destacado la importancia de crear un entorno en línea seguro, especialmente para las y los menores y otros grupos vulnerables. Esto requiere un enfoque coordinado que involucre tanto a actores públicos como privados, así como una cooperación internacional efectiva (OCDE, 2011, pp. 3-5).

Otro de los desarrollos más significativos en este campo es la promulgación de leyes y regulaciones específicas destinadas a proteger la privacidad de los niños en línea. Ejemplos destacados incluyen al Reglamento General de Protección de Datos (GDPR) de la Unión Europea, que establece requisitos estrictos para el procesamiento de datos personales de menores, y la Ley de Protección de la Privacidad en Línea de los Niños (COPPA) en los Estados Unidos, que regula la recopilación de información en línea de niñas y niños menores de 13 años. Estas leyes buscan garantizar que sus datos personales sean tratados con el máximo cuidado y que se obtenga el consentimiento adecuado de madres y padres antes de recopilar información sobre sus hijos e hijas.

Además de tales medidas, se han establecido varias organizaciones internacionales y coaliciones enfocadas en proteger los derechos de la niñez en línea. Por ejemplo, la Red Global de Internet Segura para Niños (INHOPE) trabaja para eliminar el contenido ilegal en línea que pueda dañarles, mientras que la UNICEF aboga por políticas y prácticas que protejan sus derechos en el ciberespacio. Estas organizaciones desempeñan un papel crucial al coordinar esfuerzos a nivel internacional y proporcionar recursos y orientación a los gobiernos y otras partes interesadas sobre cómo abordar los desafíos relacionados con la privacidad de la niñez.

La cooperación internacional también juega un papel clave en la protección de la privacidad de la niñez y adolescencia en línea. Los gobiernos y las organizaciones trabajan juntos para intercambiar información, compartir mejores prácticas y coordinar esfuerzos en la lucha contra la explotación infantil en línea y otras formas de abuso. Los acuerdos internacionales, como la Convención de las Naciones Unidas sobre los Derechos del Niño (*sic*), proporcionan un marco legal y normativo para proteger los derechos de las niñas y niños en todos los aspectos de sus vidas, incluida su privacidad en línea.

Sin embargo, a pesar de estos esfuerzos, persisten desafíos significativos en la protección de la privacidad de la niñez a nivel internacional. La naturaleza transfronteriza de Internet plantea dificultades en la aplicación y cumplimiento de las leyes y regulaciones relacionadas con la privacidad de las infancias y adolescencias, ya que la jurisdicción y las leyes varían de un país a otro. Además, el rápido avance de la tecnología presenta nuevos desafíos, como el aumento de la recopilación de datos a través de dispositivos conectados, que requieren respuestas adaptables y ágiles por parte de los reguladores y las organizaciones de protección de la infancia.

La actividad internacional en torno a la privacidad de la niñez refleja la creciente conciencia sobre la importancia de proteger los derechos de la niñez en el ciberespacio. A través de la promulgación de leyes y regulaciones, el establecimiento de organizaciones internacionales y la cooperación entre países, se están dando pasos importantes para abordar los desafíos relacionados con la privacidad de las y los menores en línea. Sin embargo, se necesitan esfuerzos continuos y colaborativos para adaptarse a los cambios tecnológicos y garantizar que puedan disfrutar de un entorno en línea seguro y protegido en todo el mundo.

VIII.3. ESTADO ACTUAL DE PROTECCIÓN EN MÉXICO

Nuestro país cuenta con una robusta legislación en materia de protección de la niñez y adolescencia. A nivel constitucional, por ejemplo, el artículo 4o., párrafo noveno, señala que las y los niños cuentan con los derechos a “la satisfacción de sus necesidades alimentarias, a la salud, a la educación y al sano esparcimiento para su desarrollo integral”.

Asimismo, se establece que, en todas las decisiones y actuaciones del Estado, deberá velarse y cumplirse el principio de interés superior de la niñez, el cual deberá guiar tanto el diseño y ejecución, como el seguimiento y evaluación de políticas públicas enfocadas a este sector poblacional. Cabe señalar que, de conformidad con la sentencia recaída al Amparo en Revisión 203/2016, “el interés superior de la niñez es un concepto triple [es decir] un derecho sustantivo [en sí mismo]; un principio jurídico de interpretación fundamental y una norma de procedimiento” (SCJN, 2016, p. 43).

A nivel legal, se cuenta con la Ley General de Derechos de Niñas, Niños y Adolescentes (LGDNNA) que, además de retomar el citado principio, reconoce que la niñez y adolescencia son titulares de derechos, entre los que se encuentran los de prioridad, identidad, al desarrollo, a la no discriminación, a una vida libre de violencia y a la integridad personal, al descanso y esparcimiento, a la libertad de expresión y acceso a la información, a la intimidad y al acceso a las NTIC.

Estos últimos, regulados tanto en el Capítulo Décimo Séptimo como Vigésimo, respectivamente, resultan de necesaria atención para el presente ensayo, pues en ellos converge, precisamente, el objeto de estudio de este.

Dentro del primero de ellos se garantiza el “derecho a la intimidad personal y familiar, [así como] a la protección de datos personales” y prohíbe, entre otros aspectos, la difusión o divulgación ilícita de información personal que atente contra su honra, reputación e, incluso, su propia imagen (LGDNNA, art. 76). Además, señala que por

[...] violación a la intimidad de niñas, niños y adolescentes [se entenderá] cualquier manejo directo de su imagen, nombre, datos personales o referencias que permitan su identificación [...], que menoscabe su honra o reputación, sea contrario a sus derechos o que los ponga en riesgo, conforme al principio de interés superior de la niñez. (LGDNNA, art. 77)

Finalmente, por cuanto hace a este derecho, se precisa que “cualquier medio de comunicación que [pretenda] difundir entrevistas realizadas a la niñez o adolescencia, deberá recabar el consentimiento[...] de quienes ejerzan la patria potestad, así como la propia opinión de la persona entrevistada [...]”, y que quien entrevista se guíe por el principio de respeto, en virtud del cual “no podrá mostrar actitudes ni emitir comentarios que afecten o impidan objetivamente el desarrollo integral de niñas, niños y adolescentes”. (LGDNNA, art. 78)

Respecto del derecho al acceso a las NTIC, se señala, entre otros aspectos, que las “[n]iñas, niños y adolescentes tienen derecho de acceso y uso seguro a internet [entendido] como [un] medio efectivo para ejercer [diversos] derechos [entre los que se encuentran los de] comunicación, educación, salud, esparcimiento, no discriminación [y] acceso a la información. (LGDNNA, 101 Bis 2).

Además de ello, resulta necesario señalar que el 9 de octubre de 2023, el Consejo Nacional del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales aprobó la *Carta de Derechos de la Persona en el Entorno Digital. Código de Buenas Prácticas*, que, si bien no se trata de un cuerpo normativo, sí funge como una guía orientadora para la protección de derechos humanos en el mundo digital. En este sentido, dicha *Carta* señala, entre otros aspectos, que:

2.2. Los derechos de las niñas, niños y adolescentes deberán ser asegurados de manera prioritaria, especialmente cuando se trate de aquellos relativos a su protección y auxilio en cualquier circunstancia [...] 2.4. Todas las autoridades deberán garantizar un enfoque integral, transversal y con perspectiva de derechos humanos en el diseño e instrumentación de políticas y programas de gobierno, enfocados en el [goce] de derechos [...] en entornos digitales. (INAI, 2021, p. 52)

Otro ámbito a través del cual se ha buscado proteger los derechos de la niñez y adolescencia es mediante la actividad jurisdiccional, en donde, a golpe de sentencia, se han establecido diversos criterios para garantizarlos.

Un ejemplo de ello es la sentencia recaída al Procedimiento Especial Sancionador TECDMX-PES-178/2018 emitida por el Tribunal Electoral de la Ciudad de México. En dicho procedimiento fue denunciada la conducta de una candidata a alcaldesa que, a través de la red social *X (Twitter)*, publicó diversas imágenes en las que se apreciaban cinco personas menores de edad. Dicho órgano jurisdiccional consideró que la protección del interés superior de la niñez debe estar garantizado.

[...] en todos aquellos casos en que en la propaganda política o electoral se use la imagen, nombre o datos que permitan hacer identificable a un menor como recurso propagandístico. [Además de ello, consideró que] una vulneración a la intimidad de [las y] los menores [puede materializarse a través de] cualquier tipo de manejo directo de su imagen, nombre, datos personales o referencias que permitan su identificación en los medios de comunicación –incluidas las redes sociales–, ya sea porque se menoscabe su honra o reputación, se contravengan sus derechos o los ponga en riesgo. (TECDMX, 2018, pp. 37-38)

En el análisis de fondo, se llevó a cabo el estudio de los “Lineamientos para la Protección de Niñas, Niños y Adolescentes en Materia de Propaganda y Mensajes Electorales”, emitidos por el Consejo General del Instituto Nacional Electoral, y se concluyó que, para el caso de que niñas, niños o adolescentes aparecieran en propaganda política o electoral, así como en mensajes de autoridades electorales, resultaba indispensable contar con el consentimiento del padre, madre o quien ejerciera la patria potestad, plasmado de manera escrita, informada e individual. Con base en lo anterior, el órgano jurisdiccional consideró la existencia de la infracción, toda vez que fueron advertidas diversas irregularidades, como la falta de concordancia entre el nombre de una madre, tanto en el acta de nacimiento como en la credencial para votar, y condenó a la denunciada al pago de una multa equivalente a \$3,062.80, así como una amonestación pública a los partidos políticos postulantes (TECDMX, 2018).

Otro ejemplo de actividad jurisdiccional se ubica en la jurisprudencia 20/2019, emitida por el Tribunal Electoral del Poder Judicial de la Federación, la cual, en esencia señala que “cuando [...] aparezcan [personas] menores de edad en propaganda política o electoral, deberá recabarse el referido consentimiento [o, en su caso], difuminar, ocultar o hacer irreconocible la imagen, voz o cualquier otro dato que les identifique” (TEPJF, 20/2019).

Además de ello, en el Procedimiento Especial Sancionador SRE-PSD-43/2021, la Sala Regional Especializada del TEPJF estimó que los sujetos obligados debían ajustar sus actos de propaganda, incluidos aquellos efectuados a través de redes sociales, cuando en ellos aparecieran niñas, niños o adolescentes, precisando que no bastaba el citado consentimiento, sino que, en adición, era indispensable contar con una “anotación” del padre o madre en la que constara que conocía el propósito, características, riesgos, alcances, plazos, formas de transmisión, medios de difusión y contenido de dicho material, así como la proyección de un video hacia la persona menor de edad en la que se le explicara las implicaciones de su participación (TEPJF, 2021, pp. 8-9).

Finalmente, el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, en su carácter de órgano garante cuasijurisdiccional, ha implementado también diversas acciones a favor de una cultura de la protección de datos personales en internet. Ejemplo de ello ha sido “Monstruos en Red”, un programa que, en apego a los principios

de la COPPA, tiene por objetivo concientizar a la niñez respecto del uso de las NTIC, con especial énfasis en la necesidad de aprender sobre la privacidad y la protección de datos personales.

Asimismo, y en el marco del evento “La protección de datos personales en la niñez”, se organizó la obra infantil “Caperucita Roja Digital”, como un ejercicio enfocado en mostrar la necesidad e importancia de mantener la privacidad segura en internet, a efecto de evitar conductas penadas, tales como el robo de identidad o la violencia digital. Por último, y en el marco del Pleno Infantil del año 2023, las y los comisionados infantiles firmaron los “5 Compromisos por la Privacidad de la Niñez en la CDMX”, siendo estos los siguientes:

- Aprende a no compartir información personal en Internet, como tu nombre, dirección o número de teléfono;
- Recuerda ajustar la configuración de privacidad de tus redes sociales;
- Conoce las políticas de privacidad de los sitios web y aplicaciones que utilizas;
- Optimiza y actualiza tus equipos en los cuales navegas en internet; y
- Procura almacenar tu información personal en un lugar seguro.

VIII.4. CONCLUSIONES

La combinación de un alto porcentaje de niñas, niños y adolescentes que usan internet y un elevado promedio de horas navegando, sugiere la necesidad urgente de implementar medidas para proteger y educar a la juventud mexicana sobre el uso seguro y responsable de la tecnología digital.

La protección de los derechos de la niñez en la era digital actual es crucial para garantizar un desarrollo saludable y una participación segura y significativa en la sociedad. Esto implica proporcionar un acceso equitativo a la tecnología, proteger la seguridad y el bienestar de las y los niños en línea, promover la alfabetización digital desde una edad temprana y respetar su privacidad y autonomía en el mundo digital. Además, es fundamental abordar los riesgos asociados con la sobreexposición en el ciberespacio, como el *sharenting*, el *oversharing* y el *morphing*, y promover prácticas de uso responsable de las redes sociales por parte de madres, padres y personas cuidadoras.

A nivel internacional se están realizando importantes esfuerzos para proteger la privacidad de la niñez, a través de leyes y regulaciones específicas, la creación de organizaciones internacionales y la cooperación entre países. Sin embargo, persisten desafíos significativos, como la aplicación de regulaciones en un entorno transfronterizo y la adaptación a los avances tecnológicos.

México no se ha quedado atrás: desde tres perspectivas –normativa, jurisdiccional y cuasijurisdiccional– se ha ido consolidando un amplio marco jurídico que busca garantizar los derechos a la privacidad y a la protección de datos personales de las

infancias y juventudes, lo que, a su vez, permite proteger otros derechos humanos, como a la imagen o a la honra, y combatir la comisión de conductas delictivas, como el robo de identidad, la alteración digital de imágenes o el ciberacoso.

Si bien resulta imperativo abordar estos desafíos de manera efectiva y coordinada, es necesario señalar, también, que las NTIC no representan inherentemente un riesgo, sino que el peligro radica en cómo se emplean. Puede haber abuso por parte de individuos que cometen delitos en línea, así como por aquellos que no toman medidas para salvaguardar su privacidad, proteger sus datos personales y garantizar su seguridad digital. Es crucial reconocer que la innovación tecnológica, con internet como paradigma, debe estar al servicio de las personas, respetando sus derechos humanos y libertades fundamentales.

En última instancia, proteger los derechos digitales de la niñez y adolescencia requiere un esfuerzo conjunto y continuo de gobiernos, empresas, instituciones educativas y la sociedad en su conjunto para garantizar un entorno digital seguro y enriquecedor para niñas, niños y adolescentes.

REFERENCIAS

- Cervera Navas, L. (2009). *Lo que hacen tus hijos en internet*, Integral.
- Comité de los Derechos del Niño (CDN). (20 de noviembre, 1989). Convención sobre los Derechos del Niño (Conv.DN). <https://www.ohchr.org/es/instruments-mechanisms/instruments/convention-rights-child>
- Consejo de Europa (CE). (16 de abril de 2014). CM/Rec(2014) 6. *Guía de los derechos humanos para los usuarios de internet*, <https://rm.coe.int/16804c177e>
- Constitución Política de los Estados Unidos Mexicanos (CPEUM). (5 de febrero de 1917, última reforma: 15 de octubre de 2025). <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>
- Declaración de los Derechos del Niño (DDN). (1924). <https://www.ciprodeni.org/wp-content/uploads/2018/08/Declaracion-de-Ginebra-1924.pdf>
- Fondo de las Naciones Unidas para la Infancia (UNICEF). (6 de febrero, 2018). Los más de 175.000 niños que se conectan en línea por primera vez todos los días disfrutan de grandes oportunidades, pero confrontan también graves riesgos. <https://www.unicef.org/es/comunicados-prensa/los-m%C3%AAs-de-175000-ni%C3%B1os-que-se-conectan-en-l%C3%ADnea-por-primera-vez-todos-los-d%C3%ADas>
- González Contró, M. (2013). Derechos de niñas, niños y adolescentes. En E. Ferrer Mac-Gregor Poisot, J. L. Caballero Ochoa y Ch. Steiner (Coords.). *Derechos humanos en la Constitución. Comentarios de jurisprudencia constitucional e interamericana I* (pp. 639-666), Suprema Corte de Justicia de la Nación; Universidad Nacional Autónoma

- de México, Instituto de Investigaciones Jurídicas; Fundación Konrad Adenauer. <https://www.scjn.gob.mx/sites/default/files/pagina/documentos/2016-11/Dh%20en%20la%20Constitucion%20comentarios%20TOMO%201.pdf>
- Holzer, N. (2017). Oversharing. Padres que comparten en exceso en redes sociales. Dimensiones éticas y antropológicas de la cuestión, *Palabras*, año1(1), 92-106. <https://repositorio.uca.edu.ar/handle/123456789/7476>
- Instituto Mexicano de la Juventud (IMJUVE). (01 de septiembre de 2017). ¿Conoces a las y los nativos digitales? <https://www.gob.mx/imjuve/articulos/conoces-a-las-y-los-nativos-digitales>
- Instituto Nacional de Estadística y Geografía (INEGI). (2020). Modulo sobre Ciberacoso (MOCIBA) 2021. [https://www.inegi.org.mx/programas/mociba/2020/#:~:text=El%20M%C3%B3dulo%20sobre%20Ciberacoso%20\(MOCIBA,12%20meses%2C%20as%C3%AD%20como%20la.](https://www.inegi.org.mx/programas/mociba/2020/#:~:text=El%20M%C3%B3dulo%20sobre%20Ciberacoso%20(MOCIBA,12%20meses%2C%20as%C3%AD%20como%20la.)
- INEGI e Instituto Federal de Telecomunicaciones (IFT). (2023). Encuesta nacional sobre disponibilidad y uso de tecnologías de la información en los hogares (ENDUTIH) 2022. Comunicado de prensa núm. 367/23. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/ENDUTIH/ENDUTIH_22.pdf
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (s.f.). *Carta de Derechos de la Persona en el entorno digital. Código de buenas prácticas*. INAI. https://www.idaip.org.mx/archivos/transparencia/ruoch/BIBLIOTECA%20DIGITAL/Carta_DDigitales.pdf
- Ley General de Derechos de Niñas, Niños y Adolescentes (LGDNNA). (publicada: 4 de diciembre de 2014). <https://www.diputados.gob.mx/LeyesBiblio/ref/lgdnnna.htm>
- Organización de Naciones Unidas (ONU), Foro para la Gobernanza de Internet (2015). *Carta de derechos humanos y principios para internet*. <https://www.palermo.edu/cele/pdf/Carta-de-Derechos-Humanos-y-Principios-para-Internet-en-Espanol.pdf>
- Organización de Estados Americanos (OEA). (1969). Convención Americana sobre Derechos Humanos. (Promulgación y publicación *Diario Oficial de la Federación*: 7 de mayo de 1981) https://www.oas.org/dil/esp/1969_Convenci%C3%B3n_Americana_sobre_Derechos_Humanos.pdf.
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2011). The protection of children online. Risks faced by children online and policies to protect them. *OECD Digital Economy Papers*. (179). https://www.oecd.org/content/dam/oecd/en/publications/reports/2011/05/the-protection-of-children-online_g17a1f9f/5kgcjf71pl28-en.pdf
- Suprema Corte de Justicia de la Nación (SCJN). (9 de noviembre de 2016). Amparo en Revisión 203/2016. https://www2.scjn.gob.mx/juridica/engroses/2/2016/2/2_194858_3129_firmado.pdf

- Tribunal Electoral de la Ciudad de México (TECDMX). (18 de octubre de 2018). TECDMX-PES-178/2018. Sentencia. http://transparencia.tecdmx.org.mx/sites/default/files/archivos/art128/20/sentencias/2018/4to_trimestre/SENTENCIA-TECDMX-PES-178-2018.pdf
- Tribunal Electoral del Poder Judicial de la Federación (TEPJF). Jurisprudencia 20/2019, Sexta Época, *Gaceta de Jurisprudencia y Tesis en Materia Electoral*, Año 12, Núm. 24, 2019, pp. 30 y 31. <https://www.te.gob.mx/ius2021/#/>
- TEPJF. (17 de junio de 2021). SRE-PSD-43/2021. Sentencia. <https://www.te.gob.mx/media/SentenciasN/pdf/especializada/SRE-PSD-0043-2021.pdf>
- Wierzba, S. M. (Mayo 2023). La sobreexposición de jóvenes en redes sociales como riesgo inevitable, *Derecho, Universidad y Justicia. Nuevas tecnologías e innovación en el campo jurídico*, 2(3), 130-141. SAIJ - La sobreexposición de jóvenes en redes sociales como riesgo evitable

CAPÍTULO IX

INFO CDMX: vanguardia en la protección de datos personales

Laura Lizette Enríquez Rodríguez¹

SUMARIO: IX.1. Introducción; IX.2. Actividad cuasijurisdiccional; IX.3. Vigilancia del cumplimiento de principios y disposiciones en materia de protección de datos personales; IX.4. Otras acciones; IX.5. Conclusiones.

PALABRAS clave: Acceso a la información, protección de datos personales, INFO CDMX, recurso de revisión, denuncia, vigilancia, obligaciones, verificaciones, socialización, difusión.

IX.1. INTRODUCCIÓN

El Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX) tiene encomendada la garantía de dos derechos fundamentales en este siglo XXI: el derecho de acceso a la información pública y el derecho a la protección de datos personales (CPCDMX, 2017, art. 49).

A 19 años de su creación, la labor del INFO CDMX ha estado marcada por un contexto de creciente evolución e intensificación, especialmente en los últimos años, del uso e implementación de nuevas tecnologías y herramientas digitales. Proceso que ha traído consigo, entre otras cosas, el cada vez mayor uso e intercambio de datos e información personal para el acceso a bienes y servicios.

Lo que, a su vez, se ha reflejado también en un crecimiento en la preocupación de la sociedad capitalina por el cuidado de su información personal, así como en la consolidación del derecho a la protección de datos personales y los mecanismos para su ejercicio.

¹ Comisionada Presidenta del INFO CDMX.

Para muestra de ello, el registro de solicitudes de ejercicio de derechos de acceso, rectificación, cancelación y oposición a datos personales da cuenta de un crecimiento importante a lo largo de los años que pone en relieve la consolidación del ejercicio de estos derechos en la capital del país: desde 2004 al 20 de junio de 2025, se han presentado 130,752 solicitudes en materia de datos personales (INFO CDMX, 2025a, p. 2).

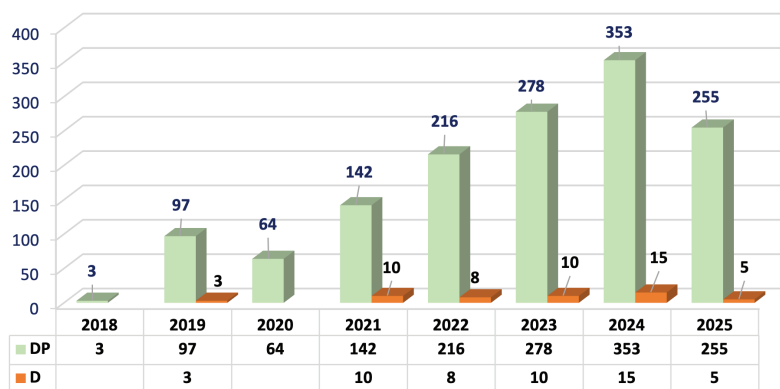
En este escenario, el INFO CDMX se ha visto obligado a redoblar esfuerzos para fortalecer la garantía de este derecho a través de su quehacer institucional. Para el propósito del presente artículo se presentarán dichas acciones a partir de tres vertientes: la actividad cuasijurisdiccional, a través de la resolución de recursos de revisión y denuncias en materia de datos personales; la vigilancia del cumplimiento de diversas obligaciones en materia de datos personales respecto de los sujetos obligados de la capital; así como otras acciones, entre las que destacan la realización de actividades que promueven la socialización, difusión y conocimiento del derecho a la protección de datos personales, así como sus prerrogativas.

IX.2. ACTIVIDAD CUASIJURISDICCIONAL

El pleno del INFO CDMX tiene entre sus atribuciones la resolución de recursos de revisión en materia de acceso a la información y protección de datos personales, así como de denuncias en dichas materias. Estos recursos de revisión, así como las denuncias, representan mecanismos legales para salvaguardar los derechos de la sociedad respecto del tratamiento de sus datos personales por parte de los entes públicos de la capital. Respecto de los recursos de revisión en materia de datos personales aprobados por el pleno del Instituto, se ha registrado una evolución creciente: pasando de aprobar 3 recursos en la materia en 2018; 97 en 2019; 64 en 2020; 142 en 2021; 216 en 2022; 278 en 2023; 353 en 2024, y 255 al 9 de julio de 2025.

Por otro lado, respecto de las denuncias en materia de datos personales, el pleno del Instituto resolvió 3 en 2019; 10 en 2021; 8 en 2022; 10 en 2023; 15 en 2024, y 5 en lo que va del ejercicio 2025.

Recursos y denuncias aprobadas por el Pleno del INFO CDMX en materia de datos personales



Fuente: (Secretaría Técnica del INFO CDMX).

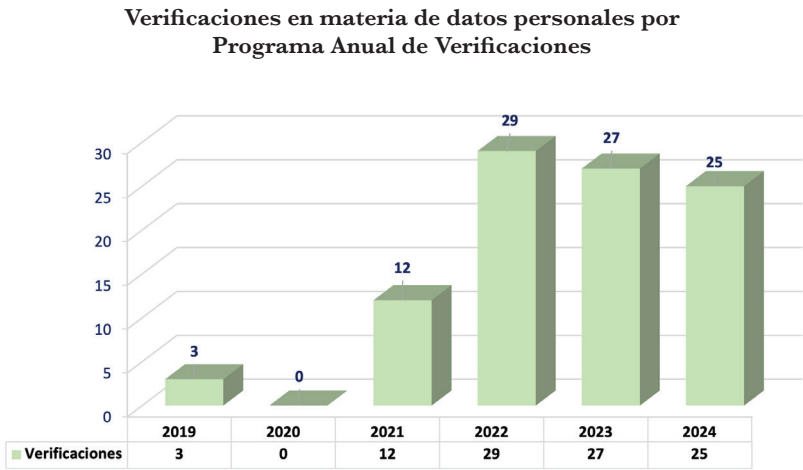
La función cuasijurisdiccional del pleno del INFO CDMX constituye un pilar esencial para la defensa del derecho a la protección de datos personales en la Ciudad de México. A través de la resolución de recursos de revisión y denuncias, el Instituto no solo corrige actos u omisiones de los entes públicos, sino que fortalece el ejercicio efectivo de estos derechos por parte de la sociedad.

El crecimiento sostenido en el número de resoluciones en materia de datos personales refleja tanto una mayor conciencia social sobre la relevancia de este derecho, como la consolidación del propio Instituto como garante de su tutela. No obstante, estas cifras también evidencian la necesidad de seguir impulsando acciones de difusión, capacitación y acompañamiento para que más personas conozcan y ejerzan sus derechos, cerrando así brechas de información y acceso que aún persisten.

IX.3. VIGILANCIA DEL CUMPLIMIENTO DE PRINCIPIOS Y DISPOSICIONES EN MATERIA DE PROTECCIÓN DE DATOS PERSONALES

La Ley de Datos local establece que, entre las atribuciones del INFO CDMX, se encuentra el “vigilar y verificar el cumplimiento de los principios y disposiciones contenidos en dicha Ley y los ordenamientos que deriven de ésta” (LPDPPSOCDMX, art. 111). En ese sentido, desde 2019 el Instituto lleva a cabo verificaciones en materia de datos personales a los sujetos obligados de la capital.

Dichas verificaciones han registrado un crecimiento importante a lo largo de los años: de verificar tres sujetos obligados en 2019, se llegó a un pico máximo en 2022, con 29 sujetos obligados; 27 en 2023 y 25 en 2024. Revisando un total de 1,625 sistemas de datos personales a lo largo de estos años, lo que representa el 65.52% de sistemas en la capital del país y el 82.34% de sujetos obligados. El Programa Anual de Verificaciones 2025, contempla la verificación de 20 sujetos obligados más que, de concluirse de manera satisfactoria, representaría la verificación en materia de datos personales del 100% de los sujetos públicos de la capital.



Fuente: (Dirección de Datos Personales del INFO CDMX).

Derivado de la pandemia por Covid-19, el Instituto se vio en la necesidad de explorar nuevas rutas o mecanismos para continuar realizando las tareas encomendadas por la normativa. Concretamente, en materia de verificaciones a los sujetos obligados, desde el Instituto se desarrolló un *software* para verificar y auditar: el SIVER, que sistematiza cada uno de los roles, etapas y funciones de las verificaciones y auditorías establecidas en la normativa local.

A partir de su implementación en 2022, a través del SIVER se han obtenido beneficios, como la disminución del gasto de recursos económicos, debido a que ya no se imprimen los expedientes de las verificaciones, lo que, a su vez, contribuye al cuidado del medio ambiente; los traslados a las oficinas de los sujetos obligados se redujeron en un 95%; el tiempo de las verificaciones se redujo en un 60%; además de obtenerse resultados más precisos sobre los niveles de cumplimiento por sujeto obligado. Además,

al ser desarrollado en código abierto, este *software* ha sido compartido con organismos garantes de 10 entidades de la República a través de convenios de colaboración, fortaleciendo el federalismo cooperativo.

Por el desarrollo de dicho *software*, el Instituto recibió el Primer Lugar para el Sector Público del Premio de Innovación y Buenas Prácticas para la Protección de Datos Personales 2023, organizado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI, 2024).

Por otro lado, la normativa local establece que en la Ciudad de México se debe contar con un Registro Electrónico de Datos Personales, (LPDPPSOCDMX, 2018, arts. 36 y 37) en el cual los sujetos obligados deberán inscribir los sistemas de datos personales bajo su custodia y protección.

En mérito de lo anterior, el primer Registro Electrónico fue aprobado por el Instituto en 2010. Dos años después, se aprobó la versión 2.0; en 2019, se aprobó la versión 2.5 para apegarse a lo establecido en la Ley de Datos local; y, recientemente, se aprobó la versión RESDP 3.0 (INFO CDMX, 2024a) con importantes ajustes y mejoras en este Registro.

Al contar con una versión de consulta pública —única en su tipo a nivel nacional— accesible a cualquier persona interesada, se puede conocer qué sistemas tiene cada sujeto obligado, cuál es su nivel de seguridad, así como mayores detalles sobre el sistema, los responsables de este, los usuarios y encargados, entre otros elementos.

Además, y derivado de la entrada en vigor de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (LPDPPSOCDMX) en 2018, desde el Instituto se han elaborado, emitido, revisado y mejorado algunos documentos como los *Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados*, los *Lineamientos para la realización de Verificaciones y Auditorías*, la *Guía para la Realización de Verificaciones y Auditorías*, la *Guía para la Elaboración del Documento de Seguridad*, entre otros instrumentos normativos.

La vigilancia del cumplimiento de los principios y disposiciones en materia de protección de datos personales constituye una función estratégica del INFO CDMX para garantizar que los sujetos obligados actúen conforme al marco legal y resguarden adecuadamente la información personal bajo su custodia. A través de las verificaciones y la implementación de herramientas como el SIVER, el Instituto ha logrado profesionalizar, sistematizar y hacer más eficientes los procesos de supervisión, contribuyendo no solo a fortalecer la cultura de la protección de datos en la capital, sino también a generar modelos replicables a nivel nacional.

Estas acciones reflejan un compromiso institucional con la mejora continua, la innovación y la transparencia, al tiempo que permiten detectar áreas de oportunidad y promover buenas prácticas entre los entes públicos. La existencia de un RESDP público y actualizado también es muestra del esfuerzo por ofrecer certeza y confianza a la sociedad sobre el tratamiento de sus datos personales, reforzando así la rendición de cuentas y la tutela efectiva de este derecho en la Ciudad de México.

IX.4. OTRAS ACCIONES

Finalmente, el tercer elemento en el que quisiera detenerme se refiere a la socialización y difusión del derecho a la protección de datos personales, tanto para las personas servidoras públicas responsables del tratamiento de datos de los sujetos obligados de la capital, como respecto de la sociedad en general.

En el marco de las tareas para el fortalecimiento del derecho a la protección de datos personales, destaca la consolidación de la Red de Protección de Datos Personales de la Ciudad de México (INFO CDMX, 2024b), una instancia de interrelación y comunicación continua con los sujetos obligados, cuyo propósito es crear vínculos, estrategias y acciones, tendientes a fortalecer el cumplimiento con las bases, principios y procedimientos para garantizar el derecho a la protección de datos personales.

De este espacio han surgido distintos proyectos como la “Jornada de Seminarios Especializados en materia de Protección de Datos Personales en la Ciudad de México”, de la cual, de 2021 a 2025, se han organizado cinco ediciones, en las que se desarrollaron un total de 16 sesiones de seminarios especializados y 18 talleres prácticos. Lo que representó la participación de más de 10,000 personas asistentes, con el objetivo de proporcionarles conocimientos básicos y herramientas respecto a diversas temáticas de utilidad en materia de protección de datos personales.

En estos años, también se han consolidado acciones para la difusión y socialización de este derecho, con eventos de carácter internacional, como las conmemoraciones del “Día Internacional de la Protección de Datos Personales”, que se realizan desde 2011; u otras acciones como la “Feria de la Transparencia y la Protección de Datos Personales” realizada en lugares emblemáticos como el Paseo de la Reforma y el Zócalo Capitalino.

En materia de promoción y difusión de la cultura de la protección de datos personales, se han realizado diversos talleres, destacando: Taller Nacional: Ley Olimpia; Taller Virtual Derechos y Riesgos Digitales; Taller Mujeres por la TRANSPARENCIA y la Protección de Datos Personales; Taller virtual para la protección de los datos personales de la comunidad LGBTTTIQ+; entre otros.

Con el objetivo de promover el derecho a la protección de datos personales en las infancias y juventudes de la capital, también se ha llevado a cabo el “Concurso Comisionada y Comisionado Infantil para formar parte del Pleno Niñas y Niños”, ediciones 2022, 2023 y 2024, y los concursos de redes sociales *Tik Tok* e *Instagram*, “60 segundos para informarme” y “La transparencia, derecho llave para el ejercicio de otros derechos”. Asimismo, en 2025, se realizó el “Concurso de Dibujo Infantil Ilustrando la Transparencia y la Privacidad”, así como el “Concurso de Historieta Juvenil Protegiendo Nuestra Identidad Digital”. Estas acciones han contribuido a impulsar desde edades tempranas el ejercicio activo de los derechos digitales y el desarrollo de una ciudadanía informada y crítica. Además, se han visitado 96 escuelas primarias

y secundarias y atendido aproximadamente a 438 grupos escolares. En total, se ha beneficiado directamente a alrededor de 12,303 niñas, niños y adolescentes, en temas fundamentales para el ejercicio de sus derechos en la era digital.

El INFO CDMX ha sido también un actor clave en la construcción de publicaciones como la *Carta de Derechos de la Persona en el Entorno Digital* (INAI, 2021), un código de buenas prácticas que aborda los principales derechos de la era digital. También destaca la publicación titulada *Revoluciones: protección de datos personales y privacidad en la era digital. Orígenes, avances, tensiones y desafíos. Una mirada desde el periodismo gráfico* (Enríquez Rodríguez, 2023), en la cual, a través de la caricatura política como ensayo gráfico y acompañada de diversas reflexiones por parte de especialistas en la materia, se reflexiona sobre los retos de la protección de datos personales en México.

Otra de las publicaciones editoriales impulsadas por el INFO CDMX es la obra *Desafíos del derecho a la protección de datos personales en la era digital: una mirada desde América Latina* (Mendoza Enríquez y Enríquez Rodríguez, 2024) que reúne diversos ensayos escritos por mujeres especialistas de la región. A través de sus aportaciones, se exploran los retos actuales que enfrentan los sistemas de protección de datos personales en un entorno digital cada vez más complejo, marcado por profundas transformaciones tecnológicas y sociales.

De 2012 a 2016 también se implementó un programa para reconocer las mejores prácticas e innovaciones en materia de datos por parte de los entes públicos que sobresalieran en el cumplimiento de la normativa y que realizaran acciones innovadoras en la materia.

En el escenario internacional, el INFO CDMX ha formado parte de dos de los foros más importantes en materia de protección de datos personales: la Red Iberoamericana de Protección de Datos Personales (RIPDP, 2024) y la Asamblea Global de la Privacidad (GPA, 2024).

La socialización y difusión del derecho a la protección de datos personales constituyen un componente fundamental para lograr su efectivo reconocimiento y ejercicio por parte de la sociedad. Las acciones impulsadas por el INFO CDMX en esta materia no solo fortalecen las capacidades institucionales de quienes integran los sujetos obligados, sino que también contribuyen a construir una cultura pública más consciente y participativa respecto a los riesgos y oportunidades que plantea la era digital.

Iniciativas como la Red de Protección de Datos Personales, los talleres especializados, las ferias, los concursos dirigidos a niñas, niños y adolescentes, así como las publicaciones de alcance nacional e internacional, son ejemplos claros del compromiso institucional por acercar este derecho a todos los sectores de la sociedad. Estas actividades no solo refuerzan la labor preventiva del Instituto, sino que abonan a un cambio cultural más profundo, donde la protección de los datos personales sea entendida como un componente esencial para el ejercicio pleno de otros derechos y para la consolidación de una ciudadanía digital informada y responsable.

IX.5. CONCLUSIONES

Es indudable que los últimos años han estado marcados por los intensos cambios y desarrollos tecnológicos en México y en el mundo, posicionando a los datos personales como un elemento indispensable para el acceso a múltiples bienes y servicios.

En este escenario, el INFO CDMX ha consolidado un modelo institucional que trasciende la mera aplicación de la normativa en materia de protección de datos personales para situarse como un referente en innovación, buenas prácticas y construcción de ciudadanía en este ámbito. Su experiencia demuestra que la protección de datos personales no puede entenderse únicamente como una cuestión técnica o legal, sino como una responsabilidad pública que implica acompañar a las personas en el ejercicio de sus derechos, generar confianza social e impulsar cambios culturales sostenidos.

El desarrollo de herramientas tecnológicas propias, la modernización de registros públicos y la implementación de metodologías innovadoras han permitido al Instituto no solo fortalecer su capacidad de supervisión y vigilancia, sino también proyectar sus avances hacia otras entidades del país, abonando a la consolidación de un federalismo cooperativo en materia de transparencia y privacidad.

A ello se suma una labor constante de socialización y sensibilización, que ha permeado en distintos sectores de la población –incluidas niñas, niños, adolescentes y grupos históricamente vulnerados–, acercando el derecho a la protección de datos personales a la vida cotidiana y fomentando su ejercicio informado.

Por otra parte, la participación activa del Instituto en foros internacionales y su aportación en publicaciones especializadas lo colocan como un actor protagónico en la discusión global sobre los retos que impone la era digital. Esta vocación refuerza la importancia de construir una visión local con impacto regional y global, en la que la protección de datos personales sea vista como un derecho indispensable para el ejercicio de otros derechos y para el fortalecimiento de las democracias.

En suma, el camino recorrido por el INFO CDMX demuestra que es posible innovar, generar conocimiento, construir alianzas y transformar las prácticas institucionales para responder a los desafíos de la era digital. El reto hacia el futuro será consolidar y perfeccionar estos avances, con la convicción de que sólo es posible alcanzarlos cuando se coloca, en todo momento, a las personas y a sus derechos humanos en el centro de las acciones.

REFERENCIAS

- Constitución Política de la Ciudad de México (CPCDMX). (5 de febrero de 2017, última reforma: 23 de diciembre de 2024). *Gaceta Oficial de la Ciudad de México*. https://data.consejeria.cdmx.gob.mx/images/leyes/estatutos/CONSTITUCION_POLITICA_DE_LA_CDMX_14.2.2.pdf
- Enríquez Rodríguez, L. L. (Coord.). (2023). *Revoluciones: protección de datos personales y privacidad en la era digital. Orígenes, avances, tensiones y desafíos. Una mirada desde el periodismo gráfico*. INAI. <https://infocdmx.org.mx/images/biblioteca/2023/Revoluciones.pdf>
- Global Privacy Assembly (GPA). (2024). Lista de miembros acreditados. <https://globalprivacyassembly.com/participation-in-the-assembly/list-of-accredited-members/>
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2021). *Carta de Derechos de la Persona en el Entorno Digital. Código de Buenas Prácticas*. INAI. https://www.idaip.org.mx/archivos/transparencia/ruoch/BIBLIOTECA%20DIGITAL/Carta_DDigitales.pdf
- INFO CDMX. (2024a). Registro Electrónico de Sistemas de Datos Personales (RES-DP) 3.0 <https://datospersonales.infocdmx.org.mx/publichome>
- INFO CDMX. (2024b). Red de Protección de Datos Personales Ciudad de México. <https://portalddp.infocdmx.org.mx>
- INFO CDMX. (2025a). Estadísticas. <https://infocdmx.org.mx/index.php/estadisticasdelpeno.html>
- INFO CDMX. (2025b). SIVER. <https://portalddp.infocdmx.org.mx/Home/Siver>
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). (2024). Reconoce INAI proyectos ganadores del Premio a la Innovación y Buenas Prácticas en la Protección de Datos Personales 2023. Comunicado INAI/037/24. <https://home.inai.org.mx/wp-content/documentos/SalaDePrensa/Comunicados/Comunicado%20INAI-037-24.pdf>
- Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México (LPDPPSOCDMX). (10 de abril de 2018, última reforma: 11 de febrero de 2021). *Gaceta Oficial de la Ciudad de México*. https://data.consejeria.cdmx.gob.mx//images/leyes/leyes/LEY_DE_PROTECCION_DE_DATOS_PERSONALES_EN_POSESION_DE_SUJETOS_OBLIGADOS_DE_LA_CDMX_4.pdf
- Mendoza Enríquez, O. A., y Enríquez Rodríguez, L. L. (Coords.). (2024). *Desafíos del derecho a la protección de datos personales en la era digital. Una mirada desde América Latina*. Tirant lo Blanch. https://infocdmx.org.mx/images/biblioteca/2024/DesafiosDerecho-PDP_EraDigital.pdf
- Red Iberoamericana de Protección de Datos Personales (RIPDP). (2024). Países miembros. <https://www.redipd.org/la-red/integrantes/paises>

CAPÍTULO X

Las cinco generaciones de las normas de protección de datos y el derecho a la autodeterminación informativa en la jurisprudencia de la Corte IDH

Oscar Raúl Puccinelli Parucci¹

SUMARIO: X.1. Introducción: Las cinco generaciones de normas de protección de datos; X.2. El reconocimiento jurisprudencial del derecho a la autodeterminación informativa en el Caso CAJAR de la Corte IDH; X.3. Conclusiones.

PALABRAS clave: Derechos humanos, TIC, derechos digitales, protección de datos, autodeterminación informativa, privacidad, archivos de inteligencia, *habeas data*.

X.1. INTRODUCCIÓN. LAS CINCO GENERACIONES DE NORMAS DE PROTECCIÓN DE DATOS

Desde que en la década de 1970 el *Land* de Hesse alemán aprobara la primera ley de protección de datos, pueden revistarse hasta la actualidad cinco generaciones de normas de protección de datos, teniendo en consideración tanto el reconocimiento progresivo de los derechos humanos, como, especialmente, los cambios tecnológicos y su impacto sobre éstos.

La primera generación, tributaria de la época de Arpanet (la predecesora de Internet), se inauguraba por la ley alemana recién citada y durará hasta 1981, con la aprobación, en el ámbito del Consejo de Europa, del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, (OEA, 2012) norma que, junto con las Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales emanadas de la Organización para la Cooperación y el Desarrollo Económicos (OCDE, 2002), servirán de cierre de esta etapa y de apertura de la siguiente.

¹ Doctor en Derecho Constitucional por la Universidad de Buenos Aires; profesor de grado y de posgrado en diversas Universidades Latinoamericanas; Vicepresidente de la Red Académica Internacional de Protección de Datos; miembro de la Red Global de Derechos Humanos Digitales; Recipiendario de la Cátedra Alan Turing por el INFO CDMX y Juez de la Sala Segunda de la Cámara de Apelación en lo Civil y Comercial de Rosario.

Son frutos de esta etapa las leyes de Suecia (1973), Francia (1977), Alemania Federal (1977), Austria (1978), Dinamarca (1978), Noruega (1978) y Luxemburgo (1979). Además, se incorporaron disposiciones en las constituciones de Portugal (1976, reformada en 1991) y de España (1978), frente a las preocupaciones derivadas de los avances de la informática.

En el ámbito americano, en los Estados Unidos se adoptaron la *Fair Credit Reporting Act* (FCRA, 1970), la *Family Educational Rights and Privacy Act* (FERPA, 1974) y la *Privacy Act* (1974), norma que complementa la *Freedom of information act* (FOIA, 1966 y reformas de 1974 y 1976). En el ámbito latinoamericano, en gran medida bajo regímenes autoritarios y con escaso acceso a las Tecnologías de la Información y Comunicación (TIC), no se dictaron normas constitucionales ni legales.

La segunda generación de leyes arranca en 1981 y se extenderá hasta 1995, cuando fuera aprobada por el Parlamento Europeo y el Consejo la Directiva 95/46/CE, relativa a la protección de las personas físicas, en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos” (24 de octubre de 1995, L 281).

Esta etapa es ya tributaria de internet (en 1983 el Departamento de Defensa estadounidense decidió incorporar el protocolo TCP/IP en su red, que pasó a llamarse “Arpanet Internet” –con el tiempo internet, a secas–) y de la “web 1.0”, que apareció hacia 1990, en la forma más básica de navegadores de solo texto, una web unidireccional pues sólo se podía consumir contenido sin posibilidad de interactuar. Sus normas partirán de las primeras leyes de protección de datos y sistematizarán más adecuadamente los principios y derechos reconocidos, a la par de preocuparse por el libre flujo de los datos debidamente tratados, en un entorno marcado por notorios avances tecnológicos de variada índole.

Como consecuencia de las reglas emanadas del Convenio 108, se aprobaron numerosas leyes europeas, algunas nuevas y otras reformadas, en concreto: Reino Unido (1984), Finlandia (1987), Dinamarca (1987 y 1991), Irlanda (1988), Países Bajos (1989), República Federal Alemana (1990), Portugal (1991), Suecia (1992), Hungría (1992), Bélgica (1992) y España (1992). Al inicio de ese período, precisamente en 1983, cuando apareció internet, se reconoció por primera vez un derecho autónomo “a la autodeterminación informativa” por parte del Tribunal Constitucional alemán, en su célebre sentencia sobre la inconstitucionalidad de la Ley de Censo de Población de 1982 (TCE, 1983).

En el ámbito internacional global, la Asamblea General de la ONU adoptó una serie de principios muy básicos para la reglamentación de los ficheros computadorizados de datos personales (ONU, 1990).

Ya en América, Canadá adoptó la *Privacy act*, aplicable al sector público (1983), y en los Estados Unidos se aprobaron diversas normas sectoriales, la *Cable TV Privacy Act* (1984); la *Video Privacy Protection Act* (1988); la *Telephone Consumer Protection Act* (1991) y; la *Driver’s Privacy Protection Act* (1994). En Latinoamérica no se aprobaron leyes de

protección de datos, pero aludieron a la problemática desde distintos ángulos las constituciones de Guatemala (1985); Nicaragua (1987, reformada en 1995); Brasil (1988); Colombia (1991); Paraguay (1992); Perú (1993 con su reforma de 1995) y; Argentina (1994).

La tercera generación de normas se abre con la aprobación de la Directiva 95/46/CE y se extenderá hasta 2009, cuando la 31a. Conferencia Internacional de Autoridades de Protección de Datos y Privacidad adoptó la “Propuesta Conjunta para la Redacción de Estándares Internacionales para la protección de la Privacidad, en relación con el Tratamiento de Datos de carácter personal (Resolución de Madrid)” (AEPD, 2009).

Así, a partir de la Directiva 95/46/CE, que requería la transposición de sus normativas, los países comunitarios aprobaron o modificaron sus leyes, entre ellos inicialmente Italia (1996); Suecia (1998); Reino Unido (1998) y; España (1999), y luego el resto de los países, completándose el ciclo de reformas durante este período. Se destaca, como punto de inflexión normativa en la región, la aprobación, en 2000, de la Carta de Derechos Fundamentales de la Unión Europea (CDFUE) “Declaración de Niza”, que consagró como derecho autónomo al derecho a la protección de datos (CDFUE, 2012, art. 8), separado del derecho a la vida privada (CDFUE, 2012, art. 7), siguiendo en definitiva la configuración teórica del fallo del Tribunal Constitucional del período anterior.

A partir de allí, las regulaciones comunitarias no dejaron de sucederse, entre ellas el Reglamento (CE) 45/2001 de protección de datos de las instituciones de la UE (21 de enero de 2001, L 8/1), la Directiva 2000/31/CE, sobre el comercio electrónico (17 de julio de 2000, L 178/1), la Directiva 2002/58/CE sobre la privacidad y las comunicaciones electrónicas (31 de julio de 2002, L 201) y la Directiva 2003/98/CE relativa a la reutilización de la información del sector público (31 de diciembre de 2003, L345/90). También dentro de este período, se aprobó en 2004 el Marco de Privacidad del Foro de Cooperación Económica Asia-Pacífico (APEC), (Tellez Valdés, 2013, p. 481) que será actualizado en 2015, y promueve un enfoque flexible para la protección de la privacidad de la información en las economías de sus Estados miembros –varios de los cuales son americanos–,² a fin de evitar la creación de barreras innecesarias para los flujos de información y asegurar el intercambio continuo y el crecimiento económico en la región.

A esas alturas se gestaron cambios tecnológicos muy relevantes que modificaron sustancialmente la vida diaria de las personas, que ya masivamente se volcaron a la Red –entre ellos, la aparición del *smartphone* con *wifi*, poco antes de las redes sociales, que ya permitían a los usuarios incorporar contenidos, y tornaron a la web en inte-

² Integran la APEC: Australia, Brunéi, Canadá, Chile, China, Corea del Sur, Estados Unidos, Filipinas, Hong Kong, Indonesia, Japón, Malasia, México, Nueva Zelandia, Papúa Nueva Guinea, Perú, Rusia, Singapur, Tailandia, Taiwán y Vietnam.

ractiva (“web 2.0”, “social” o “participativa”)–, estado de cosas que generó inusitadas amenazas que motivaron una profunda movilización y cambios en el enfoque de la protección de datos, los cuales, aun insuficientemente, fueron volcados en los estándares contenidos en la Resolución de Madrid.

Pasando a las Américas, Canadá adoptó la *Personal Information Protection and Electronic Documents Act* –aplicable al sector privado– (2000); en los Estados Unidos fueron aprobadas diversas leyes federales, en concreto, la *Health Insurance Portability and Accountability Act* (1996); la *Children’s Online Privacy Protection Act* (1998); la *Gramm Leach Bliley Act* (1999); la *Fair and Accurate Credit Transactions Act* (2003), y la *Controlling the Assault of Non-Solicited Pornography And Marketing Act* (2003), y en el Caribe adoptaron leyes Bahamas (2003) y San Vicente y Granadinas (2003).

Ya en Latinoamérica, se destaca la creación, en La Antigua Guatemala (2003), de la Red Iberoamericana de Protección de Datos (RIPD, s.f.) y la Declaración de Santa Cruz de la Sierra, Bolivia, 2003 (SEGIB, 2003 y 2014), por la que se reconoció el rango de derecho fundamental del derecho a la protección de los datos de carácter personal. Se aprobaron además normas constitucionales en Ecuador (1998), Venezuela (1999); Panamá (2004); Bolivia (2004 y 2009); Honduras (2006) y; México (2007). En el plano subconstitucional, se aprobaron leyes en Chile (1999), Argentina (2000), Paraguay (2001), Uruguay (2004 y 2008) y, Colombia (2008 y 2012).

La cuarta generación se inicia a partir de la Resolución de Madrid y se extenderá hasta que, en 2016, se aprobara el Reglamento (UE) 2016/679 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos (Reglamento general de protección de datos) (4 de mayo de 2016, L 199/1), que derogó la Directiva 95/46/CE e impulsó la revisión Directiva 2002/58/CE, instrumento que significó otro punto de inflexión por la incorporación de nuevos y sustanciales cambios regulatorios que respondieron mucho más certeramente a las nuevas tecnologías que, incorporadas en la etapa anterior, se profundizaron en esta, ingresándose a la “web 3.0” (la web semántica).

A la Resolución de Madrid se le adicionaron el Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos, (CE, 2009), las nuevas Directrices de la OCDE sobre protección de la privacidad y flujos transfronterizos de datos personales, aprobadas en 2013 (OCDE, 2002) y la Directiva 2013/37/UE que reforma a la 2003/98/CE relativa a la reutilización de la información del sector público, también de 2013. (27 de junio de 2013, L 175/1).

En Américas, la OEA aprobó en 2015 los *Principios sobre la protección de la privacidad y los datos personales* (OEA, 2021) –los que fueron luego actualizados en 2021–, en los Estados Unidos se aprobó la *Health Information Privacy Protection Act* (2013) y, en el Caribe, Curaçao (2010), San Martín (2010), Santa Lucía (2011), y Trinidad y Tobago (2011).

Ya en Latinoamérica, se dictaron normas constitucionales en México (2009); Ecuador (2008) y; República Dominicana (2010), en el plano legal se aprobaron leyes en México (2010), Perú (2011), Costa Rica (2011), Nicaragua (2012) y República Dominicana (2013).

La quinta generación arrancó a partir del Reglamento General de Protección de Datos, en tiempos en que la “web 3.0” transitaba hacia la “web 4.0” (la web simbiótica), al calor de la intensificación del uso de la tecnología *blockchain*, de los metaversos y multiversos, de la Inteligencia Artificial Generativa (*GenAI*)³ y de las neurotecnologías, entre otros fenómenos disruptivos que hacen presagiar una pronta iniciación de una sexta generación de normas.

Complementaron inmediatamente al Reglamento, la Directiva (UE) 2016/680 relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos (27 de abril de 2016, L 119/89) ; la Directiva (UE) 2016/681 relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave (27 de abril de 2016, L 119/132) y la Directiva (UE) 2016/1148 relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión (19 de julio de 2016, L 194/1).

En 2018, entrando en vigencia el Reglamento General de Protección de Datos (RGPD), se aprobó el Protocolo adicional al Convenio 108 de 1981 (Convenio 108 Plus), por el cual se modernizó el antiguo convenio, el Reglamento (UE) 2018/1724 relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) 1024/2012 (21 de noviembre de 2018, L 295/1); el Reglamento (UE) 2018/1725 (Gobernanza de datos) relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) 45/2001 y la Decisión 1247/2002/CE (21 de noviembre de 2018, L 295/39), en el cual se establece un Supervisor Europeo de Protección de Datos como organismo independiente de la UE, que se encarga de supervisar la aplicación de las normas sobre protección de datos en las instituciones europeas y de investigar las denuncias y el Reglamento (UE) 2022/868 relativo a la gobernanza europea de datos y por el que se modifica el Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). (3 de junio de 2022, L 152/1).

³ La Inteligencia Artificial Generativa es una rama de la IA que se enfoca en la creación de contenido original a partir de datos preexistentes, siendo sus primeras aplicaciones más populares del mercado Midjourney y ChatGPT.

También se aprobaron la Directiva (UE) 2019/790 sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE (17 de mayo de 2019, L 130/92); la Directiva (UE) 2019/1024 relativa a los datos abiertos y la reutilización de la información del sector público (26 de junio de 2019, L 175/56); la Directiva (UE) 2019/1937 relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión (26 de noviembre de 2019, L 305), la Directiva (UE) 2022/2555 (Directiva SRI2), relativa a las medidas para un elevado nivel común de ciberseguridad en toda la Unión (27 de diciembre de 2022, L 333/80), el Reglamento (UE) 2022/1925, sobre mercados disputables y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales) (12 de octubre de 2022, L 265/1) y el Reglamento (UE) 2022/2065 relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE sobre comercio electrónico (Reglamento de Servicios Digitales) (27 de octubre de 2022, L 277/1).

De otro lado, en 2022 la OCDE adoptó su Declaración sobre un futuro digital fiable, sostenible e inclusivo (OCDE, 2022) y en 2023 se aprobó la Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital (23 de enero, *DOUE*).

Como consecuencia de muy recientes desarrollos de la inteligencia artificial generativa (*GenAI*) y de las neurotecnologías, se dictaron recomendaciones y regulaciones de todo tipo, entre las cuales la Comisión Europea lanzó en 2018 sus *Directrices éticas para una IA fiable* (Com. E, 2019), y propuso un Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de inteligencia artificial) y se modifican determinados actos legislativos de la Unión (Com. E, 2021), que fue aprobado a inicios de 2024 por el Parlamento Europeo.

En América se dictaron cuatro normas de *soft law* sumamente relevantes que impactan en la región. En el ámbito de la OEA, los Principios sobre la privacidad y la protección de datos personales, de 2015, que fueron actualizados en 2021 (OEA, 2021) y la Red Iberoamericana de Protección de Datos (RIPD), aprobó, por un lado, los *Estándares de protección de datos personales para los estados iberoamericanos* (RIPD, 2017), gestados en sintonía con el Reglamento General de Protección de Datos de la Unión Europea y, por el otro, las *Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial* (RIPD, 2029b), y las *Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial* (RIPD, 2020a).

En los Estados Unidos, en 2018 se aprobó la “Ley de Clarificación del Uso de Datos en el Extranjero” (*CLOUD Act*), y en los estados federados, se dictaron normas generales sobre protección de datos y privacidad o respecto del consumidor desde 2017 en Nevada, California, Colorado, Delaware, Indiana, Iowa, Kentucky, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah y Virginia.

En el Caribe se aprobaron leyes en Bermuda (2016), Islas Cayman (2017) y Saint Kitts & Nevis (2018), en el ámbito latinoamericano se destaca en este período la adopción de normas constitucionales en Chile (2018 y 2021) y Cuba (2019), y de leyes emitidas en México (2017), Brasil (2018), Panamá (2019), Paraguay (2020) y Ecuador (2021).

X.2. EL RECONOCIMIENTO JURISPRUDENCIAL DEL DERECHO A LA AUTODETERMINACIÓN INFORMATIVA EN EL CASO CAJAR DE LA CORTE IDH

Con un escaso marco normativo específico, que se reduce en la práctica a unas breves directrices aprobadas por la Asamblea General de la OEA en 2015 y actualizadas en 2021, la Corte IDH emitió su primer fallo en materia de protección de datos en el Caso Corporación Colectivo de Abogados “José Alvear Restrepo” (CAJAR) vs. Colombia (Corte IDH, 2023), donde condenó a Colombia por violación a diversos derechos contenidos en la CADH y en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer, en virtud de haber realizado actividades de inteligencia contrarias a estas normas, en perjuicio de determinados miembros de la Corporación “CAJAR”, una organización no gubernamental dedicada a la defensa y promoción de los derechos humanos, y sus familiares.

En este fallo reconoció dos nuevos derechos autónomos que se derivan del contenido de la CADH: el “derecho a la defensa de los derechos humanos” y el derecho a la “derecho a la autodeterminación informativa”, emulando, en el caso de este último, lo hecho por el Tribunal Constitucional alemán en 1983, extrayéndolo de los derechos a la dignidad y a la autodeterminación y también de los derechos a la privacidad y de acceso a la información.

Debido a estas las violaciones detectadas, la Corte –con dos disidencias parciales y un voto concurrente del juez Mudrovitsch, que trata muy pormenorizadamente a este nuevo derecho– ordenó diversas medidas de reparación, entre ellas la depuración y acceso a los archivos y la modificación de las leyes vigentes en función de las directrices que imparte.

En capítulo VIII, al tratar el fondo del asunto, la Corte trata en abstracto al derecho a la autodeterminación informativa en cuanto a origen, alcances y contenido (Corte IDH, 2023, párr. 566 a 608), y luego aplica tales conceptos al caso concreto (Corte IDH, 2023, párr. 636 a 651).

Así, en cuanto al derecho extraído de las implicitudes de la CADH, alude a la dignidad de la persona, al derecho a la vida privada, englobante del derecho a la autonomía personal, al derecho al desarrollo personal y al derecho a establecer y desarrollar relaciones con otros seres humanos y con el mundo exterior. Y agrega que, en ese contexto de autonomía y libre desarrollo de la personalidad, la persona también

es libre para autodeterminarse a fin de decidir cuándo y en qué medida revela aspectos de su vida privada, lo que incluye definir qué tipo de información, incluidos sus datos personales, puede ser conocida por los demás, derecho que obliga a “prever un marco de actuación de las autoridades en el ámbito de la recopilación y utilización de datos personales, a fin de evitar su obtención, uso, retención, divulgación e intercambio de forma inadecuada o incompatible con aquellos derechos” (Corte IDH, 2023, párr. 571).

Fija luego una serie de estándares, afirmando preliminarmente

[...] que los Estados deben adoptar políticas tendientes a prohibir el tratamiento de datos personales [...] salvo cuando exista consentimiento informado de la persona afectada [o habilitación legal, y] a la vez, deben adoptar medidas positivas tendientes a informar a las personas [sobre] sus derechos en esta materia y sobre las condiciones legales para el tratamiento de datos personales [quienes deben estar notificadas sobre la] recolección, almacenamiento, tratamiento o divulgación de datos. (Corte IDH, 2023, párr. 574)

Agrega que las autoridades

[...] están limitadas a obtener los datos verídicos, pertinentes y necesarios para el cumplimiento estricto de sus funciones, de acuerdo con el marco legal aplicable [...] [que] las facultades de utilización, conservación y tratamiento de los datos deben ejercerse en consonancia con los fines para los que fueron recopilados y por el tiempo imprescindible para ello [...] [y que] la gestión de los datos debe garantizar que estos se mantengan actualizados, completos y exactos, así como asegurar, por mecanismos adecuados y razonables, su protección y seguridad, en el sentido de evitar su acceso, pérdida, destrucción, utilización, modificación o divulgación no autorizados. (Corte IDH, 2023, párr. 576)

Ya en lo estrictamente referido a las facultades de los servicios de inteligencia, dado que son ejercidas, por lo general, sin consentimiento del titular de los datos, exige que se las regule por una ley formal del

[...] Poder Legislativo, accesible al público [(no secreta), la cual debe prever], con especificidad, las facultades de los organismos de inteligencia, [tanto] para la recopilación de datos personales [...] como para implementar y mantener archivos que [los] incluyan [regulando] con la mayor precisión posible: a) los motivos que habilitan la existencia de [los] archivos [...] de los organismos de inteligencia; [b)] la limitación del accionar de las autoridades de inteligencia a esos motivos acordes con los fines propios de las actividades de inteligencia; [c)] las clases y tipos de datos de carácter personal que las autoridades están facultadas para conservar en sus archivos, y [d)] los parámetros aplicables para la utilización, conservación, verificación, rectificación, eliminación o revelación de tales datos. (Corte IDH, 2023, párr. 577)

Con cita de los casos “Leander vs. Suecia” y “Rotaru vs. Rumania” del TEDH, dice que los datos sensibles no pueden, en principio, ser tratados, pero que, si resultare necesario, una ley debe especificar los motivos habilitantes, los tipos de datos permitidos y los criterios adecuados para su tratamiento, limitando dicho tipo de información a la estricta y razonablemente necesaria para cumplir con sus funciones (Corte IDH, 2023, párr. 578).

Carga luego a los organismos de inteligencia con la obligación de “evaluar periódicamente la necesidad de conservar los datos [...] y, en su caso, corroborar [su] exactitud, [por lo que se deben] actualizar o rectificar los datos de advertirse alguna inexactitud, o bien eliminarlos si ya no fuere necesaria su conservación para el cumplimiento de sus funciones” (Corte IDH, 2023, párr. 580).

Destaca que

A nivel internacional se señala la necesidad de que una institución independiente de los organismos de inteligencia sea la encargada de supervisar la utilización que hacen dichas autoridades de toda información y de los datos de carácter personal [que tratan y que esa institución], además de poder acceder a los archivos de inteligencia [y] [...] ordenar la eliminación [...] [o] la revelación de esta información a las personas afectadas. (Corte IDH, 2023, párr. 581)

Alude luego a que

Los estándares internacionales refieren también a la necesidad de disponer de métodos razonables, ágiles, sencillos, eficaces y gratuitos para que las personas cuyos datos personales han sido recopilados puedan solicitar el acceso, rectificación y eliminación de los datos, así como el derecho a oponerse a su tratamiento y, en lo aplicable, el derecho a su “portabilidad” [...] [y que] En caso de que fuera necesario restringir los alcances de estos derechos, los fundamentos [...] deberían especificarse en la legislación nacional y preverse de manera compatible con los estándares internacionales aplicables. (Corte IDH, 2023, párr. 582)

Menciona también que

En el ámbito europeo se reconoce el derecho de las personas a saber si los datos de su titularidad son o no objeto de tratamiento por parte de las autoridades [...] [y a recibir] información sobre los fines y la base jurídica del tratamiento; las categorías de datos personales que se tratan; los destinatarios o las categorías de destinatarios [...] y el plazo y los criterios [de conservación]. [agrega que] En el caso de información confidencial relacionada con la seguridad pública, la seguridad nacional o la protección de los derechos humanos, es posible restringir al interesado el derecho de acceso [debiendo] el responsable del tratamiento [...] justificar por escrito los motivos de la denegación. (Corte IDH, 2023, párr. 583)

Consecuentemente, los particulares deben poder acceder a sus datos y “reclamar su rectificación cuando éstos no sean exactos [y] cualquier excepción a esta regla, además de estar prevista legalmente, debe ser proporcional y necesaria para el desempeño de los servicios de inteligencia” (Corte IDH, 2023, párr. 584).

El párrafo 585 sintetiza lo anterior, señalando qué facultades deben reconocerse a los titulares de los datos⁴ y ya en entre los párrafos 586 y 588 reafirma que esos elementos

[...] dan configuración a un derecho humano autónomo: el derecho a la autodeterminación informativa, reconocido en distintos ordenamientos jurídicos de la región, y que encuentra acogida en el contenido tutelar de la Convención Americana, en particular a partir de los derechos recogidos en los artículos 11 y 13, y, en la dimensión de su protección jurisdiccional, en el derecho que garantiza el artículo 25. (Corte IDH, 2023, párr. 586)

Que este nuevo derecho “participa en la protección a la vida privada en cuanto prohíbe las injerencias arbitrarias o abusivas y garantiza el amparo ‘de la ley contra esas injerencias’ (art. 11, CADH); [que] se sustenta en el derecho de acceso a la información[...]” (párr. 587), bajo el control del Estado, por el cual las autoridades están obligadas a suministrarla o de brindar una respuesta fundamentada cuando por algún motivo permitido se limite su acceso (art. 13.1, CADH); y que

⁴ “585. En suma, los estándares reseñados refieren que, desde la perspectiva de la persona cuyos datos consten en los archivos públicos, resulta imprescindible, en aras de garantizar su autonomía y la libertad para autodeterminarse, reconocer su derecho a acceder y controlar aquellos datos, con los alcances siguientes:

- (i) el derecho a conocer qué datos se encuentran en los registros de los órganos públicos, en soportes físicos, magnéticos, electrónicos o informáticos, de dónde provienen, cómo fueron obtenidos, para qué son utilizados, el plazo de su conservación, si son compartidos con otras instancias o personas, la razón de ello y, en general, las condiciones de su tratamiento;
- (ii) el derecho a reclamar la rectificación, modificación o actualización de los datos, en el caso de ser inexactos, incompletos o no estar actualizados;
- (iii) el derecho a exigir la eliminación, cancelación o supresión de los datos, en caso de constatar la ilegalidad de su recopilación o conservación, o la inexistencia de razones que justifiquen su mantenimiento en archivos o bases de datos estatales, en tanto ello no afecte otros derechos, lo que necesariamente debe ser ponderado en orden a la naturaleza de los archivos de que se trate y la información que contienen, siempre de acuerdo a la regulación aplicable;
- (iv) el derecho a oponerse al tratamiento de los datos, en los casos en que, en razón de la situación particular de la persona, se cause un daño en su perjuicio, así como en los supuestos que la normativa sobre la materia disponga, y
- (v) cuando fuere posible y de acuerdo a las previsiones legales pertinentes, el derecho a recibir los datos en un formato estructurado, de uso común y lectura mecánica, y requerir su transmisión sin que lo impida la autoridad que los conserva.

En definitiva, se trata de un derecho autónomo que sirve, a su vez, de garantía de otros derechos, como los concernientes a la privacidad, a la protección de la honra, a la salvaguarda de la reputación y, en general, a la dignidad de la persona. [remarca asimismo que] [...] el derecho alcanza, con las limitaciones aplicables [...] a cualquier dato de carácter personal en poder de todo órgano público, y opera igualmente respecto de registros o bases de datos a cargo de particulares, cuestiones sobre las que no se ahonda en razón del objeto de este proceso internacional. (Corte IDH, 2023, párr. 588)

En el párrafo 589 refiere a la icónica sentencia del Tribunal Constitucional alemán del 15 de diciembre de 1983 que configuró

[...] el derecho a la “autodeterminación informativa”, sosteniendo que es imprescindible como “requisito previo para la autodeterminación individual”, que la persona tenga la libertad para decidir “qué tipo de información personal es conocida por ciertas partes de su entorno social”, pues, de lo contrario, se “podría obstaculizar en gran medida su libertad para tomar planes y decisiones”, y entonces “[e]l libre desarrollo de la personalidad requiere que el individuo esté protegido contra la recopilación, el almacenamiento, el uso y el intercambio ilimitados de sus datos personales. (Corte IDH, 2023)

Luego, menciona que en distintos Estados de la región, se ha reconocido y desarrollado por vía jurisprudencial el contenido del nuevo derecho –sin que siempre se lo hubiera denominado con el rótulo escogido en el fallo–, ilustrando con diversos fallos dictados por tribunales nacionales de clausura de la región –Argentina, Brasil, Chile, Colombia, Costa Rica, Guatemala, México y Paraguay– (Corte IDH, 2023, párr. 590 a 598).

En el párrafo 599 agrega que:

[...] la efectividad del derecho a la autodeterminación informativa exige que los Estados prevean mecanismos o procedimientos adecuados, ágiles, gratuitos y eficaces para dar trámite y atender, por parte de la misma autoridad que administra los datos o por otra institución competente en materia de protección de datos personales o de supervisión, las solicitudes de acceso y control [sobre] los datos, con plazos razonables definidos para su resolución y bajo la responsabilidad de funcionarios debidamente capacitados. [y afirma que] Esta exigencia, deriva del deber que establece el art. 2 de la CADH, en cuanto abarca la expedición de normas y el desarrollo de prácticas conducentes a la observancia de los derechos humanos, incluidos procedimientos administrativos apropiados como garantía esencial para hacer valer y ejercer el derecho. (Corte IDH, 2023)

Ya en el párrafo 600 afirma que, por derivación “el art. 25.1 de la CADH, se debe garantizar el derecho a la protección judicial” del nuevo derecho a través de “un recurso sencillo y rápido ante los tribunales de justicia, que [deben proveer] protección adecuada [...], en el caso de denegarse, total o parcialmente, el acceso a los datos personales o a alguno de los otros contenidos del derecho” (Corte IDH, 2023), destaca que en tal dirección, algunos sistemas jurídicos de los Estados de la región lo han adoptado bajo diferentes modalidades - entre ellas el *habeas data*-, y que sin perjuicio del *nomen iuris* que se emplee, debe configurar un recurso, acción o proceso jurisdiccional que provea tutela efectiva al derecho en el orden interno.

Entre los párrafos 601 y 609 finaliza trazando las limitaciones válidas al derecho en el ámbito de los archivos de inteligencia, reconociendo que los objetivos mismos de las actividades de inteligencia tornan inviable, en determinadas circunstancias, brindar el acceso total o parcial a los archivos de las autoridades, por lo que remite en este aspecto a los criterios definidos por la jurisprudencia interamericana sobre las limitaciones válidas al derecho de acceso a la información (v.gr. “Claude Reyes y otros vs. Chile”), en concreto: a) “[...] cualquier restricción al derecho, como podría ser la calificación como reservada de la información en poder de las autoridades de inteligencia, debe estar previamente fijada en una ley [...]” (párr. 601), que “debe ser, en la mayor medida posible, clara y precisa, estableciendo límites temporales para la reserva” (párr. 602); b) “[...] la autoridad debe garantizar que los datos personales no serán divulgados ni puestos a disposición de terceros en contravención del marco legal” (párr. 602); c) “el carácter reservado de la información que impida su acceso y control debe considerarse siempre excepcional, de manera que la ley debe prever, con especificidad, los motivos para calificar como reservada a determinada información, en función de su contenido” (párr. 602); y, d) “la limitación debe responder a un fin legítimo en una sociedad democrática (art. 13.2, CADH)” (Corte IDH, 2023, párr. 602).

Destaca luego que,

la reserva de información personal en poder de los organismos de inteligencia [por motivos] de seguridad nacional no [puede fundarse] mediante una calificación general [que la] considere relacionada con dicho fin, sino que es necesario que la ley designe las categorías específicas y estrictas que, en función de dicho objetivo, son alcanzadas por la reserva. (Corte IDH, 2023, párr. 603)

Y en esta dirección, “en congruencia con los criterios internacionales sobre la materia, identifica diversos supuestos concretos que, respondiendo al objetivo de la seguridad nacional, podrían legitimar una regulación legal [por la que se autorice al Estado a no] proveer la información en poder de los servicios de inteligencia” (Corte IDH, 2023, párr. 604).⁵

⁵ En concreto, información sobre: “[...] planes de defensa en curso; las capacidades o el uso de sistemas de armamentos o comunicaciones por las fuerzas militares; medidas destinadas al resguardo del territorio o las instituciones nacionales frente a concretas amenazas, siempre que la efectividad de las medidas

Finaliza afirmando que “la restricción impuesta [a los derechos], según ha exigido la jurisprudencia interamericana, debe cumplir con los requisitos de idoneidad, necesidad y proporcionalidad en las circunstancias del caso concreto” (Corte IDH, 2023, párr. 605);⁶ que de “considerarse inviable el acceso y control de los datos, la autoridad competente [lo dispondrá mediante] una decisión suficientemente motivada, por razones de debido proceso (art. 8.1, CADH)” (Corte IDH, 2023, párr. 606).

[...] que, al igual que las limitaciones en materia de actividades de inteligencia, está vedado a las autoridades utilizar la reserva de la información con el interés encubierto de favorecer o perjudicar a una determinada actividad o ideología política, o de cualquier otra manera que implique algún tipo de discriminación [...]; que sin importar si el acceso a los datos personales es denegado o no por las autoridades, recae en estas el deber de administrar dicha información adecuadamente, evitando su alteración, pérdida, transmisión y acceso no autorizados, siempre que subsistan los motivos que justifiquen su conservación [...]; [que en] casos de violaciones a los derechos humanos, la reserva de la información justificada en razones de interés público o seguridad nacional no puede amparar la negativa de las autoridades para aportar la información requerida por las instancias judiciales o administrativas encargadas de la investigación o de procesos pendientes [...] [que] en el supuesto de investigación de un hecho punible, la decisión de calificar como secreta la información y la consecuente denegatoria de su entrega jamás puede depender exclusivamente de un órgano estatal a cuyos miembros se les atribuye la comisión del hecho [...] [y que] la categoría reservada de determinada información no debe entenderse indefinida en el tiempo, sino que tal carácter, y la subsiguiente negativa a su acceso, deberá mantenerse durante el periodo estrictamente necesario para el cumplimiento del fin legítimo perseguido, con revisiones periódicas a fin de verificar dicha necesidad. (Corte IDH, 2023, párr. 607)

dependa de su confidencialidad; operaciones, fuentes o métodos de los servicios de inteligencia concernientes a asuntos de seguridad nacional, e información relacionada con asuntos de seguridad nacional suministrada por Estados extranjeros u organismos intergubernamentales, así como comunicaciones diplomáticas sobre tales asuntos, respecto de los cuales exista una expectativa expresa de confidencialidad”. (Corte IDH, 2023, párr. 604)

⁶ “En otras palabras, la reserva de la información contenida en los archivos de inteligencia debe ajustarse a las exigencias del principio de proporcionalidad, esto es: a) que la reserva sea idónea o adecuada para alcanzar el fin que persigue, precisamente, la negativa de posibilitar el acceso a la información; b) que la reserva sea necesaria, por considerarse absolutamente indispensable para alcanzar aquel fin, descartando la existencia de cualquier otra medida menos gravosa para el derecho de acceso a la información que resulte igualmente idónea para la realización del fin perseguido, y c) que la reserva resulte estrictamente proporcional, en el sentido que la limitación al derecho de acceso a la información no se advierta exagerada o desmedida frente a las ventajas que se obtienen por medio de tal limitación y la consecuente realización del fin perseguido. Así, la aplicación del test de proporcionalidad en casos concretos puede posibilitar que, garantizando la realización del fin legítimo perseguido, se permita el acceso parcial a determinados archivos, documentos o datos”. (Corte IDH, 2023, párr. 605)

Concluye luego en que

Todo lo anterior exige que [...] el marco legal disponga de mecanismos de depuración y desclasificación de los archivos de inteligencia, en el sentido de posibilitar el acceso público a los documentos y datos cuya reserva ya no esté justificada, y la previsión de periodos fijos de desclasificación automática de la información, siempre salvaguardando la confidencialidad de los datos sensibles o de aquellos que, conforme la normativa aplicable, la divulgación requiera el consentimiento de su titular [...]. [y en que] A su vez, en garantía del derecho a la autodeterminación informativa [...], el sistema jurídico debe prever un mecanismo judicial que permita a la persona objetar las razones invocadas por la autoridad administrativa para negarle el acceso a sus datos, instrumento jurisdiccional que puede estar precedido, según lo disponga la regulación interna, de la revisión de aquella negativa por instancias administrativas [...]. [y siempre permitiendo que] En todo caso, la autoridad judicial, [esté habilitada para acceder a] la información cuyo acceso ha sido denegado. (Corte IDH, 2023, párr. 608)

El fallo bajo comentario contó, como se anticipó, con el voto concurrente del juez Mudrovitsch, quien con un estilo particular de neto corte comentarista y complementario del fallo, abunda en los fundamentos de los dos nuevos derechos extraídos de la CADH, y con respecto a la autodeterminación informativa, destaca sus antecedentes históricos, evolución y contenidos, en cuyo contexto alude a otros aspectos no considerados en el voto mayoritario (v.gr., el “derecho a la integridad de los sistemas de información”), dejando algunos interrogantes que deberán ser analizados en otros casos que lleguen a los estrados de la Corte.

X.3. CONCLUSIONES

El derecho a la protección de datos –o, si se prefiere, a la autodeterminación informativa, como la Corte IDH escogió aquí rotularlo–, ha evolucionado a lo largo de sus cinco generaciones de normas hacia una versión sumamente compleja que consagra una multiplicidad de derechos, principios y obligaciones. Sin embargo, el enorme e incesante desarrollo de este derecho no se ve reflejado en el tardío fallo de la Corte IDH, muy probablemente porque el propio tribunal destaca que los –por cierto limitados– estándares que detalla, “si bien podrían tener aplicación en las esferas de competencias de toda la administración pública y de actores privados que lícitamente recopilen y administren datos personales, su inclusión en esta Sentencia, por el objeto del proceso bajo juzgamiento, se circunscriben al quehacer de los servicios de inteligencia” (Corte IDH, 2023, párr. 571).

En tal sentido, más allá de otorgarle un gran valor a la sentencia por sus bondades generales, se trata de una oportunidad aprovechada a medias, que reclama un ulterior y pronto desarrollo de la Corte, como lo afirma el juez Mudrovitsch al referir, en su

voto concurrente, aunque aludiendo más específicamente a una extensión temática al reconocimiento del “derecho a la integridad de los sistemas” (Corte IDH, 2023, párr. 159 y 251).

Efectivamente, se observa que tanto la enumeración de las facultades reconocidas a los titulares de los datos, como la mención de los principios que deben regir los tratamientos es sumamente exigua para el contexto tecnológico actual, pues —salvo por el derecho a la portabilidad cuya operatividad no está claramente declarada—, los contenidos enunciados como integrantes del derecho a la protección de datos no difieren prácticamente de los reconocidos por el Tribunal Constitucional alemán en 1983, cuando apenas afloraba internet.

Auspiciamos que en la futura labor expansiva de lo sostenido en “CAJAR”, la Corte eche mano a otras fuentes modélicas consolidadas, como el Reglamento General de Protección de Datos de la Unión Europea (RGDP, 2016) o su pariente próximo para Iberoamérica: los *Estándares de protección de datos personales para los Estados Iberoamericanos* (RIPD, 2017) que precisamente siguen el molde de tal reglamento europeo (aunque no lo calcan pues, v.gr., no incluye el “derecho al olvido”), estándares que además, al ser un producto de la Red Iberoamericana de Protección de Datos, exhibe el consenso regional al que acude desde hace más de una década la Corte IDH para fundar su labor interpretativa-creativa (v.gr, así lo hizo en la sentencia bajo comentario y también en 2012 en el Caso Artavia Murillo y otros (Fecundación en Vitro) vs. Costa Rica al reconocer el derecho al acceso a las técnicas de reproducción asistida), esto porque sus reglas fueron seguidas en la región por todas las leyes y reformas legales ulteriores a su adopción y porque tal Red está integrada por todas las autoridades de control iberoamericanas.

En síntesis, celebramos este fallo que, aunque tardío —por las razones que fueran— e insuficiente —aunque sea por los motivos dados por la Corte—, reconoce a este nuevo y tan trascendental derecho en la sociedad digital —el que no tuvo ni pudo tener recepción en el marco de la CADH, ya que se aprobó en 1969—, augurando un pronto y potente despliegue.

REFERENCIAS

- Agencia Española de Protección de Datos (AEPD). (2009) *Estándares internacionales de protección de datos personales y privacidad. Resolución de Madrid*. https://www.edps.europa.eu/sites/default/files/publication/09-11-05_madrid_int_standards_es.pdf.
- Carta de los Derechos Fundamentales de la Unión Europea (CDFUE) (2012/C 326/02). (26 de octubre de 2012). *Diario Oficial de la Unión Europea*, C326. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:C2012/326/02>
- Comisión Europea (Com. E). (2019). *Directrices éticas para una IA fiable*. <https://data.europa.eu/doi/10.2759/14078>.

- (Com. E). (21 de abril de 2021). Propuesta de Reglamento por el que se establecen normas armonizadas en materia de inteligencia artificial (Ley de Inteligencia Artificial) y se modifican determinados actos legislativos de la Unión. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX:52021PC0206>
- Consejo de Europa (CE). (18 de junio de 2009). Convenio del Consejo de Europa sobre el Acceso a los Documentos Públicos. <https://rm.coe.int/1680084826>.
- Corte Interamericana de Derechos Humanos (Corte IDH). (18 de octubre 2023). Caso Miembros de la Corporación Colectivo de Abogados “José Alvear Restrepo” vs. Colombia. Excepciones Preliminares, Fondo, Reparaciones y Costas. Sentencia Serie C. No. 506. https://www.corteidh.or.cr/docs/casos/articulos/serieC_506_esp.pdf.
- Declaración Europea sobre los Derechos y Principios Digitales para la Década Digital. (23 de enero de 2023). *Diario Oficial de la Unión Europea (DOUE)*. [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123\(01\)](https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32023C0123(01))
- Directiva 95/46/CE del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos. (24 de octubre de 1995) *Diario Oficial de las Comunidades Europeas*, L 281. <https://www.oas.org/es/sla/ddi/docs/Directiva-95-46-CE.pdf>
- Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio de 2000, relativa a determinados aspectos jurídicos de los servicios de la sociedad de la información, en particular el comercio electrónico en el mercado interior (Directiva sobre el comercio electrónico). (17 de julio de 2000). *Diario Oficial de las Comunidades Europeas*, L 178/1. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2000-81295>
- Directiva 2002/58/CE del Parlamento Europeo y del Consejo, 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas). (31 de julio de 2002). *Diario de las Comunidades Europeas*, L 201. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32002L0058>
- Directiva 2003/98/CE del Parlamento Europeo y del Consejo, 17 de noviembre de 2003, relativa a la reutilización de la información del sector público. (31 de diciembre de 2003). *Diario Oficial de la Unión Europea*, L 345/90. <https://www.boe.es/doue/2003/345/L00090-00096.pdf>.
- Directiva 2013/37/UE del Parlamento Europeo y del Consejo de 26 de junio de 2013, por la que se modifica la Directiva 2003/98/CE relativa a la reutilización de la información del sector público. (27 de junio de 2013). *Diario Oficial de la Unión Europea*, L 175/1. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=CELEX%3A32013L0037&qid=1762748562745>

- Directiva (UE) 2016/680 del Parlamento Europeo y del Consejo relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por parte de las autoridades competentes para fines de prevención, investigación, detección o enjuiciamiento de infracciones penales o de ejecución de sanciones penales, y a la libre circulación de dichos datos y por la que se deroga la Decisión Marco 2008/977/JAI del Consejo. (27 de abril de 2016). *Diario Oficial de la Unión Europea*, L 119/89. <https://www.boe.es/doue/2016/119/L00089-00131.pdf>
- Directiva (UE) 2016/681 del Parlamento Europeo y del Consejo relativa a la utilización de datos del registro de nombres de los pasajeros (PNR) para la prevención, detección, investigación y enjuiciamiento de los delitos de terrorismo y de la delincuencia grave. *Diario Oficial de la Unión Europea*, L 119/132. (27 de abril de 2016). <https://www.boe.es/doue/2016/119/L00132-00149.pdf>.
- Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, 6 de julio de 2016, relativa a las medidas destinadas a garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión. (19 de julio de 2016). *Diario Oficial de la Unión Europea*, L 194/1. <https://www.boe.es/doue/2016/194/L00001-00030.pdf>
- Directiva (UE) 2019/790 del Parlamento Europeo y del Consejo, 17 de abril de 2019, sobre los derechos de autor y derechos afines en el mercado único digital y por la que se modifican las Directivas 96/9/CE y 2001/29/CE. (17 de mayo de 2019). *Diario Oficial de la Unión Europea*, L 130/92. <https://www.boe.es/doue/2019/130/L00092-00125.pdf>.
- Directiva 2019/1024 del Parlamento Europeo y del Consejo, 20 de junio de 2019, relativa a los datos abiertos y la reutilización de la información del sector público. (26 de junio de 2019). *Diario Oficial de la Unión Europea*, L 175/56. <https://eur-lex.europa.eu/legal-content/ES/ALL/?uri=CELEX%3A32019L1024>
- Directiva (UE) 2019/1937 del Parlamento Europeo y del Consejo, 23 de octubre de 2019, relativa a la protección de las personas que informen sobre infracciones del Derecho de la Unión. (26 de noviembre de 2019). *Diario Oficial de la Unión Europea*, L 305. <https://www.boe.es/doue/2019/305/L00017-00056.pdf>.
- Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión, por la que se modifican el Reglamento (UE) 910/2014 y la Directiva (UE) 2018/1972 y por la que se deroga la Directiva (UE) 2016/1148 (Directiva SRI 2). (27 de diciembre de 2022). *Diario Oficial de la Unión Europea*, L 333/80. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-81963>.
- Organización de los Estados Americanos (OEA). (2012). Convenio No. 108 del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y Protocolo adicional al Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de

- carácter personal, a las autoridades de control y a los flujos transfronterizos de datos. <https://www.oas.org/es/sla/ddi/docs/u12%20convenio%20n%20108.pdf>.
- OEA. (2021). Principios actualizados sobre la privacidad y la protección de datos personales. OEA. https://www.oas.org/es/sla/cji/docs/Publicacion_Proteccion_Datos_Personales_Principios_Actualizados_2021.pdf.
- Organización de Naciones Unidas (ONU). (14 de diciembre de 1990). A/RES/45/95. Principios rectores sobre la reglamentación de los ficheros computadorizados de datos personales. <https://docs.un.org/es/A/RES/45/95>
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (2002). Directrices de la OCDE sobre la protección de la privacidad y los flujos transfronterizos de datos personales. <https://doi.org/10.1787/9789264196391-en>.
- OCDE. (2022). *Declaración sobre un futuro digital fiable, sostenible e inclusivo*. <https://legalinstruments.oecd.org/api/download/?uri=/public/f347ae7c-4e38-4e7a-8d29-af489cffb84e.pdf>
- Red Iberoamericana de Protección de Datos (RIPD). (s.f.) Quiénes somos. <https://www.redipd.org/la-red/quienes-somos>
- RIPD. (2017). *Estándares de protección de datos personales para los Estados Iberoamericanos*. https://www.redipd.org/sites/default/files/inline-files/Estandares_Esp_Con_logo_RIPD.pdf
- RIPD. (2019a) *Orientaciones Específicas para el Cumplimiento de los Principios y Derechos que Rigen la Protección de los Datos Personales en los Proyectos de Inteligencia Artificial*. <https://www.redipd.org/sites/default/files/2020-02/guia-orientaciones-espec%C3%ADficaproteccion-datos-ia.pdf>
- RIPD. (2019b) *Recomendaciones Generales para el Tratamiento de Datos en la Inteligencia Artificial*. <https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf>
- Reglamento (CE) 45/2001 del Parlamento Europeo y del Consejo, 18 de diciembre de 2000, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos comunitarios y a la libre circulación de estos datos. (21 de enero de 2001). *Diario Oficial de las Comunidades Europeas*, L 8/1. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32001R0045&qid=1762745231700>
- Reglamento (UE) 2016/679 del del Parlamento Europeo y del Consejo, 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos). (4 de mayo de 2016). *Diario Oficial de la Unión Europea*, L 119/1. <https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32016R0679&qid=1762747577783>
- Reglamento (UE) 2022/868 del Parlamento Europeo y del Consejo, 30 de mayo de 2022, relativo a la gobernanza europea de datos y por el que se modifica el

- Reglamento (UE) 2018/1724 (Reglamento de Gobernanza de Datos). (3 de junio de 2022). *Diario Oficial de la Unión Europea*, L 152/1. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2022-80835>.
- Reglamento (UE) 2018/1724 del Parlamento Europeo y del Consejo, 2 de octubre de 2018, relativo a la creación de una pasarela digital única de acceso a información, procedimientos y servicios de asistencia y resolución de problemas y por el que se modifica el Reglamento (UE) 1024/2012. (21 de noviembre de 2018). *Diario Oficial de la Unión Europea*, L 295/1. <https://www.boe.es/doue/2018/295/L00001-00038.pdf>.
- Reglamento (UE) 2018/1725 del Parlamento Europeo y del Consejo, 23 de octubre de 2018, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones, órganos y organismos de la Unión, y a la libre circulación de esos datos, y por el que se derogan el Reglamento (CE) 45/2001 y la Decisión 1247/2002/CE (21 de noviembre de 2018). *Diario Oficial de la Unión Europea*, L 295/39. <https://www.boe.es/buscar/doc.php?id=DOUE-L-2018-81849>.
- Reglamento (UE) 2022/1925 del Parlamento Europeo y del Consejo, 14 de septiembre de 2022, sobre mercados disputable y equitativos en el sector digital y por el que se modifican las Directivas (UE) 2019/1937 y (UE) 2020/1828 (Reglamento de Mercados Digitales). (12 de octubre de 2022). *Diario Oficial de la Unión Europea*, L 265/1. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R1925>.
- Reglamento (UE) 2022/2065 del Parlamento Europeo y del Consejo, 19 de octubre de 2022, relativo a un mercado único de servicios digitales y por el que se modifica la Directiva 2000/31/CE (Reglamento de Servicios Digitales). (27 de octubre de 2022). *Diario Oficial de la Unión Europea*, L 277/1. <https://eur-lex.europa.eu/legal-content/ES/TXT/?uri=celex%3A32022R2065>.
- Reglamento General de Protección de Datos (RGPD). (14 de abril de 2016). <https://gdpr-info.eu/>
- Secretaría General Iberoamericana (SEGIB). (14 y 15 de noviembre de 2003). XIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Declaración de Santa Cruz de la Sierra-Bolivia. <https://www.segib.org/wp-content/uploads/2024/07/DeclaraciondeSantaCruz.pdf>
- Secretaría General Iberoamericana (SEGIB). (8 y 9 de diciembre de 2014). XXIV Cumbre Iberoamericana de Jefes de Estado y de Gobierno. Declaración de Veracruz-México. <https://www.segib.org/wp-content/uploads/2025/09/Resolucion-Veracruz.pdf>
- Téllez Valdés, J. (2013). *Lex cloud computing. Estudio jurídico del cómputo en la nube en México*. UNAM, IIIJ. <https://archivos.juridicas.unam.mx/www/bjv/libros/7/3249/1.pdf>.
- Tribunal Constitucional de España (TCE). (1983). Sentencias. *Boletín de Jurisprudencia Constitucional* (33), enero 1984, 126-170. https://app.congreso.es/est_bjc/

BIBLIOGRAFÍA COMPLEMENTARIA

- Carta de los Derechos Fundamentales de la Unión Europea (CDFUE) (2000/C 364/01). (7 de diciembre de 2000). *Diario Oficial de las Comunidades Europeas*. https://www.europarl.europa.eu/charter/pdf/text_es.pdf
- Organización de los Estados Americanos (OEA). (2015). *Guía legislativa sobre la privacidad y la protección de datos personales en las américas*. https://www.oas.org/es/sla/ddi/docs/proteccion_datos_personales_Guia_Legislativa_CJI.pdf.
- Organización para la Cooperación y el Desarrollo Económicos (OCDE). (23 September 1980). Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data. <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0188>
- OCDE. (2013). *Recommendation on Digital Security Risk Management for Economic Operators*. https://www.oecd.org/content/dam/oecd/en/publications/reports/2015/10/digital-security-risk-management-for-economic-and-social-prosperity_glg5c3dc/9789264245471-en.pdf

CAPÍTULO XI

Revista *Abogacía*: divulgación jurídica, democracia y derechos humanos

*Mateo Mansilla-Moya*¹

*Ivana Paredes Calderón*²

SUMARIO: XI.1. Reflexiones preliminares; XI.2. Derecho al acceso a la información y revistas de divulgación jurídica; XI.3. Revista *Abogacía* y acceso a la información; XI.4. Notas para continuar con la reflexión.

RESUMEN: Las reflexiones compartidas en este texto tienen como eje rector el papel que juegan las publicaciones periódicas de divulgación jurídica –particularmente a partir de la experiencia y las reflexiones suscitadas en la conformación de la revista *abogacía*– en la construcción de la democracia, en el fortalecimiento del Estado de derecho y en el respeto y garantía de la cultura de la legalidad y de la justicia, como un mecanismo para promover y garantizar el ejercicio de los derechos a la libertad de pensamiento, opinión y expresión, y el acceso a la información.

XI.1. REFLEXIONES PRELIMINARES

El respeto, la promoción, la protección y la garantía de los derechos humanos no pueden reducirse a una obligación constitucional (jurídica) de las autoridades del Estado. Los derechos humanos tienen una relevante dimensión horizontal que sirve como guía para la configuración de relaciones interpersonales a partir de parámetros éticos determinados. En este sentido, el actuar de quienes integran una comunidad, ya desde la sociedad civil, ya desde el sector privado, ya desde el sector público, debe estar determinado por los valores que han resuelto proteger a través del pacto político fundacional que los integra como una comunidad política afin. En el caso de nuestra comunidad, los valores acordados –y contruidos en torno a la noción de la *dignidad*– se manifiestan bajo la categoría política/jurídica/ética *derechos humanos*.

¹ Mateo Mansilla-Moya. Director de la revista *abogacía*. Profesor en la Facultad de Derecho de la Universidad Nacional Autónoma de México. Integrante del Consejo Consultivo del Mecanismo de Protección Integral de Personas Defensoras de Derechos Humanos y Periodistas de la Ciudad de México.

² Ivana Paredes Calderón. Estudiante de Derechos Humanos y Gestión de Paz en la Universidad del Claustro de Sor Juana. Integrante del equipo editorial de revista *abogacía*.

Los derechos humanos, como uno de los múltiples discursos que existen en torno a la dignidad, al ser el que ha sido adoptado por la Constitución Política y, por ende, por las estructuras jurídica y política del país, es el que se ha tornado eje rector de las relaciones entre las autoridades estatales (tanto de los tres poderes tradicionales y los órganos constitucionales autónomos, como de los tres órdenes de gobierno) con las personas que habitan o transitan por el territorio –los derechos humanos, entendidos en su dimensión de derechos positivos, se reducen, en la mayoría de los casos, a quienes gozan de la categoría de *ciudadanía* (habiendo cumplido con los requisitos constitucionales y el reconocimiento del Estado)–. No obstante, este discurso, en un sentido más amplio, y como guía ética para la configuración de las relaciones entre personas, no se reduce a la cuestión de la ciudadanía, también de las personas entre sí y de éstas con su entorno; sobre todo, a partir de la adhesión de nociones como derechos ambientales a los denominados Derechos Económicos, Sociales y Culturales (ahora, DESCAs).

A partir de lo anterior, y tomando en consideración el contexto específico de México (los fuertes –pero insuficientes– esfuerzos institucionales y normativos por transitar al ideal democrático desde hace más tres décadas, las crecientes y generalizadas violaciones de los derechos humanos, la escalada de violencias política y criminal, la reconfiguración de la tradicional división de poderes, los reduccionismos dicotómicos y la visceralidad política, las inercias en la praxis política propias de la dictablanda del siglo XX, la falta de cultura política y de sociedad civil organizada), en revista *abogacía* nos hemos planteado cuestiones concretas sobre el papel que desempeñamos como medio de divulgación jurídica que allega a las personas información que impacta tanto sus decisiones (en las esferas privada y pública) como sus vidas.

Este texto recoge algunas de las reflexiones que hemos hecho desde el equipo editorial y las aterriza en lo relativo al derecho humano de acceso a la información, en un esfuerzo conjunto con el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX) por invitar a la reflexión crítica y la labor divulgativa sobre estos tópicos en nuestro compromiso institucional por la promoción, respeto y garantía de los derechos humanos con los que trabajamos en un marco de institucionalidad democrática. Las reflexiones aquí presentes, pueden trasladarse a otros derechos conexos e igual de importantes para el fortalecimiento de la democracia, como la verdad, la memoria y la justicia. Pero al respecto escribiremos en otros espacios.

Este trabajo busca alcanzar dos objetivos. El primero, reflexionar sobre la función social de las revistas de divulgación jurídica para lograr dimensionar adecuadamente el rol sustancial que juegan en la construcción del Estado de derecho, en la concreción de la democracia y en el sostenimiento de un régimen de derechos humanos; el segundo, compartir el trabajo que se ha realizado desde la revista *abogacía* para convertir a la publicación en un universo de sentido humanista, inserto en un contexto de derechos humanos, que sirva como plataforma de diálogo democrático y de acceso a la información.

Partimos de la premisa que empieza a asomarse en este apartado: las empresas privadas desarrollamos un rol sustancial en la protección, promoción, respeto y garantía de los derechos humanos. Así, pues, la existencia de *abogacía* como medio de comunicación y, particularmente, como plataforma de divulgación jurídica y de diálogo reflexivo, crítico y propositivo, en una comunidad que adopta los valores humanistas en su tránsito a una democracia, ha posibilitado que se asuma como un agente más en la divulgación de los derechos humanos, en la reflexión situada sobre su realidad y el carácter propositivo para su mejora, en el fortalecimiento de la institucionalidad y en un mecanismo (privado) garante del derecho de acceso a la información.

XI.2. DERECHO AL ACCESO A LA INFORMACIÓN Y REVISTAS DE DIVULGACIÓN JURÍDICA

El acceso a la información es un derecho llave; su ejercicio abre la puerta al de otros derechos humanos: las libertades de pensamiento, opinión, expresión, asociación y agrupación, la participación política (a través del ejercicio del voto o de la participación en cargos de representación popular), los derechos a la verdad y la memoria, entre otros; todos éstos son esenciales para la consolidación de un régimen democrático.

Si bien el derecho de acceso a la información tiene una dimensión pública que supone que todas las personas pueden

[...] solicitar gratuitamente la información generada, administrada o en posesión de las autoridades públicas –poder ejecutivo, poder legislativo, poder judicial, órganos desconcentrados, descentralizados y autónomos, fideicomisos y fondos públicos, partidos políticos, cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad–, quienes tienen la obligación de entregarla sin que la persona necesite acreditar interés alguno ni justificar su uso. (INFO CDMX, s.f.),

Este derecho también tiene una dimensión privada –que se adelanta en las reflexiones preliminares de este texto–: la posibilidad de que la gente se pueda allegar de la información que se genere o administre por entes distintos a los públicos, como la de los espacios académicos y la de los medios de comunicación, y que sean sustanciales para la participación en los espacios y las decisiones de carácter público. En este sentido, y a partir de las acciones concretas que se han realizado desde la revista *abogacía*, pensamos a las publicaciones periódicas de divulgación jurídica (también las de naturaleza privada) como instrumentos que garantizan derechos humanos y como elementos producto y productores de la democracia al ser garantes del acceso a la información.

Cuando el equipo editorial de la revista nos sentamos a imaginar el contenido de la publicación y a marcar ruta de acción, nos gusta volver a un símil que Ginés Cutillas le compartió a Óscar Esquivias –ambos directores de revistas literarias en España– en una creativa y reflexiva conversación epistolar que sostuvieron y que, posteriormente, fue publicada en la prestigiada revista española *Cuadernos Hispanoamericanos* en 2024; en una carta, Ginés compartió a Oscar:

Fundar una revista se parece a fundar una ciudad: uno crea un ágora, allí se reúne gente, se crean relaciones y se levantan edificios de letras e imágenes, con una estética reconocible, porque cada revista acaba teniendo una identidad propia. (Miles, 2024, p. 45)

Y es que hacer una revista de divulgación jurídica no se reduce a reunir textos para su publicación. El hecho de que las voces y las plumas de quienes están reflexionando temas relevantes para lo jurídico y lo político, genera un ágora, una plataforma de diálogo donde los textos ya no existen de forma aislada e inconexa, sino que, por el contrario, lo hacen en diálogo con los de otras personas y en contextos determinados. Así, pues, la publicación-ciudad erige ideas y opiniones como edificios en forma de entrevistas, artículos, reseñas, columnas, poemas e imágenes que se conjugan en el espacio de la publicación, y la convierten en un universo entero de sentido. Justo ahí, en esa ciudad, se replica el ideal de comunidad al que aspiramos donde la revista está siendo producida: una comunidad democrática que se rige por los valores que protegen los derechos humanos: pluralidad, respeto, igualdad, paz y justicia.

Las revistas de divulgación jurídica, a diferencia de las publicaciones de difusión –que están dirigidas principalmente a las personas del gremio que las produce–, tienen como objetivo acercar un conocimiento especializado a todos los integrantes de la comunidad, independientemente de su formación académica o de sus conocimientos previos. En este sentido, los textos que se publican, a pesar de su rigor metodológico y académico, establecen limitaciones en cuanto al uso del lenguaje, la redacción y la extensión de los textos que publican con el objetivo de facilitar la legibilidad a la mayor cantidad posible de personas.

Las publicaciones de esta naturaleza desempeñan un rol sustancial en la construcción de la democracia al servir como plataformas de acceso a la información, divulgación de opiniones y puente de diálogo en torno a los tópicos coyunturales que inquietan a la comunidad en determinados contextos sociales, políticos y económicos. Independientemente de los tópicos que se abordan en estas revistas, lo que se divulga es de interés público; en este sentido, también sirven como plataformas de la democracia porque acercan a la comunidad a lo que acontece en la esfera pública. Dice Jesús Galindo Cáceres que “existe una relación entre la cultura de la información y la cultura política, pues hay un paquete de información que se relaciona con el interés público, el cual afecta en sus referencias y consecuencias implicadas a toda la

población o a una mayoría significativa” (como se citó en Escalera Zúñiga, 2023, p. 5). Así mismo, tienden a promover, a través del análisis crítico, la reflexión sobre el mundo jurídico y la cultura de la legalidad. La cultura de la legalidad se refiere a la forma en la que las personas se vinculan conscientemente entre sí y con su entorno en atención a las normas jurídicas positivas, tomando en consideración el bien común y las implicaciones que las acciones u omisiones personales tienen en la colectividad –reconociéndose, a sí mismas, como parte de algo más grande–.

El contenido de este tipo de publicaciones está determinado por el contexto coyuntural en el que la publicación se inserta, e involucra en sus páginas –a través de artículos, entrevistas, columnas de opinión, reseñas– a operadores jurídicos que se desenvuelven en diversidad de entornos: académicos, litigantes, jueces, legisladores, activistas de derechos humanos, estudiantes, entre otros. Cabe destacar aquí, que la inclusión de la pluralidad de plumas es, en sí misma, una práctica democrática, pues representan la polifonía de la sociedad, de espacios de enunciación particulares que se expresan desde su propia experiencia de vida y desde sus posturas políticas y culturales. La convergencia de la diversidad de perspectivas en un mismo espacio posibilita el diálogo y el acceso a información y visiones diversas en torno a tópicos similares, poniendo al alcance de los lectores información plural para que puedan tomar decisiones informadas y razonadas a partir de posturas fundadas y contrastadas.

Al ser publicaciones que toman el pulso de la comunidad que las conforma, son también espacios que recogen la memoria de la sociedad. La información aquí publicada se vincula con la actitud de las sociedades hacia el control, el conocimiento, la cultura, la política y la educación (Escalera Zúñiga, 2023, p. 5). La posibilidad de que las personas puedan acceder a las opiniones y reflexiones sobre lo que aconteció en momentos determinados de la historia de su comunidad, implica también la posibilidad de que construya sentido en torno a lo relativo al Estado democrático y social de derecho.

Estas publicaciones también aportan elementos culturales importantes para el desarrollo de conocimientos vinculados con la educación, la sociedad, la geografía, la política, la economía, los problemas mundiales y la diversidad de expresiones artísticas –la revista *abogacía, la voz y pluma de los juristas* publica, en cada una de sus ediciones, poemas y reseñas y análisis de cine, música y literatura; también dialoga con artistas (pintores, músicos, escritores, entre otros) sobre su obra–, que fortalecen el conocimiento integral y, también, las habilidades de sensibilidad y empatía³ hacia las demás personas, necesarias para la protección de su dignidad (y, por ende, para la materialización del discurso de los derechos humanos).

³ No es objeto de este estudio ahondar en este punto. Sin embargo, resulta relevante destacar que los estudios de literatura neurocognitiva han demostrado el impacto que tiene en los procesos neurocognitivos de los lectores la lectura de literatura de ficción o poética a contraposición de los efectos que tiene la lectura de textos académicos, resultando los primeros motores del desarrollo, en el cerebro, del área en la que se encuentran las neuronas “espejo”, las que funcionan para la empatía.

XI.3. REVISTA *ABOGACÍA* Y ACCESO A LA INFORMACIÓN

Hay algunos matices que hay que considerar para respaldar el argumento anterior, pues el hecho de que exista una publicación periódica no necesariamente implica que, a través de ésta la comunidad pueda acceder a la información y se garanticen los derechos anteriormente referidos. Entre otros, es de suma importancia que quienes editan la publicación tengan consciencia de la dimensión protectora y garantista que puede tener su medio, lo que conlleva a un ejercicio responsable de la edición en atención al impacto que puede tener en la comunidad, en la democracia y en el Estado de derecho.

Al servir como mecanismo para la protección de los derechos antes aludidos, la revista de divulgación jurídica se convierte, a su vez, en un espacio propicio para el desarrollo de prácticas democráticas, así como para la promoción y garantía de derechos humanos.

En revista *abogacía* hemos emprendido acciones concretas para que la publicación periódica sirva como un medio que coadyuve, a través del acceso a la información, a la construcción de la democracia, la divulgación de la cultura de derechos y de justicia.

En el sentido de la democracia, hemos adoptado los valores que la sostienen y hemos publicado una pluralidad de voces derivadas de las múltiples experiencias de vida que aportan al diálogo democrático en diversidad de códigos. Aunado a ello, este medio ha roto un cerco académico elitista, mediante la invitación a voces que son disruptivas y valiosas en materia de derechos humanos y justicia. Igualmente, ha traducido un lenguaje cerrado, que se cree pertenece exclusivamente a quienes tienen el saber legítimo sobre cómo funciona formalmente el derecho. Fuera de los marcos normativos, el derecho también existe en las calles, en las comunidades y en los mismos cuerpos. Ha servido para enlazar conceptos como violencia, justicia, movimientos sociales, historia y memoria con el derecho en su dimensión social y cultural.

Esto también facilita un ejercicio de justicia epistémica (Fricker, 2017), es decir, no se invalidan los saberes que se encuentran fuera del ámbito académico jurídico, y se reconoce a las personas ajenas al gremio que contribuyen al debate político y social. La influencia de los saberes indígenas, feministas, barriales y populares, que también poseen un amplio conocimiento y que crean nuevas formas y juegan un papel sustancial en la defensa de los derechos humanos, aporta igualmente a la erosión del derecho hegemónico.

En la era contemporánea, en donde la hegemonía ha perdido fuerza por el levantamiento de nuevos cuerpos y nuevas identidades, hay una necesidad de reflexionar acerca del “cómo hacer” de diferentes maneras, que influya repensar lo que ya creíamos pensado. La información aparte de ser útil debe ser incómoda y disruptiva.

Desde *abogacía*, asumimos la responsabilidad de contribuir al libre ejercicio del derecho, al acceso a la información. Sin embargo, es necesario reconocer que el conocimiento jurídico suele estar restringido, lo que reproduce jerarquías dentro del

sistema legal y, por ende, excluye a personas y comunidades ajenas al gremio. La democratización de la información jurídica es un acto de defensa para el público. Esto nos hace conscientes de que poseemos un dominio sobre esta información y, con ello, la capacidad de construir realidades. Nosotros hemos decidido ejercerlo como un vehículo de transformación, en donde se rompen barreras para reproducir estas dinámicas de poder y se comprende, se apropia y se disputa el lenguaje del derecho.

El derecho al acceso a la información debe ser igualitario, lo que implica no solo la disponibilidad de contenidos, sino su comprensibilidad y relevancia. ¿De qué sirve acceder a la información jurídica, si esta permanece en un lenguaje técnico que muchas personas no pueden interpretar? Lo valioso de *abogacía* es que habilita otras formas de acercarse al derecho: formas que reconocen distintos modos de pensar, de aprender y de nombrar la justicia. Es un espacio que no solo pretende informar, sino que invita a la reinterpretación y expande la imaginación jurídica que permite que diferentes mentes encuentren sentido en lo legal. Aparte de velar por los marcos normativos, la revista nos da la oportunidad de explorar las habilidades de comunicación entre individuos y conocer un derecho de territorio, no de escritorio.

XI.4. NOTAS PARA CONTINUAR CON LA REFLEXIÓN

El constitucionalismo, la democracia y los derechos humanos nos competen a todos quienes conformamos una comunidad política. De ahí que nuestra existencia en tal comunidad se ajuste a las relaciones y las normas ahí determinadas; de ahí, también, que lo que se haga sirva para posibilitar su permanencia y la supervivencia de sus integrantes. En este sentido, cabe concluir que la existencia tanto de una profesión (como la jurídica) y de medios de divulgación jurídica, sirvan a los fines que se plantea la propia comunidad; es decir, que sirvan a fines sociales más amplios que los intereses privados.

Una revista de divulgación jurídica, como se ha reflexionado desde *abogacía*, en el contexto mexicano, debe servir a los fines sociales que conllevan la protección de los valores democráticos y de derechos humanos. En este sentido, deben configurarse como modelos de dichos valores: publicaciones polifónicas, democráticas, respetuosas, reflexivas, críticas y propositivas. Deben, a su vez, configurarse como mecanismos para el ejercicio de los derechos humanos, como el acceso a la información.

REFERENCIAS

- Escalera Zúñiga, L. I. (2023) Archivos: guía para alcanzar la utopía. En A. Barnard Amozurrutia y L. L. Enríquez Rodríguez (coords.). *Perspectivas y novedades en el ámbito de la archivística*. Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX); Porrúa.
- Fricker M. (2017) *Injusticia epistémica: el poder y la ética del conocimiento*. (R. García Pérez trad.) Herder.
- Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX) (s.f.), Solicita información pública. ¿Qué es el Derecho de Acceso a la Información Pública? <https://infocdmx.org.mx/index.php/solicita-informacion-publica/que-es-el-acceso-a-la-informacion-publica.html>
- Miles, V. (Coord). (junio, 2004) Óscar Esquivias y Ginés Cutillas: “Las revistas literarias como clima de conversación y propuesta estética moral”. *Cuadernos Hispanoamericanos*. 886. 44-49. <https://cuadernoshispanoamericanos.com/oscar-esquivias-y-gines-cutillas-las-revistas-literarias-como-clima-de-conversacion-y-propuesta-estetica-y-moral/>

CAPÍTULO XII

El conocimiento como presupuesto de la libertad: un breve análisis

Diego Bernal Toriello¹

SUMARIO: XII.1. Preámbulo; XII.2. El conocimiento; XII.3. La libertad; XII.4. La relación entre el conocimiento y la libertad; XII.5. Importancia del derecho a conocer; XII.6. Conclusión

PALABRAS clave: Libertad, derecho a conocer, conocimiento, decidir, acceso a la información, información pública.

XII.1. PREÁMBULO

El 11 de junio de 2013 se publicó el Decreto por el que se reforman y adicionan diversas disposiciones de los artículos 6o., 7o., 27, 28, 73, 78, 94 y 105 de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), en materia de telecomunicaciones en el *Diario Oficial de la Federación*. En virtud de ese decreto, entre otras modificaciones, se adicionó el segundo párrafo del artículo 6o. de la Constitución Federal, en el que se reconoció que toda persona “[...] tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión” (CPEUM, art. 6o.).

Unos años después, en la Ciudad de México, en términos de los artículos 6o., fracciones V y XVII; 73, fracción IX, y 101, fracción VI, de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, publicada en la *Gaceta Oficial de la Ciudad de México* el 6 de mayo de 2016, que en adelante se referirá como la Ley de Transparencia, se estableció que corresponde a los Comisionados y Comisionadas del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, promover, difundir y velar que las personas conozcan y ejerzan sus derechos de acceso libre a la información.

¹ Abogado por la Escuela Libre de Derecho y maestrando en Derecho Constitucional por la misma institución. Socio fundador de Bernal Toriello y García Vázquez Abogados S.C.

El derecho de acceso a la información, que en adelante identificaré como el derecho a conocer, ya había sido reconocido en otras instancias y latitudes, previo a ser regulado en México. Por ejemplo, la Opinión Consultiva OC-5/85 de la Corte IDH, de fecha 13 de noviembre de 1985, reconoce que con fundamento en los artículos 13 y 29 del Pacto de San José, en toda sociedad democrática deben proliferar las posibilidades de circulación de noticias e información (párr. 69).

A su vez, el Pacto Internacional de Derechos Civiles y Políticos (PIDCP), al cual México se adhirió el 24 de marzo de 1981, prevé en su artículo 19 el derecho de toda persona a “[...] la libertad de expresión; este derecho comprende la libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras [...]” (PIDCP, 1966, art. 19.2).

En suma, durante el siglo XX hubo un sólido reconocimiento internacional del derecho a conocer, el cual se reflejó en nuestro país; primero, mediante la suscripción de tratados internacionales en la materia, y después, en la adopción de ese derecho en normas domésticas.

El derecho a conocer es, a mi consideración, un instrumento que sirve para ejercer los múltiples derechos y libertades reconocidos en el bloque de constitucionalidad, de manera informada.

El objetivo del presente artículo es exponer, en primer lugar, la estrecha relación entre la libertad y el conocimiento. En segundo lugar, se abordará la relevancia del conocer para efectos de la adopción de decisiones y en el ejercicio de derechos. Se analizarán algunos antecedentes históricos relevantes para entender los conceptos de conocimiento y de libertad, así como su relación, y la injerencia de ambos en la adopción informada de decisiones.

XII.2. EL CONOCIMIENTO

En este artículo no pretendo abundar en las características ni historia del conocimiento, sino exponer sucintamente algunas ideas que se han formulado a lo largo de la historia, para llegar a una sencilla conclusión sobre él.

En la actualidad es generalmente aceptado que existen distintas clasificaciones y tipos de conocimiento, por ejemplo, matemático, intuitivo, lógico, empírico, científico, religioso, de primero o segundo grado, etcétera. De todas estas especies, me interesa abordar el conocimiento científico.

Abbagnano afirmó que el conocimiento “[...] significa llegar a la presencia del objeto, apuntar a él o, con el término preferido de la filosofía contemporánea, *trascender* a él.” (Abbagnano, 1974, p. 222). Al exponer la postura de Kant, afirmó que el conocimiento es “[...] el acto de reunir diferentes representaciones y comprender su multiplicidad [...]” (Abbagnano, 1974, p. 224).

Platón sostuvo, en el siglo IV a.C., que el conocimiento es una creencia debidamente justificada. Para el griego no toda idea era conocimiento, pues distinguió las opiniones del conocimiento (Corilla, B., *et al.*, 2022).

Kant (2005), durante el siglo XVIII, retomando ideas de Descartes, afirmó que el conocimiento se configura dentro de la mente del sujeto que razona. En este sentido, la sensibilidad es el rasgo humano que permite representar el conocimiento en la mente y, por lo tanto, conocer (pp. 27-48). El prusiano identificó el conocimiento *a priori* como aquel asido sin haber aprendido por la experiencia, y formulado a través de la representación de la mente, asimismo, escribió sobre el conocimiento *a posteriori*, adquirido a través de las experiencias (Kant, 2005, pp. 107-108). Así, Kant distinguió entre el conocimiento que se formula de forma meramente intelectual, del obtenido empíricamente.

Por su parte, Hegel propuso que el conocimiento proviene de la consciencia de espíritu, la cual está compuesta, en su parte más primaria, de razón y de autoconsciencia. Para Hegel, la realidad es dialéctica, y la filosofía engloba al conocimiento absoluto. Ese conocimiento es asequible mediante un proceso dialéctico en que entran en tensión la razón, la consciencia del espíritu y la certeza sensible (Hegel, 1973). Hegel sostuvo que conocer es un proceso que unifica al mundo subjetivo, propio del espíritu, con el mundo objetivo o tangible, o, en otras palabras, el conocimiento lleva lo objetivo a la consciencia (Abbagnano, 1974, p. 220).

En la actualidad, se admite que la epistemología es la rama de la filosofía que estudia los problemas que atañen a la obtención y validez del conocimiento científico. Abbagnano define a la epistemología la teoría del conocimiento. (Abbagnano, 1974, pp. 227 y 228)

Se puede entender al conocimiento como la relación de la conciencia humana consigo misma, frente al objeto que se hace presente. Los procesos de conocimiento tienden a establecer las condiciones que permiten hacer posible la presencia del objeto o, en todo caso, preverla (Abbagnano, 1974, pp. 221-222). Entonces, en términos sencillos, el conocimiento es la representación intelectual del objeto, lo cual presupone la interacción o análisis suficiente del objeto conocido. En consecuencia, para conocer, es necesario que haya un acercamiento al objeto.

XII.3. LA LIBERTAD

En el siglo IV a.C., Aristóteles afirmó que las personas “actúan”, a diferencia de los animales, que solamente reaccionan a estímulos. La actuación humana, para el Estagirita, conlleva la planeación y la elección (Aristóteles, 1985, pp. 178-207). Mientras que los animales reaccionan programática e instintivamente, las personas actúan actuando y modelando la realidad, y no solo reaccionando a ella.

Los textos bíblicos prevén que nada puede suceder sin que Dios lo permita (1 Sm. 14:45; Lc. 21:18). Entonces, la libertad humana para tomar decisiones está, realmente, sujeta a la voluntad divina (Js. 1:8).

Para el siglo IV, Agustín de Hipona, al interpretar los textos bíblicos, pareció identificar la razón pragmática de la humanidad (Libro V), pero como sostiene Concha Roldán (2005) “[...] su explicación de la historia universal es esencialmente religiosa, en el sentido de que deriva su luz de la revelación” (p. 40). Así, si bien el Doctor de la Gracia amagó con defender la autonomía de la actuación humana, terminó concluyendo que las personas adoptan decisiones encaminadas a cumplir el deseo divino, sean o no conscientes de ello.

En el siglo XIV, Giovanni Pico Della Mirandola, un pensador italiano, sostuvo que los seres humanos, por ser hijos de Dios, gozan de libre albedrío regalado por el Creador (Pico della Mirandola, 2006, p. 8). En ejercicio de ese libre albedrío, las personas tienen la libertad de inventarse y darse forma a sí mismas (Savater, 2016, p. 22). Así, Pico della Mirandola concibió que, en virtud de la dignidad humana, las personas pueden ejercer el libre albedrío para configurar su identidad, no obstante, la fuente de esa dignidad es divina (Pico della Mirandola, 2006, pp. 9-30).

Entre los siglos XVII y XVIII, Giambattista Vico defendió que el rasgo común de las naciones es ser dirigidas por la Providencia, retomando algunas ideas de Agustín de Hipona. Vico concibió la Providencia como “[...] el ordenamiento de las cosas hacia un fin” (Matute Aguirre, 2023, p. 52). En la especie, para él se trataba de un fin divino. Entonces, tal como en el caso de San Agustín, concibió a la libertad de elección de las personas como circunscrita a la voluntad de Dios, de modo que no existe un verdadero libre albedrío (Matute Aguirre, 2023, p. 53-55).

En el siglo XIX, Voltaire, inspirado por el espíritu de la Ilustración, criticó los mitos religiosos. A lo largo de su libro *Filosofía de la historia*, Voltaire se dedicó a desarticular los acontecimientos de las narraciones bíblicas, intentando demostrar que la voluntad de las personas no estaba sometida al yugo celestial. Por ejemplo, al abordar la narración de la creación del mundo, el francés abundó en explicaciones racionales y conjeturas sobre cómo llegaron los autores del Génesis a escribir tales hechos (Voltaire, 2000, pp. 26-28). Sin embargo, Voltaire atribuyó el destino de la humanidad a otro factor, semejante a la Providencia, pero ahora secular, llamado Progreso (pp. 52-55). Conforme a este “nuevo” hilo conductor de la historia, las decisiones humanas se rigen por una orientación predeterminada al avance científico.

Rousseau, contemporáneo de Voltaire, sostuvo que la perfectibilidad humana se basa en la educación, en contraposición a la corrupción humana devenida de la ignorancia. (Savater, 2015, p. 24)

A mediados del siglo pasado, Hannah Arendt (2016) sostuvo, de forma semejante a Aristóteles, que las personas pueden mostrarse a sí mismas a través de la acción (pp.

199-255). Arendt, de origen judío, vivió las crueldades del nazismo en Alemania, por lo que, como sostienen Srnicek y Williams (2017), para cuando escribió, ya había sido defraudada por las expectativas del Progreso del siglo XX (pp. 7-17).

Arendt no atribuyó el derecho de elegir a alguna fuente divina o metafísica. El mero hecho de ser persona otorga legitimación suficiente para tomar decisiones. La autora sostuvo que, en todo caso, las personas toman decisiones constreñidas por las consecuencias que éstas puedan generar, pero no obligadas por una fatalidad irresistible (Arendt, 2016, pp. 247-249).

Karl Popper (1992), contemporáneo de Arendt, expresó que las personas están en libertad de tomar decisiones, con las respectivas consecuencias sociales que conllevan, es decir, para él no existe una sola opción. Ni Dios, ni la Providencia, ni el Progreso constriñen la voluntad de las personas a decidir en determinado sentido (pp. 71-72).

Finalmente, en el siglo XXI, Fernando Savater (2015) sostuvo que la libertad es relativa debido a que el espectro de actuación del individuo libre se encuentra circunscrito, fácticamente, por su entorno (pp.15-25 y 39-51). Así, todas las personas pueden elegir en el espectro tan amplio como su contexto lo permita.

Así, en términos sencillos, la libertad se puede entender en sentido negativo, como la ausencia de coacción o presión para tomar decisiones. Quien es libre para tomar decisiones, toma las decisiones que quiere.

XII.4. LA RELACIÓN ENTRE EL CONOCIMIENTO Y LA LIBERTAD

Cobran vigencia las palabras de Jesús, cuando afirmó que “[...] conoceréis la verdad, y la verdad os hará libres” (Jn. 8:31). Jesús, naturalmente, hacía referencia a cuestiones teológicas. Sin embargo, su planteamiento es, pienso, universalmente válido. El conocimiento da libertad.

Piense el lector que sufre de una grave diarrea, y se le presentan dos medicamentos distintos para contrarrestarla. El primero está dentro de una caja verde, el otro, dentro de una caja roja. Siendo que no se conoce el contenido de las cajas, el lector escogerá por azar, superstición, etcétera. En el caso planteado, si el lector escogió la caja verde, murió, pues contenía una pastilla de purgante. Si eligió la caja roja se salvó, pues contenía un antidiarreico.

Por casos como el recién propuesto, es válido concluir que el conocimiento es un presupuesto para la elección en libertad. La libertad ejercida sin conocimiento del objeto es un mero azar.

Quien está más informado, o sea, quien goza de un conocimiento más robusto, está en posibilidad de escoger de forma más libre.

XII.5. IMPORTANCIA DEL DERECHO A CONOCER

La Constitución Federal prevé diversas garantías del derecho a conocer. Una de ellas, que estimo particularmente relevante, es la prevista en el artículo 6o. de la Carta Magna, apartado A), incisos I y III.

Conforme a la fracción I del artículo señalado, se considera pública toda información en posesión de autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos, así como de cualquier persona física, moral o sindicato que reciba y ejerza recursos públicos o realice actos de autoridad, en cualquier nivel de gobierno.

La fracción III prevé que toda persona, sin necesidad de acreditar interés o legitimación algunos, tiene acceso gratuito a la información pública. Este libre acceso a la información pública permite conocer cómo, cuándo y dónde han sido ejercido los recursos públicos. Asimismo, se puede indagar acerca de los efectos y resultados de ese ejercicio de recursos.

En lo que atañe al derecho a conocer, la Asamblea Legislativa de la Ciudad de México dio un paso adelante, e impuso a las autoridades en la materia el deber de promover, difundir y velar por que las personas conozcan y ejerzan dicho derecho. Ello, conforme a los artículos 6o., fracciones V y XVII; 73, fracción IX y 101, fracción VI de la Ley de Transparencia.

La Organización de Estados Americanos ha sostenido que:

El acceso a la información es una herramienta clave para fomentar mayor eficiencia y eficacia en las acciones del estado, especialmente en el manejo de recursos públicos y es esencial para la rendición de cuentas y la transparencia de sus operaciones. Asimismo, promueve mayor responsabilidad en el respeto y promoción de los derechos individuales [...]" (OEA, 2013, p. 9)

Lo anterior resulta lógico, pues en la medida de que las personas conozcan cuál ha sido el destino del erario, gozan de mayor libertad para ejercer sus derechos civiles y políticos. Pueden, por ejemplo, votar por la persona candidata y/o por los partidos políticos que acrediten dar resultados en los temas que son de su interés. Así, aplicando el análisis de Fernando Savater (2016), el panorama de actuación se abre en razón de que se conoce más (pp. 15-25 y 39-51).

El valor del derecho a conocer no se agota en el ejercicio de derechos políticos, sino que impacta todas y cualesquiera decisiones. Como lo sostuvo la OEA (2013), el derecho a conocer es instrumental, debido a que su ejercicio impacta el ejercicio de otros derechos, tales como los económicos, civiles, políticos y culturales, entre otros, dado que conocer permite adoptar decisiones informadas, mitigando riesgos y maximizando derechos y libertades (pp. 10-11).

XII.6. CONCLUSIÓN

Regresando al ejemplo de la caja verde y la caja roja, quien conozca el contenido de cada una de ellas podrá escoger la caja de su preferencia más libremente, que quien no lo conoce. Entonces, quien conoce el contenido de las cajas es verdaderamente libre para escoger, pudiendo representar de antemano los efectos y consecuencias de su decisión. Como lo dijo Jesús, el conocer la verdad te hace libre. Libre para elegir.

Concluyo con una sentencia puntual: si el lector ejerce su derecho a conocer se ensanchará su visión, estará informado y gozará de una libertad mayor para elegir.

REFERENCIAS

- Abbagnano, N. (1974). *Diccionario de filosofía* (2a. ed.). Fondo de Cultura Económica.
- Agustín de Hipona. *La ciudad de Dios*.
- Arendt, H. (2016). *La condición humana*. Paidós.
- Aristóteles. (1985). *Ética a Nicómaco* (J. Pallí Bonet, Trad.). Gredos.
- Constitución Política de los Estados Unidos Mexicanos (5 de febrero de 1917, última reforma publicada DOF 15 de abril de 2025).
- Corilla, B., García, G., Granados, A., Khoury, R., Limo, M. F., Román, M., Salas, M., Tapia, C., y Vilcarino, A. (traductores) (2022) Platón, Menón, 96d1-99b9. *Estudios de Filosofía*, 20, 83-93. <https://revistas.pucp.edu.pe/index.php/estudiosdefilosofia/article/view/26249/24660>
- Corte Interamericana de Derechos Humanos (Corte IDH). (13 de noviembre de 1985). Opinión consultiva OC-5/85 La colegiación obligatoria de periodistas (arts. 13 y 29 Convención Americana sobre Derechos Humanos) Serie A No. 5. <https://www.corteidh.or.cr/tablas/a12040.pdf>.
- Hegel, G. W. F. (1973). *Fenomenología del espíritu*. Fondo de Cultura Económica.
- Kant, I. (2005). *Crítica de la razón pura*. (trad. P. Ribas). Taurus.
- Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México. (6 de mayo de 2016). *Gaceta Oficial de la Ciudad de México* (última reforma. 26 de febrero de 2021). https://data.consejeria.cdmx.gob.mx/images/leyes/leyes/LEY_DE_TRANSPARENCIA_ACCESO_A_LA_INFORMACION_PUBLICA_Y_RENDICION_DE_CUENTAS_DE_LA_CDMX_5.1.pdf
- Matute Aguirre, A. (2023). *Lorenzo Boturini y el pensamiento histórico de Vico*. Universidad nacional autónoma de México, Instituto de Investigaciones Históricas. (Serie Novohispana 26).

- Organización de Estados Americanos (OEA). (2013). El acceso a la información pública, un derecho para ejercer otros derechos. <https://www.oas.org/es/sap/dgpe/concursoinformate/docs/cortosp8.pdf>
- Pacto Internacional de Derechos Civiles y Políticos (PIDCP). (16 de diciembre de 1966, entrada en vigor 23 de marzo de 1976). <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>
- Pico della Mirandola, G. (2006). *Discurso sobre la dignidad del hombre*. Editorial π.
- Popper, K. R. (1992). *La sociedad abierta y sus enemigos*. Paidós.
- Roldán, C. (2005). *Entre Casandra y Clío. Una historia de la filosofía de la historia*. Akal.
- Reina-Valera. (1960). B
- Santa Biblia. <https://www.biblegateway.com/passage/?search=1%20Samuel%2014&version=RVR1960>
- Savater, F. (2016). *El valor de elegir*. Ariel.
- Srnicek, N. y Williams, A. (2017). *Inventar el futuro. Poscapitalismo y un mundo sin trabajo*. Malpaso.
- Voltaire. (2000). *Filosofía de la historia*. Tecnos.

CAPÍTULO XIII

La participación ciudadana es la clave frente a la crisis de confianza y legitimidad en los tribunales mexicanos

Fátima Gamboa¹

SUMARIO: XIII.1. Preámbulo; XIII.2. En medio de una crisis de legitimidad y confianza; XIII.3. ¿Cómo mejoramos la participación ciudadana?; XIII.4. Nuestra propuesta, un modelo de justicia abierta feminista.

PALABRAS clave: Acceso a la justicia, independencia judicial, justicia abierta feminista, participación ciudadana.

XIII.1. PREÁMBULO

La participación ciudadana es esencial para crear un sistema de justicia más transparente e igualitario. Por eso, desde EQUIS Justicia para las Mujeres promovemos un modelo de Justicia Abierta Feminista, una propuesta que busca transformar los tribunales en instituciones más cercanas y confiables, que escuchen a la ciudadanía y que no dejen a nadie atrás. A lo largo de estas líneas veremos cómo estos mecanismos pueden fortalecer la independencia judicial y mejorar el acceso a la justicia para todas las personas, principalmente para las mujeres y poblaciones más vulneradas en México.

Hace nueve años, el presidente de un Tribunal me preguntó cómo imaginamos o entendíamos la participación ciudadana, porque no la veía ni posible ni viable dentro de los poderes judiciales. Nunca se había hablado de esto. Es decir, hace unos años, las dudas y la incredulidad aparecían cuando escuchaban hablar de participación ciudadana en el Poder Judicial, porque se creía que podía afectar a la neutralidad misma del sistema de justicia. Por eso, el trabajo de EQUIS Justicia para las Mujeres (en adelante EQUIS) con los poderes judiciales ha sido clave para dar sentido al concepto, para dibujar un nuevo panorama y mapear iniciativas existentes sobre el tema. Ha sido clave para que entiendan que la participación ciudadana está relacionada con la rendición de cuentas, con sistemas de anticorrupción, con la observación activa dentro de la política judicial, etc.

¹ Abogada maya, directora de EQUIS Justicia para las Mujeres, A.C. Maestra en Derechos Humanos por la Universidad Iberoamericana; y experta en derechos de los pueblos y mujeres indígenas por la Universidad Carlos III de Madrid. Ha publicado: *Reforma Judicial Feminista: Desmantelar las fábricas de injusticias*; *¿Por qué necesitamos una reforma judicial feminista?*; y *Justicia abierta feminista*.

En EQUIS buscamos garantizar el acceso a la justicia y transformar las estructuras de poder que perpetúan la opresión y exclusión. Desde 2015, hemos trabajado para fomentar y acompañar la creación de un sistema judicial más igualitario y transparente. Nuestra propuesta es un “Modelo de Justicia Abierta Feminista”. Este modelo propone tribunales que sean no solo eficientes, sino también participativos, asegurando que la voz de todas las mujeres sea escuchada (EQUIS, 2023b).

XIII.2. EN MEDIO DE UNA CRISIS DE LEGITIMIDAD Y CONFIANZA

En México, los poderes judiciales enfrentan una profunda crisis de legitimidad y confianza. Por un lado, la Encuesta Nacional sobre las Dinámicas de las Relaciones en los Hogares (ENDIREH) revela que 7 de cada 10 mujeres han experimentado violencia en algún momento de su vida, pero la mayoría no busca ayuda debido a la desconfianza en las instituciones y el miedo a la revictimización. Solo 27 de cada 1000 mujeres víctimas de violencia de pareja solicitan ayuda, cifra que empeora en el caso de violencia comunitaria, donde solo 8 de cada 1000 solicitan ayuda (Gamboa Estella, s.f., p. 5). Este grave déficit de confianza hacia las instituciones no es un dato menor, es una crisis estructural en el sistema, que lleva implícita una crisis de confianza en el sistema judicial.

La desconfianza se comprende al ver cómo las sentencias judiciales a menudo ignoran o minimizan la violencia de género. El análisis de más de 100 sentencias en el informe “No es Justicia” de EQUIS, mostró que un 47% de jueces/juezas invisibilizan las violencias, un 69% no protegen a las mujeres y un 86% no reparan integralmente los daños. (RCJ, 2021, pp. 15, 17 y 19). A esto se suma que la ciudadanía percibe a los jueces y juezas como la segunda autoridad más corrupta después de la policía de tránsito.

En cuanto a participación ciudadana, sí podemos decir que los datos han mejorado, pero sigue siendo insuficiente. Desde 2017, hemos preguntado a los tribunales si cuentan con mecanismos de participación ciudadana, observando una evolución en la conceptualización de estos mecanismos. En los primeros años, muchas respuestas reflejan una falta de comprensión sobre la participación ciudadana, como hemos evidenciado al inicio. Según el informe “(In)Justicia Abierta” de 2019, de Equis Justicia para las Mujeres, solo 2 de 32 poderes judiciales contaban con mecanismos de participación ciudadana reales y significativos.

El informe de 2023 reporta una notable mejora, pues el 53.1% de los tribunales reportan tener mecanismos de participación ciudadana, pero solo la mitad de estos son efectivos, y aún se percibe la confusión sobre lo que constituye una verdadera participación ciudadana, y por tanto la necesidad urgente de sensibilización y educación en este ámbito, pero también muestran una mejora en la inclusión de acciones que promueven el diálogo y la colaboración con la ciudadanía (EQUIS, 2023a. p. 17).

XIII.3. ¿CÓMO MEJORAMOS LA PARTICIPACIÓN CIUDADANA?

La participación ciudadana es la base sobre la cual descansa la legitimidad y democratización judicial

En EQUIS clasificamos los mecanismos de participación ciudadana en diferentes niveles:

- Primero. “Escuchar: recopilar las expresiones de la ciudadanía sobre un tema específico”.

Incluyen las encuestas de calidad de servicio y reuniones, tanto con barras de abogados/abogadas, cómo con academia y movimientos sociales, asociaciones de base y comunidades organizadas.

- Segundo. “Dialogar: Fomentar el diálogo bilateral entre ciudadanía y autoridades”.

Mesas de trabajo en materia de género y diálogos participativos son ejemplos de este nivel.

- Tercero. “Responder: Las autoridades responden a las inquietudes de la ciudadanía con compromisos o acciones concretas”.

Esto incluye la creación de proyectos específicos basados en las sugerencias de la comunidad.

- Cuarto. “Involucrar: Diversos actores participan activamente con sus recursos e ideas”.

Observatorios ciudadanos y jurados universitarios en procesos judiciales, son ejemplos de este nivel de participación (EQUIS, 2023a. p. 11).

Para que la participación ciudadana sea efectiva debe tomar en cuenta los cuatro niveles. Pero queremos señalar particularmente el cuarto nivel: *involucrar*, porque sigue siendo un reto importante: “De los 25 mecanismos reportados, el 72% se enfocan en asociaciones profesionales, mientras que solo tres incluyen colectivas y movimientos de víctimas”. Es vital que los tribunales amplíen su alcance para incluir a todas las voces, especialmente las más vulneradas e invisibilizadas en los espacios de toma de decisiones, y utilicen estrategias de difusión innovadoras para informar a la ciudadanía sobre las oportunidades de participación (EQUIS, 2023a, p. 24).

La participación debe fomentar la pluralidad de voces y estar dirigida a poblaciones diversas. Los poderes judiciales deben transitar a estrategias que involucren a colectivas, movimientos sociales, organizaciones de base, personas defensoras de derechos humanos y comunidades organizadas. Este acercamiento es fundamental para eliminar las prácticas discriminatorias y clasistas que pueden replicarse en los mecanismos de participación ciudadana.

El mayor reto que enfrentan los poderes judiciales en materia de participación ciudadana es el desconocimiento del alcance e importancia de estos mecanismos. Aunque “17 tribunales reportaron tener prácticas de participación, el análisis demuestra que no necesariamente lo que consideran participación ciudadana son mecanismos que acercan y toman en cuenta la voz de la ciudadanía” (EQUIS, 2023a, p. 25).

La sensibilización y capacitación son indispensables para que los poderes judiciales comprendan su importancia. Los mecanismos de participación ciudadana no deben ser vistos como una carga adicional, sino como una responsabilidad para dar acceso igualitario y sin discriminación a todas las personas.

“En la región de Latinoamérica encontramos ejemplos que demuestran que los poderes judiciales están poniendo como prioridad [...]” (EQUIS, 2023b, p. 35), la mejora del conocimiento de su labor entre la ciudadanía y abriendo espacios de participación y escucha. Un buen ejemplo son:

[Las] encuestas de necesidades jurídicas: Son metodologías y ejercicios de participación que buscan identificar los problemas de justicia que experimentan las personas en las demandas de servicios con un enfoque “de abajo hacia arriba”. Los datos que se obtienen con las encuestas permiten cuantificar y caracterizar la problemática de acceso a la justicia. En Colombia cuentan con la Encuesta de Necesidades Jurídicas, la cual en 2021 reveló que el 80.2 % de las necesidades jurídicas declaradas por la población no encontraron una solución.

[Otro ejemplo son los] Centros de Justicia Ciudadanos: Son proyectos que acercan la justicia a las personas a partir de un servicio accesible, transparente, oportuno, innovador, ampliamente participativo y de calidad para satisfacer las necesidades jurídicas de los grupos vulnerados, más allá de los tribunales y sin llegar a la judicialización. Dan prioridad a las soluciones no adversariales que comprometan no sólo a las partes en conflicto, sino a toda la comunidad. Chile cuenta con los Centros de Justicia Ciudadanos que buscan acercar la justicia a las personas y comunidades a partir de un proceso que promueve el diálogo para resolver conflictos. (EQUIS, 2023b, p. 35)

XIII.4. NUESTRA PROPUESTA, UN MODELO DE JUSTICIA ABIERTA FEMINISTA

El modelo de justicia abierta feminista propuesto por EQUIS es una estrategia integral para dismantelar las estructuras discriminatorias y de opresión en los tribunales. Este modelo reconoce la participación ciudadana como la base sobre la cual descansa la legitimidad y la democratización judicial. Es la clave para generar legitimidad social y ciudadanizar la justicia: Equipos multidisciplinarios, mesas regionales por la justicia abierta, y observatorios ciudadanos son ejemplos de cómo se puede materializar este modelo.

Nuestra propuesta es la construcción conjunta de un modelo de Justicia Abierta Feminista. Un modelo que busca democratizar los poderes judiciales, garantizar una justicia accesible en todos los territorios, para todas las personas, y asegurar que las políticas judiciales estén basadas en evidencia y diseñadas con la participación ciudadana. Queremos darle una repensada a nuestro sistema de justicia, para garantizar el acceso a la justicia, y a las justicias, en plural, para todas las mujeres y poblaciones históricamente vulneradas. (Gamboa Estrella, julio, 2024)

Este enfoque busca escuchar a la ciudadanía, pero sobre todo busca involucrarla activamente en la administración de justicia, garantizando que las decisiones judiciales sean transparentes y representativas de las necesidades de la sociedad. La participación ciudadana fortalece la autonomía e independencia del Poder Judicial al permitir que la sociedad desempeñe un rol activo tanto como usuaria de los servicios judiciales y como auditora del actuar de los tribunales (EQUIS, 2023a, p. 6).

En los últimos años hemos impulsado iniciativas de participación ciudadana que nos aportan evidencia sobre la importancia de involucrar a la ciudadanía en su derecho de acceso a la justicia.

El Consejo Consultivo de Oaxaca [que aún está en vías de implementación, es un buen ejemplo]. Es un mecanismo participativo para impulsar un mejor sistema de justicia [que] pone al centro la igualdad y la perspectiva de género. Participan organizaciones de la sociedad civil y dentro de sus facultades se encuentra la posibilidad de funcionar como un órgano especializado y de consulta para generar lineamientos, proyectos y actividades en materia de derechos humanos, género y transparencia del Poder Judicial de Oaxaca. (EQUIS, 2023b, p. 36)

Además, está

[El] Observatorio Judicial de Coahuila. Es un órgano ciudadano de consulta y apoyo del Poder Judicial del Estado de Coahuila de Zaragoza, adscrito a la Presidencia del Tribunal Superior de Justicia. Tiene por objeto coadyuvar en la supervisión y vigilancia del quehacer de los órganos jurisdiccionales y no jurisdiccionales del Poder Judicial, para identificar problemáticas en el funcionamiento de los mismos y formular, en su caso, recomendaciones y propuestas para su mejor operación. Está integrado por un Consejo Técnico General, por Capítulos Regionales y por Observadores Ciudadanos. (EQUIS, 2023b, p. 40)

A nivel nacional, desde Equis hemos acompañado

[al] Observatorio Ciudadano de los Centros de Justicia para las Mujeres. Espacio de trabajo colaborativo entre organizaciones civiles locales para recopilar y generar información sobre las condiciones de operación de los Centros de Justicia para las Mujeres, con una evaluación y capacidad para emitir recomendaciones para su fortalecimiento. (EQUIS, 2023b, p. 36)

La participación ciudadana es la respuesta a la crisis de confianza y legitimidad en los tribunales mexicanos, porque mejora la relación con la ciudadanía y fortalece la independencia judicial. El modelo de Justicia Abierta Feminista en conjunto es esencial para superar las barreras de discriminación y exclusión, y avanzar hacia un sistema judicial más justo y equitativo para todas las personas (EQUIS, 2023b, p. 42). Siguiendo esta línea, Equis forma parte del Pacto por una Justicia Abierta con Perspectiva de Género, que es el marco para impulsar acciones hacia la construcción de un modelo de justicia abierta que responda a las diferentes realidades y contextos de los poderes judiciales estatales. Un pacto mediante el cual se garantice el derecho de acceso a la justicia en condiciones de igualdad y la democratización judicial.

REFERENCIAS

- EQUIS Justicia para las Mujeres. (2023a). Mecanismos de participación ciudadana en los poderes judiciales de México. <https://equis.org.mx/wp-content/uploads/2023/02/Mecanismos-de-participacion-ciudadana.pdf>
- EQUIS Justicia para las Mujeres. (2023b) Modelo de justicia abierta feminista. <https://equis.org.mx/wp-content/uploads/2023/02/Justicia-abierta-feminista.pdf>
- Gamboa Estrella, F. (s.f.) *Reforma judicial feminista. Desmantelar las fábricas de injusticias*. EQUIS Justicias para las Mujeres. <https://equis.org.mx/wp-content/uploads/2024/07/Reforma-Judicial-Feminista.pdf>
- Gamboa Estrella, F. (24 de julio de 2024). ¿Por qué necesitamos una reforma judicial feminista? *Nexos*. <https://eljuegodelacorte.nexos.com.mx/por-que-necesitamos-una-reforma-judicial-feminista/>
- Instituto Nacional de Estadística y Geografía (INEGI). (2021). Encuesta Nacional sobre la Dinámica de las Relaciones en los Hogares (ENDIREH) 2021. <https://www.inegi.org.mx/programas/endireh/2021/>
- INEGI (2023). Encuesta Nacional de Victimización y Percepción sobre Seguridad Pública (ENVIPE) 2023. <https://www.inegi.org.mx/programas/envipe/2023/>
- Red por la Ciudadanización de la Justicia (RCJ).(2021). *No es Justicia. Análisis de sentencias y resoluciones judiciales del país*. <https://equis.org.mx/wp-content/uploads/2021/02/noesjusticia.pdf>

CAPÍTULO XIV

Acceso a la energía eléctrica e internet como condición *sine qua non* para la garantía de los derechos digitales

Andrés Acosta Padilla¹

SUMARIO: XIV.1. Introducción; XIV.2. Acceso a la energía eléctrica en México; XIV.3. Acceso a internet y derechos digitales; XIV.4. Conclusiones.

PALABRAS clave: Energía eléctrica, internet, derechos digitales, desarrollo integral, derechos de minorías.

XIV.1. INTRODUCCIÓN

El acceso universal a la energía eléctrica e internet se ha posicionado como requisito de primer orden para el goce y ejercicio de los derechos digitales. En un mundo globalizado y una aplicación cada vez más intensiva de la tecnología en la vida cotidiana de las personas, el combate decidido de las brechas energética y digital forma parte de la batalla en la reducción de las desigualdades en nuestro país.

Es imperativa la necesidad de concientizar a todas las personas usuarias de internet de que sus derechos también son exigibles en el entorno digital, de ello dependerá el uso virtuoso y responsable de la tecnología al servicio de su desarrollo integral.

Por su parte, el Estado no debe vislumbrarse más allá de un prestador de servicios públicos, sino como un garante de derechos humanos, por ello su obligación de intervenir a través de regulación eficiente y política pública que promueva el acceso universal a la energía eléctrica e internet, con mayor ahínco en la población vulnerable. Su inclusión es su derecho y obligación de las instituciones democráticas.

XIV.2. ACCESO A LA ENERGÍA ELÉCTRICA EN MÉXICO

El Instituto Nacional de Estadística y Geografía (INEGI), reportó que en “2023 el total de población en México fue de 129.5 millones de personas, de las cuales 67 millones correspondió a mujeres (51.7%) y 62.5 millones a hombres (48.3%)” (INEGI,

¹ Profesor de Carrera de la Facultad de Derecho de la Universidad Nacional Autónoma de México y Miembro de la Barra Mexicana, Colegio de Abogados. andresacosta@derecho.unam.mx

22 de mayo, 2024, p. 2). El mismo año la Comisión Federal de Electricidad (CFE) informó que “la cobertura del servicio de energía eléctrica ascendió al 99.43%” de la población (CFE, 6 de febrero, 2024), lo que deja entrever ese mismo año 743 mil 685 personas carecían de esta cobertura (SENER, 2024, p. 152).

El avance en la materia es significativo, basta contrastar el número de viviendas que no disponían de energía eléctrica al iniciar el siglo XXI, en ello el INEGI identifica que en el año 2000 eran 988 mil 804 viviendas, mientras que para 2020 fueron 268 mil 863 viviendas. Tratándose de un análisis por entidad federativa, Chiapas (23 mil 972 viviendas), Oaxaca (25 mil 242 viviendas) y Veracruz (32 mil 038 viviendas), fueron en 2020 las entidades con mayores viviendas sin acceso a la energía eléctrica. (INEGI, 2020)

Lo anterior reviste una importancia mayúscula en tanto que algunas personas teóricas de los derechos humanos y juzgadores han propuesto reconocer al acceso a la energía eléctrica como un derecho humano, transitando de la visión restrictiva del acceso a la electricidad como actividad de interés público. No podría ser de otra manera, pues cada vez más derechos humanos dependen del acceso a la energía eléctrica; la operación eficiente del equipamiento de un centro médico garantiza el derecho a la salud, el funcionamiento de las plataformas tecnológicas de servicios educativos coadyuva en la garantía del derecho a la educación, sólo por poner un par de ejemplos.

Al respecto, la Tesis aislada 1.3o.C.100 K(10a.) del Tribunal Colegiado en materia civil del Primer Circuito, indica que:

ACCESO A LA ENERGÍA ELÉCTRICA. DEBE RECONOCERSE COMO DERECHO HUMANO POR SER UN PRESUPUESTO INDISPENSABLE PARA EL GOCE DE MÚLTIPLES DERECHOS FUNDAMENTALES.

La Constitución Política de los Estados Unidos Mexicanos reconoce derechos humanos económicos, sociales y culturales como la alimentación nutritiva, suficiente y de calidad; la educación de calidad; el acceso a los servicios de protección de la salud; un medio ambiente adecuado para el desarrollo y bienestar de las personas; la vivienda digna y decorosa; el acceso a la cultura; el acceso a la información y a sus tecnologías, así como a los servicios de radiodifusión y telecomunicaciones, incluido el Internet; la libertad de expresión e imprenta; la libertad de profesión, industria, comercio y trabajo; entre otros. El ejercicio de estos derechos depende cada vez y en mayor medida del suministro de energía eléctrica. En efecto, en el estado actual del desarrollo científico y tecnológico, los satisfactores materiales e inmateriales (tangibles e intangibles), se encuentran estrechamente ligados a la energía eléctrica, la cual es usada en prácticamente todos los ámbitos de la actividad humana para generar energía lumínica, mecánica y térmica, así como para el procesamiento de la información y la realización de las telecomunicaciones. Por esta razón, el acceso a la energía eléctrica debe reconocerse como un derecho humano por ser un presupuesto indispensable, al constituir una condición necesaria para el goce de múltiples derechos fundamentales. (Tesis: 1.3o.C.100 K, diciembre de 2018). [énfasis añadido].

Con base en lo anterior es ineludible la evolución de esta actividad de interés público hacia su reconocimiento como derecho humano exigible y justiciable. Sin embargo, debemos puntualizar que el reconocimiento como derecho humano es parte del camino y no la meta, ya que el acceso efectivo de los derechos humanos no reside en los discursos o en la tinta y papel del sistema jurídico, sino en la política pública diseñada bajo parámetros técnicos, dotada de recursos humanos, financieros, materiales y técnicos suficientes, así como su evaluación y mejora constante.

Lo anterior desemboca en lo que Stephen Holmes y Cass R. Sustein sostienen, que toda garantía de derechos implica costos, es así la crítica a la división de los derechos en negativos y positivos; entendiendo a los negativos como derechos en donde el Estado sólo de limitarse y no entrometerse en la libertad de las personas, en cuanto a los positivos, estos sí exigen un papel activo del Estado.

Sin embargo, dicha dicotomía encuentra su ineficacia al establecer que los derechos que aparentemente exigen la inactividad del Estado, por ejemplo, los derechos civiles y políticos, también le exigen un papel activo, toda vez que deben de garantizar legalidad, certeza, imparcialidad, objetividad, independencia y máxima publicidad en los comicios, véase por ejemplo cualquier presupuesto asignado a las labores sustantivas del Instituto Nacional Electoral.

En el caso del acceso a la energía eléctrica, se necesita un papel activo del Estado, ya sea a través de la regulación y supervisión de todos los participantes del mercado, o bien, su intervención directa en las actividades de la industria. En el caso mexicano, por mandato constitucional corresponde exclusivamente a la Nación la planeación y control del sistema eléctrico nacional, así como el servicio público de transmisión y distribución de energía eléctrica.

En los albores del uso de la electricidad su aplicación era con fines modestos, por ejemplo, la iluminación, sin embargo, la sociedad contemporánea exige un uso más intensivo de la electricidad, por ello es importante atender lo que el Doctor Pedro Guerra Morales indica:

La distinción entre la necesidad de sistemas aislados y conexión a la red es relevante pues los servicios intensivos en el uso de electricidad para el uso de internet (dispositivos terminales, pantallas y módems) no tendrían suficiente eficiencia alimentándose de sistemas fotovoltaicos además de que la infraestructura de las redes de acceso (centrales de comunicaciones y radiobases) demandan conexión a las redes de distribución. (Guerra Morales, 2023, p. 33)

Un ejemplo en torno al uso cada vez mayor de la electricidad —no sólo para iluminación— y la necesidad de inversión, es la Isla de Holbox, en el norte de Quintana Roo, Municipio de Lázaro Cárdenas, el Programa de Desarrollo del Sistema Eléctrico Nacional 2024 – 2038 (PRODESEN) en su Programa de Ampliación y Modernización de las Redes Generales de Distribución que no Correspondan al Mercado Eléctrico

Mayorista, indica que “las actividades en la isla demandan [...] 3.2 *megawatts* (MW), conformada por cuatro unidades de combustión interna a diésel y adicionalmente dos plantas móviles de 1.8 MW, utilizadas como respaldo”. (SENER, 2024, pp. 148)

El proyecto [de conexión de la Isla al sistema eléctrico nacional] consideró la construcción de un circuito aéreo de 58.9 kilómetros (KM) en 34.5 *kilovolts*, incluyendo fibra óptica de la subestación eléctrica Popolnah hasta la población de Chiquilá, y continua con un circuito submarino de 10.5 KM hasta la futura subestación eléctrica de Holbox. [además] de adecuar y modernizar la red de distribución de la isla. Este proyecto se concluyó en 2023 y se requirió una inversión total de 193.4 millones en 2023 para su cierre. (SENER, 2024, pp. 148 y 149)

Este caso deja entrever el incremento en la demanda energética de nuestro territorio, las necesidades ya no sólo son de iluminación como en el siglo pasado, el proyecto en comento requirió la atención del Estado y no impactó positivamente a las 743 mil 685 personas sin servicio eléctrico.

La electrificación de las comunidades rurales y zonas urbanas marginadas son otro gran reto, de esa labor se encarga el Fondo del Servicio Universal Eléctrico (FSUE). Este mismo reporta que:

Para 2024-2025, se [programó la construcción de] 10 mil 885 proyectos de electrificación financiados por el FSUE, el Instituto Nacional de los Pueblos Indígenas, entidades federativas y municipios, con una inversión de 7 mil 865 millones de pesos, [beneficiando] a 585 mil 741 habitantes, a través de 9 mil 158 obras de extensiones de red eléctrica de distribución y mil 727 obras de sistemas aislados. (SENER, 2024, p. 152)

Lo anterior es un avance significativo en la cobertura universal de energía eléctrica, pero recordemos que el uso intensivo de electricidad requerido para el acceso a otros derechos como el de la salud, educación y el acceso a las tecnologías de la información y comunicación, requiere extensiones de la red eléctrica.

Por último, es importante traer a colación un objetivo cuya fecha de cumplimiento está cada vez más cercana, me refiero al Objetivo 7. Energía asequible y no contaminante, de los Objetivos de Desarrollo Sostenible, adoptados por las Naciones Unidas en 2015 y que son un llamamiento universal por cumplir para el 2030 (ONU, 2025).

Este objetivo que nos ocupa reconoce que la electrificación es sólo un peldaño y establece metas puntuales, entre otras, acceso universal a servicios energéticos asequibles, fiables y modernos; aumento considerable en la proporción de energía renovable, ampliar la infraestructura y mejorar la tecnología para prestar servicios energéticos modernos y sostenibles para todos en los países en desarrollo. (ONU, ODS 7, 2025)

XIV.3. ACCESO A INTERNET Y DERECHOS DIGITALES

El INEGI reportó que, en 2020, en México alrededor de 83 millones de personas fueron usuarias de internet, cantidad que para 2023 se incrementó a 97 millones. Sin embargo, recordemos que ese mismo año la población total del país ascendió a 129.5 millones de personas, estableciendo un aproximado de 32.5 millones de personas en algún grado de brecha digital (INEGI e IFT, 2024).

Asimismo, la población usuaria de internet puede segmentarse por ámbito urbano y rural, para el primero se registró que 85.5% de las personas de 6 años o más utilizó internet, mientras que para el segundo segmentó fue del 66% (INEGI e IFT, 2024, p. 5).

Con relación al uso del internet, se identificó que “se usó con mayor frecuencia para comunicarse (93%), como segundo uso con mayor frecuencia el acceso a redes sociales (91.5%) y como tercer uso más frecuente el entretenimiento (88.1%)”. Geográficamente “las entidades federativas con menor porcentaje de personas usuarias de internet fueron Chiapas (59.9%), Oaxaca (70.6%) y Veracruz (71.8%)” (INEGI e IFT, 2024, pp. 2 y 3).

Contrario a la discusión en torno al acceso a la energía eléctrica como derecho, desde el 11 de junio de 2013, el párrafo tercero del artículo 6o. constitucional reconoce que el Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. En el mismo artículo, pero en su apartado B, fracción I se impone la obligación al Estado de garantizar a la población su integración a la sociedad de la información y el conocimiento, mediante una política de inclusión digital con metas anuales y sexenales.

Para garantizar lo anterior, entre otras acciones, el Estado mexicano vislumbró y creó el 2 de agosto de 2019, la empresa subsidiaria de la CFE, denominada CFE Telecomunicaciones e Internet para Todos, con el objeto de prestar y proveer servicios de telecomunicaciones sin fines de lucro, para garantizar el derecho de acceso a las tecnologías de la información y comunicación, incluido el de banda ancha e internet. (DOF, 2019)

Con base en el decreto de creación esta empresa subsidiaria logra el acceso a internet gratuito en lugares públicos de las zonas más vulnerables. En la actualidad suman más de 100 puntos de internet gratuito, por ejemplo, en Chiapas (6 mil 173 puntos), Oaxaca (3 mil 947 puntos) y Veracruz (7 mil 632 puntos) (CFE, 2024).

Garantizar el acceso universal de electricidad e internet son herramientas para el desarrollo de todas las personas, pues en la sociedad contemporánea estos servicios se vislumbran como elementos *sine qua non* para el acceso al entorno digital, entendido este último concepto como “todas aquellas plataformas y aplicaciones que nos permiten interactuar como personas y organizaciones a través de medios virtuales” (GTCD, 2023).

Para vislumbrar la trascendencia de lo anterior, vale la pena traer a colación el promedio de tiempo de uso de internet por parte de las personas usuarias en nuestro país, en 2023 el grupo de edad de “18 a 24 años registró el promedio más alto, 5.9 horas al día, continuando las personas de 25 a 34 años y de 12 a 17 años con 5.6 y 4.7 horas por día, respectivamente” (INEGI e IFT, 2024, p. 3).

Es decir, una buena parte del tiempo que una persona se mantiene despierta lo ocupa en el entorno digital, ya que en promedio las personas deben dormir 8 horas, así que son 16 horas las que se mantienen despiertas y de ellas casi 6 –en el caso de las personas de 18 a 24 años– se mantiene activas en el entorno digital.

Ahora bien, los Derechos Digitales son entendidos como “[...] la extensión al mundo digital de los derechos fundamentales ya reconocidos en nuestro ordenamiento jurídico, perfilando los más relevantes en el entorno y los espacios digitales o describiendo derechos instrumentales o auxiliares de los primeros” (MAETD, 2023).

Para mayor comprensión de estos derechos contamos con la *Carta de Derechos de la Persona en el Entorno Digital. Código de Buenas Prácticas* emitido por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, documento de carácter orientador que refleja aquellas conductas deseables a realizar tanto por el Estado como por particulares (INAI, 2024).

La guía se divide en nueve capítulos, con los siguientes títulos: I. Igualdad digital, II. Libertades en el entorno digital, III. Derecho a la seguridad y protección de datos personales, IV. Derechos a la participación a la democracia y al buen gobierno digital, V. Derechos laborales, VI. Derechos de las personas en situación de vulnerabilidad, VII. Neuroderechos, VIII. Ética en el uso de inteligencia artificial, IX. Medios de defensa y derechos de las víctimas del delito cibernético, violencia digital y de violaciones a derechos humanos. (INAI, 2024).

Cada uno de los títulos explica cada uno de los derechos vinculados, por ejemplo, en el Capítulo I de Igualdad digital, establece en el punto

1.5. El estado deberá fomentar políticas públicas encaminadas a la disminución y erradicación de las brechas digitales en razón de edad, género, lugar de residencia, origen o cualquier otro motivo que impida que las personas gocen, en igualdad de condiciones, de los medios digitales. (INAI, 2024, p. 25)

Otro buen ejemplo en la Carta se encuentra en su Capítulo IV Derecho a la participación ciudadana por medios digitales, entre otras cosas indica

2.1. El acceso a los servicios públicos y a las relaciones digitales con las administraciones públicas debe ser garantizado a toda persona, con la finalidad de promover políticas públicas activas que garanticen el acceso a los servicios públicos, a los sistemas y los procedimientos de todos los sujetos obligados. (INAI, 2024, p. 43)

Este último punto es de lo más innovador, pues la relación digital con el gobierno no solo eficiente tiempos de respuesta, sino que evita costos de transacción importantes; desde costos de transporte a la oficina gubernamental, impresión de documentos oficiales, trámite de permisos de día de descanso en el centro laboral de la persona usuaria, así como uno de los más lacerantes problemas de las sociedades: la corrupción.

La Encuesta Nacional de Calidad e Impacto Gubernamental 2023, a cargo del INEGI, documentó que en el bimestre

[...] noviembre-diciembre de 2023, a nivel nacional, 83.1% de la población consideró frecuentes los actos de corrupción, en el mismo orden nacional en 2023, los costos de incurrir en este tipo de conductas se estimaron en 11 mil 910 millones de pesos, lo que significa 3 mil 368 pesos en promedio por víctima. (INEGI, 20 de marzo, 2024, p. 3)

Aquí una de las grandes áreas de oportunidad para la naciente relación digital con el gobierno federal. Por último, los beneficios del entorno digital deben promoverse e incrementarse con estricto respeto de los derechos digitales. Para beneplácito de todas las personas, la agenda gubernamental destina esfuerzos importantes en la materia, la nueva Agencia de Transformación Digital y Telecomunicaciones dirigirá sus tareas sustantivas en 7 puntos:

1. Lograr que los trámites que existen de manera presencial estén disponibles de manera digital.
2. Reducir al mínimo la carga regulatoria sobre personas y empresas.
3. Generar ahorros y oportunidad para tener cero corrupción.
4. Crear el Centro de Atención para el Bienestar, a través del número 079, que brinde atención ciudadana las 24 horas del día.
5. Implementar inteligencia y análisis de datos para fortalecer las capacidades públicas.
6. Autonomía tecnológica y seguridad de información.
7. Internet como derecho. (Presidencia de la República, 2024)

De concretarse los esfuerzos citados, nuestra nación avanzará vertiginosamente en la instauración del buen gobierno digital en favor de las personas usuarias, pero, de manera paralela, no deberá dejar de trabajar por la inclusión al entorno digital de aquellas minorías que no han podido superar las brechas de energía e internet, como ya lo hemos vislumbrado en el presente trabajo, de ello depende el acceso efectivo a más derechos.

XIV.4. CONCLUSIONES

Sirvan las presentes líneas para develar una vez más la relevancia de los derechos digitales, los cuales se presentan no ya como el futuro en la sociedad, sino como el presente y una tarea de todos; por lo que los sectores público, privado y social deben conjuntar esfuerzos para la garantía efectiva de estos en favor de las personas usuarias.

Sin embargo, no debemos dejar de lado que existen personas en nuestro territorio que aún viven en la oscuridad o tienen acceso a electricidad para usos básicos como la iluminación, por ende, lejos están de ser usuarias de internet y los derechos digitales les son ajenos.

También resulta cierto que, frente a la gran población de la nación, son las minorías quienes no acceden a la electricidad o internet, pero la vida en democracia también exige la protección de los derechos de las minorías, de modo que es de primer orden que todas las personas se desarrollen integralmente; refiriéndonos a este concepto como “[...] el proceso en la vida de los seres humanos enfocado a tener una vida digna que cubra las necesidades fundamentales biológicas o fisiológicas, emocionales, culturales, políticas, sociales y económicas” (SEP, 2025)

El desarrollo integral para todos es un signo de una democracia viva y fortalecida, sin duda, el acceso universal a la energía eléctrica y el internet son instrumentos para que el acceso a los derechos digitales sea efectivo y la tecnología esté al servicio de los más altos fines de la humanidad.

REFERENCIAS

- Acuerdo por el que se crea CFE Telecomunicaciones e Internet para Todos. (02 de agosto de 2019). *Diario Oficial de la Federación (DOF)*. https://www.dof.gob.mx/nota_detalle.php?codigo=5567088&fecha=02/08/2019#gsc.tab=0
- Comisión Federal de Electricidad (CFE). (6 de febrero de 2024). Boletín de prensa CFE-BP-013/24vF. https://www.cfe.mx/cdn/2019/Archivos/Boletines/Bol_%2013%20Consejo%20de%20Admin%20CFE%20Distribucion%20v5.pdf
- CFE. (2024). Comunicamos a México. Internet fijo gratuito. https://internetparatodos.cfe.mx/cfe_teit_servicios/internet-fijo-gratuito/#
- Guerra Morales, P. (enero-mayo, 2023). Energía e Internet. La electricidad como habilitador de Derechos Humanos de Cuarta Generación. *Perspectivas Energéticas. Programa de Energía, año 7*(16). <https://programaenergia.colmex.mx/publicaciones/perspectivas-energeticas/>
- Instituto Nacional de Estadística y Geografía (INEGI). (2020). Demografía y Sociedad. Vivienda. <https://www.inegi.org.mx/temas/vivienda/>
- INEGI. (22 de mayo de 2024). Encuesta nacional de la dinámica demográfica (ENADID) 2023. Comunicado de prensa núm. 305/24. <https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/ENADID/ENADID2023.pdf>

- INEGI e Instituto Federal de Telecomunicaciones (IFT). (13 de junio de 2024). Encuesta nacional sobre disponibilidad y uso de tecnologías de la información en los hogares (ENDUTIH) 2023. Comunicado de prensa núm. 372/24. https://inegi.org.mx/contenidos/saladeprensa/boletines/2024/ENDUTIH/ENDUTIH_23.pdf
- INEGI. (20 de marzo de 2024). Encuesta nacional de calidad e impacto regulatorio (ENCIG) 2023. Comunicado de prensa núm. 198/24. https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/EstSegPub/ENCIG_23.pdf
- Ministerio de Asuntos Económicos y Transformación Digital (MAETD), Observatorio Nacional de Tecnología y Sociedad (ONTSI). (2023). *Derechos digitales. Edición 2023 - Datos 2022*. https://www.ontsi.es/sites/ontsi/files/2024-03/Monogr%C3%A1fico_Derechos_Digitales_online_v06_b.pdf
- Organización de las Naciones Unidas (ONU). (2025). Objetivos de Desarrollo Sostenible (ODS). Objetivos y metas de desarrollo sostenible. <https://www.un.org/sustainabledevelopment/es/sustainable-development-goals/>
- Presidencia de la República. (14 de noviembre de 2024). Presidenta Claudia Sheinbaum presenta la nueva Agencia de Transformación Digital para simplificar trámites y evitar la corrupción. Comunicado. <https://www.gob.mx/presidencia/prensa/presidenta-claudia-sheinbaum-presenta-la-nueva-agencia-de-transformacion-digital-para-simplificar-tramites-y-evitar-la-corrupcion>
- Grupo de Trabajo de Ciudadanía Digital (GTCD). (2023). ¿Qué entendemos por entorno digital? En *Construyendo ciudadanía en entornos digitales. Punto de partida*. <https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/construyendo-ciudadania-entornos-digitales-punto-partida/construyendo-4>
- Secretaría de Educación Pública (SEP). (06 de febrero de 2025). ¿Cómo favorecemos el desarrollo integral?. <https://nuevaescuelamexicana.sep.gob.mx/detalle-ficha/6241/>
- Secretaría de Energía (SENER). (31 de mayo de 2024). Programa de Desarrollo del Sistema Eléctrico Nacional 2024-2038, Capítulo 6. Programa de Ampliación y Modernización de las Redes Generales de Distribución que no correspondiente al Mercado Eléctrico Mayorista <https://www.gob.mx/sener/articulos/programa-de-desarrollo-del-sistema-electrico-nacional-2024-2038>
- Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales (INAI). (2024). *Carta de Derechos de la Persona en el Entorno Digital. Código de Buenas Prácticas*. https://infocdmx.org.mx/images/biblioteca/2022/Carta_Derechos_Persona_EntornoDigital_Digital.pdf
- Tesis: I.3o.C.100 K (10a.). (Diciembre de 2018). *Gaceta del Semanario Judicial de la Federación*. Reg. 2018528. Tomo II, p. 959. <https://sjf2.scjn.gob.mx/detalle/tesis/2018528>

