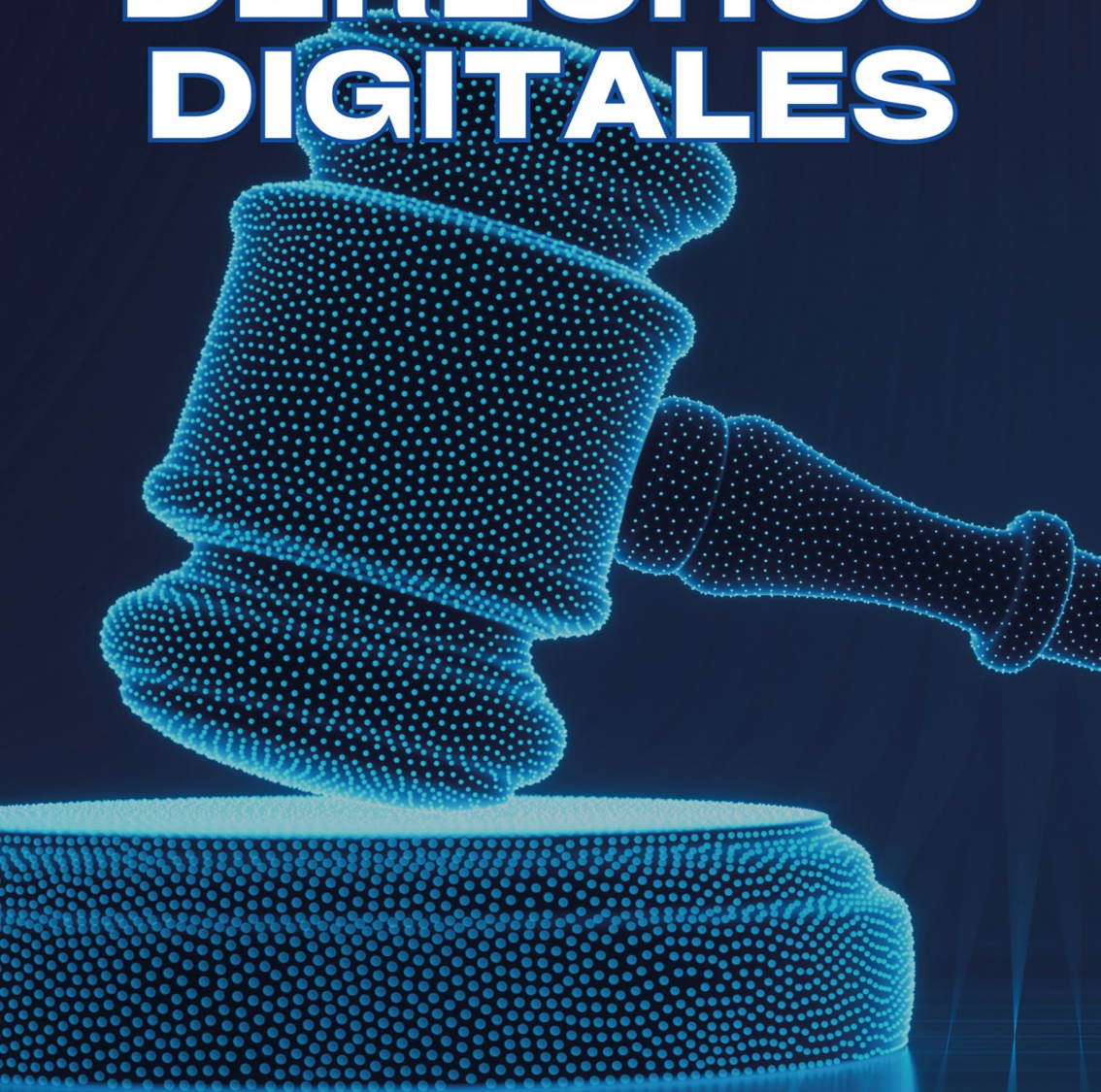


DERECHOS DIGITALES



COORDINADORES

SONIA VENEGAS ÁLVAREZ | JULIO CÉSAR BONILLA GUTIÉRREZ

ARÍSTIDES RODRIGO GUERRERO GARCÍA

COMITÉ CIENTÍFICO DE LA EDITORIAL TIRANT LO BLANCH

MARÍA JOSÉ AÑÓN ROIG

*Catedrática de Filosofía del Derecho
de la Universidad de Valencia*

ANA CAÑIZARES LASO

*Catedrática de Derecho Civil
de la Universidad de Málaga*

JORGE A. CERDIO HERRÁN

*Catedrático de Teoría y Filosofía de Derecho
Instituto Tecnológico Autónomo de México*

JOSÉ RAMÓN COSSÍO DÍAZ

*Ministro en retiro de la Suprema
Corte de Justicia de la Nación
y miembro de El Colegio Nacional*

MARÍA LUISA CUERDA ARNAU

*Catedrática de Derecho Penal
de la Universidad Jaume I de Castellón*

MANUEL DÍAZ MARTÍNEZ

Catedrático de Derecho Procesal de la UNED

CARMEN DOMÍNGUEZ HIDALGO

*Catedrática de Derecho Civil
de la Pontificia Universidad Católica de Chile*

EDUARDO FERRER MAC-GREGOR POISOT

*Juez de la Corte Interamericana
de Derechos Humanos
Investigador del Instituto de Investigaciones
Jurídicas de la UNAM*

OWEN FISS

*Catedrático emérito de Teoría del Derecho
de la Universidad de Yale (EEUU)*

JOSÉ ANTONIO GARCÍA-CRUCES GONZÁLEZ

Catedrático de Derecho Mercantil de la UNED

JOSÉ LUIS GONZÁLEZ CUSSAC

*Catedrático de Derecho Penal
de la Universidad de Valencia*

LUIS LÓPEZ GUERRA

*Catedrático de Derecho Constitucional
de la Universidad Carlos III de Madrid*

ÁNGEL M. LÓPEZ Y LÓPEZ

*Catedrático de Derecho Civil
de la Universidad de Sevilla*

MARTA LORENTE SARIÑENA

*Catedrática de Historia del Derecho
de la Universidad Autónoma de Madrid*

JAVIER DE LUCAS MARTÍN

*Catedrático de Filosofía del Derecho
y Filosofía Política de la Universidad de Valencia*

VÍCTOR MORENO CATENA

*Catedrático de Derecho Procesal
de la Universidad Carlos III de Madrid*

FRANCISCO MUÑOZ CONDE

*Catedrático de Derecho Penal
de la Universidad Pablo de Olavide de Sevilla*

ANGELIKA NUSSBERGER

*Catedrática de Derecho Constitucional
e Internacional en la Universidad de Colonia
(Alemania). Miembro de la Comisión de Venecia*

HÉCTOR OLASOLO ALONSO

*Catedrático de Derecho Internacional
de la Universidad del Rosario (Colombia)
y Presidente del Instituto Ibero-Americano
de La Haya (Holanda)*

LUCIANO PAREJO ALFONSO

*Catedrático de Derecho Administrativo
de la Universidad Carlos III de Madrid*

CONSUELO RAMÓN CHORNET

*Catedrática de Derecho Internacional
Público y Relaciones Internacionales
de la Universidad de Valencia*

TOMÁS SALA FRANCO

*Catedrático de Derecho del Trabajo y de la
Seguridad Social de la Universidad de Valencia*

IGNACIO SANCHO GARGALLO

*Magistrado de la Sala Primera (Civil)
del Tribunal Supremo de España*

ELISA SPECKMAN GUERRA

*Directora del Instituto de Investigaciones
Históricas de la UNAM*

RUTH ZIMMERLING

*Catedrática de Ciencia Política
de la Universidad de Mainz (Alemania)*

Fueron miembros de este Comité:

Emilio Beltrán Sánchez, Rosario Valpuesta Fernández y Tomás S. Vives Antón

Procedimiento de selección de originales, ver página web:
www.tirant.net/index.php/editorial/procedimiento-de-seleccion-de-originales

DERECHOS DIGITALES

SONIA VENEGAS ÁLVAREZ

JULIO CÉSAR BONILLA GUTIÉRREZ

ARÍSTIDES RODRIGO GUERRERO GARCÍA

Coordinadores

tirant lo blanch

Ciudad de México, 2024

Copyright © 2024

Todos los derechos reservados. Ni la totalidad ni parte de este libro puede reproducirse o transmitirse por ningún procedimiento electrónico o mecánico, incluyendo fotocopia, grabación magnética, o cualquier almacenamiento de información y sistema de recuperación sin permiso escrito de los autores y del editor.

En caso de erratas y actualizaciones, la Editorial Tirant lo Blanch México publicará la pertinente corrección en la página web www.tirant.com/mex/

© Sonia Venegas Álvarez

© EDITA: TIRANT LO BLANCH
DISTRIBUYE: TIRANT LO BLANCH MÉXICO

Av. Tamaulipas 150, Oficina 502

Hipódromo, Cuauhtémoc

CP 06100, Ciudad de México

Telf: +52 1 55 65502317

infomex@tirant.com

www.tirant.com/mex/

www.tirant.es

ISBN: 978-84-1071-776-3

MAQUETA: Disset Ediciones

Si tiene alguna queja o sugerencia, envíenos un mail a: atencioncliente@tirant.com. En caso de no ser atendida su sugerencia, por favor, lea en www.tirant.net/index.php/empresa/politicas-de-empresa nuestro procedimiento de quejas.

Responsabilidad Social Corporativa: http://www.tirant.net/Docs/RSC_Tirant.pdf

**Comité Editorial del Instituto de Transparencia, Acceso
a la Información Pública, Protección de Datos Personales
y Rendición de Cuentas de la Ciudad de México 2024**

Dr. Julio César Bonilla Gutiérrez

Comisionado Ciudadano del INFO CDMX

Mtra. Laura Lizette Enríquez Rodríguez

Comisionada Ciudadana del INFO CDMX

Dra. Sonia Venegas Álvarez

Especialista externa

Dra. Julieta Morales Sánchez

Especialista externa

Mtro. Juan Gómez Pérez

Especialista externo

Coordinador del Comité

Esp. Héctor Javier Maya Ibarra

Director de Vinculación y Proyección Estratégica del INFO CDMX

Secretario Técnico del Comité

Lic. Raúl Llanos Samaniego

Director de Comunicación Social 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**

Arístides Rodrigo Guerrero García

Comisionado Presidente del INFO CDMX

Julio César Bonilla Gutiérrez

Comisionado Ciudadano del INFO CDMX

Laura Lizette Enríquez Rodríguez

Comisionada Ciudadana del INFO CDMX

María del Carmen Nava Polina

Comisionada Ciudadana del INFO CDMX

Derechos digitales 2024

José Luis Mancilla Rosales

Sonia Venegas Álvarez

Rosa Alejandra Azuara Malagón

Emilio Vizarratea Rosales

Nora Angelica Damián Santiago

Onitsed Uriel Bustamante Silva

José Luis Hernández Sánchez

Sonia Venegas Álvarez

Aristides Rodrigo Guerrero García

Julio César Bonilla Gutiérrez

Coordinadores

ÍNDICE

<i>Prólogo</i>	11
JULIO CÉSAR BONILLA GUTIÉRREZ	
<i>Estado regulador y órgano autónomo regulador de las telecomunicaciones en México. Hacia el nuevo orden digital institucional.....</i>	17
JOSÉ LUIS MANCILLA ROSALES*	
<i>Legaltech: la tecnología a disposición del Derecho, una nueva oportunidad de negocios, el cambio en la prestación de servicios jurídicos o la inédita forma de aprender, enseñar, ejercer, comercializar y crear el Derecho</i>	45
SONIA VENEGAS ÁLVAREZ	
<i>Los datos personales en entornos digitales: herramientas para su protección</i>	73
ROSA ALEJANDRA AZUARA MALAGÓN	
<i>El derecho digital: un rubro necesario en el ciberespacio, el quinto dominio en operaciones militares</i>	89
EMILIO VIZARRETEA ROSALES	
<i>Ciudades inteligentes: innovación tecnológica para el futuro urbano.....</i>	117
NORA ANGÉLICA DAMIÁN SANTIAGO	
<i>Derechos digitales: asignatura pendiente en México</i>	137
ONITSED URIEL BUSTAMANTE SILVA	
<i>Inteligencia artificial y responsabilidad algorítmica. Apuntes para entender el nuevo sentido del Derecho</i>	165
JOSÉ LUIS HERNÁNDEZ SÁNCHEZ	

Prólogo

En el umbral de una nueva era marcada por la omnipresencia de la tecnología, nos encontramos ante un desafío ineludible: la comprensión y protección de nuestros derechos en el entorno digital. Esta obra colectiva, *Derechos Digitales 2024*, se presenta como una brújula esencial en el vasto y complejo océano de la Era Digital. Es el fruto del esfuerzo colaborativo de distinguidos expertos que han dedicado su vida a explorar, analizar y proponer soluciones para los numerosos retos que han surgido y a diario surgen en nuestra sociedad interconectada.

La tecnología ha permeado cada aspecto de nuestra existencia, transformando la manera en que nos comunicamos, aprendemos, trabajamos y ejercemos nuestros derechos y libertades. En este contexto, y de cara al futuro que nos ha alcanzado, los derechos digitales se convierten en un pilar fundamental para garantizar la libertad, la privacidad y la equidad en el ciberespacio. La presente obra, en tal sentido, no sólo aborda estas cuestiones desde una perspectiva teórica, sino que ofrece un enfoque práctico y propositivo para enfrentar los desafíos del mundo digital.

Desde los primeros indicios de la revolución tecnológica, se ha hecho evidente que el avance de la tecnología trae consigo oportunidades y riesgos. La capacidad de la inteligencia artificial, el *big data* y las redes sociales para influir en la opinión pública, la política y la economía plantean interrogantes críticas sobre la regulación, la ética y los derechos humanos. La obra que tiene en sus manos ofrece una visión profunda y detallada de estos temas, analizando cómo las normativas actuales se adaptan o fallan en adaptarse a las nuevas realidades digitales.

Cada contribución en esta obra refleja un compromiso con la innovación y la justicia, buscando equilibrar el progreso tecnológico con la protección de los derechos fundamentales. Los auto-

res, provenientes de diversas disciplinas, aportan una riqueza de perspectivas que enriquecen el debate sobre los derechos digitales. Su trabajo conjunto ofrece un panorama exhaustivo que va más allá de las simples aplicaciones tecnológicas, adentrándose en las implicaciones sociales, legales y éticas de la digitalización.

En un mundo donde los datos personales se han convertido en una moneda de cambio de la mayor valía, y la privacidad se ve constantemente amenazada por prácticas invasivas, es crucial establecer marcos legales robustos que protejan a las personas. En dicha inteligencia, el presente texto contiene valiosas propuestas de solución, innovadoras y efectivas, para salvaguardar la privacidad y la integridad de la información personal en el entorno digital. Se abordan temas cruciales como la ciberseguridad, destacando la importancia de proteger los sistemas informáticos de ataques malintencionados y garantizar la integridad de los datos.

Además, la obra analiza la gobernanza de Internet, un aspecto fundamental para asegurar que la red siga siendo un espacio abierto y accesible para todos. En este sentido, se discuten las políticas necesarias para evitar la monopolización de la infraestructura digital y se promueve una gestión inclusiva y democrática de los recursos tecnológicos.

El acceso equitativo a la tecnología es también un tema central en esta obra. Los autores exploran cómo la brecha digital perpetúa las desigualdades sociales y económicas, y proponen medidas para garantizar que todos, independientemente de su ubicación geográfica o situación socioeconómica, puedan beneficiarse de los avances tecnológicos. La educación digital y la alfabetización tecnológica son presentadas como herramientas clave para empoderar a las comunidades y fomentar un desarrollo inclusivo.

El impacto de la tecnología en el ámbito laboral y educativo es otro tema que se aborda con profundidad. La digitalización ha transformado la naturaleza del trabajo y la educación, planteando nuevos desafíos y oportunidades. Se explora cómo las nuevas tecnologías pueden ser aprovechadas para mejorar la

productividad y la calidad de vida, al tiempo que se protegen los derechos de los trabajadores y se garantiza un acceso equitativo a la educación de calidad. La automatización y la inteligencia artificial, por ejemplo, están cambiando rápidamente el paisaje laboral, y esta obra ofrece un análisis crítico de sus implicaciones, proponiendo políticas que aseguren una transición justa hacia el futuro del trabajo.

Asimismo, el presente esfuerzo subraya la importancia de la transparencia y la rendición de cuentas en el uso de las tecnologías digitales por parte de los gobiernos y las empresas. La vigilancia masiva y el uso indebido de datos personales son amenazas que deben ser contrarrestadas con políticas claras y mecanismos efectivos de supervisión. En este sentido, *Derechos digitales 2024* ofrece una guía práctica para la implementación de políticas públicas y corporativas que promuevan un uso ético y responsable de la tecnología. Los autores proponen la creación de organismos independientes encargados de supervisar el cumplimiento de las normativas de protección de datos y garantizar que las prácticas empresariales respeten los derechos de los usuarios.

La obra también se adentra en el futuro de los derechos digitales, analizando tendencias emergentes y proponiendo enfoques que puedan anticipar y mitigar los impactos negativos de las tecnologías aún en desarrollo. La computación cuántica, la realidad aumentada y virtual, y las tecnologías *blockchain* son exploradas en detalle, destacando tanto su potencial innovador como los riesgos que pueden presentar para la privacidad y la seguridad. En un mundo donde el cambio es la única constante, la anticipación y la preparación son esenciales para la protección de los derechos en el futuro digital.

Derechos digitales 2024 es, en última instancia, una llamada a la acción. Es un recordatorio de que, aunque la tecnología puede ser una fuerza poderosa para el bien, su impacto debe ser cuidadosamente gestionado para asegurar que no se convierta en una herramienta de opresión o exclusión. La obra insta a los legisladores, académicos, profesionales y ciudadanos a colaborar en la

construcción de un entorno digital que respete y promueva los derechos humanos.

Uno de los puntos focales de la obra es la inteligencia artificial (IA), una tecnología que, aunque promete transformar industrias enteras, también plantea desafíos éticos y legales significativos. La IA tiene el potencial de mejorar la eficiencia y la precisión en una variedad de campos, desde la atención médica hasta la educación y la justicia. Sin embargo, su capacidad para tomar decisiones autónomas basadas en grandes volúmenes de datos plantea preguntas sobre la responsabilidad algorítmica y la transparencia.

En *Derechos digitales 2024* se examina cómo la IA puede afectar los derechos fundamentales, como la privacidad y la no discriminación. Los algoritmos de IA, si no se diseñan y supervisan adecuadamente, pueden perpetuar sesgos existentes y tomar decisiones injustas. Por ejemplo, en el ámbito de la justicia penal, la IA utilizada para predecir la probabilidad de reincidencia de los delincuentes puede discriminar a ciertos grupos demográficos. Los autores proponen medidas para asegurar que la IA se desarrolle y se utilice de manera ética y transparente, incluyendo la creación de marcos regulatorios que obliguen a las empresas y organizaciones a ser responsables de los impactos de sus algoritmos.

Otro tema crucial abordado en la obra es el de las ciudades inteligentes. A medida que las áreas urbanas se digitalizan cada vez más, se crean nuevas oportunidades para mejorar la eficiencia y la calidad de vida. Sin embargo, esta digitalización también trae consigo riesgos para la privacidad y la seguridad. Los autores discuten cómo las tecnologías utilizadas en las ciudades inteligentes, como los sensores IoT (Internet de las Cosas) y la recopilación masiva de datos, pueden ser explotadas si no se regulan adecuadamente. Proponen soluciones para equilibrar la innovación con la protección de los derechos de los ciudadanos, como la implementación de políticas de privacidad sólidas y la promoción de una gobernanza inclusiva y participativa.

La obra examina asimismo el papel del derecho digital en el ciberespacio, particularmente en el contexto de las operaciones

militares y la seguridad nacional. El ciberespacio se ha convertido en el quinto dominio de las operaciones militares, junto con la tierra, el mar, el aire y el espacio. Esta militarización del ciberespacio plantea desafíos únicos para la regulación internacional y la protección de los derechos humanos. Los autores analizan cómo los gobiernos pueden equilibrar la necesidad de seguridad nacional con el respeto a los derechos digitales de los individuos, proponiendo marcos legales que promuevan la transparencia y la rendición de cuentas en las operaciones cibernéticas.

Además, *Derechos digitales 2024* aborda la cuestión de la *legal-tech*, o la tecnología al servicio del Derecho. La tecnología está revolucionando la práctica legal, desde la automatización de tareas rutinarias hasta la provisión de servicios legales a través de plataformas digitales. Los autores exploran cómo estas innovaciones pueden mejorar la eficiencia y accesibilidad del sistema legal, aunque señalan los desafíos éticos y de regulación que surgen. Por ejemplo, la automatización de la redacción de contratos y la predicción de resultados legales pueden hacer que los servicios legales sean más accesibles, pero pueden dar lugar a preocupaciones sobre la calidad y la equidad de las decisiones automatizadas. La obra propone un enfoque equilibrado que maximice los beneficios de la tecnología legal mientras se mitigan sus riesgos.

El papel de los datos personales en entornos digitales es otro tema central. En una era donde los datos son el nuevo petróleo, la protección de la privacidad de los individuos se ha vuelto crítica. Los autores discuten las herramientas y estrategias disponibles para proteger los datos personales, desde la encriptación hasta las políticas de minimización de datos. Igualmente se abordan los desafíos asociados con la recopilación y el uso de datos a gran escala por parte de empresas y gobiernos, y se proponen soluciones para garantizar que los datos se manejen de manera ética y conforme al respeto a los derechos humanos.

Los derechos digitales no son una mera extensión de los derechos tradicionales; representan un nuevo ámbito en el que nuestras libertades y dignidad deben ser defendidas con igual vigor. En

este sentido, *Derechos digitales 2024* es más que una recopilación de conocimientos; es un llamado a la acción para legisladores, académicos, profesionales y ciudadanos; es un recordatorio de que todos tenemos un papel que desempeñar en la configuración de un entorno digital que promueva la justicia, la igualdad y el respeto a los derechos humanos.

Invitamos a los lectores a sumergirse en esta obra con una mente abierta y crítica. A cuestionar, debatir y, sobre todo, a contribuir activamente en la construcción de un ciberespacio seguro, inclusivo y democrático. La tecnología tiene el potencial de ser una fuerza transformadora para el bien, pero su desarrollo y uso deben estar guiados por principios éticos y de derechos humanos.

Que este libro sirva como una guía y una inspiración para todos aquellos que buscan entender y navegar los complejos paisajes del mundo digital. Que despierte en ustedes una pasión por la justicia digital y una determinación para actuar. En un tiempo de rápidos cambios y avances tecnológicos, *Derechos digitales 2024* es una herramienta esencial para cualquiera que desee estar informado y preparado para los desafíos del futuro.

JULIO CÉSAR BONILLA GUTIÉRREZ

Comisionado Ciudadano del INFO CDMX y académico de la UNAM

Estado regulador y órgano autónomo regulador de las telecomunicaciones en México. Hacia el nuevo orden digital institucional

JOSÉ LUIS MANCILLA ROSALES*

INTRODUCCIÓN

Hablar de la introducción y aplicación de inteligencia artificial y nuevas tecnologías a un país determinado, como lo es el Estado mexicano, implica necesariamente llevar a cabo un estudio multidisciplinario que permita observar todas sus aristas. Ello significa considerar, al menos, el contexto tecnológico, económico, político y legal. No obstante, el objeto del presente consiste en esbozar desde el ámbito jurídico y de forma prospectiva las crecientes necesidades regulatorias de este nuevo orden digital.

Para lo anterior, a lo largo de este artículo veremos, primero, la aproximación al concepto de Estado regulador y en qué consiste la función regulatoria de la cual se arroga para ejercer la rectoría económica del Estado Mexicano a través de la emisión de normas administrativas generales.

En el apartado dos, se muestra a grandes rasgos la evolución que ha tenido la figura de Estado regulador en México, analizando diferentes administraciones presidenciales y la manera en que

* Profesor en las Facultades de Derecho y de Ciencias Políticas y Sociales de la UNAM.

se introdujeron y ejecutaron las políticas públicas relacionadas con los sectores de telecomunicaciones y radiodifusión. Se muestra la transición de un Estado centralizado e intervencionista en la economía a un Estado que resalta la creación de órganos descentralizados (o autónomos), como es el caso del Instituto Federal de Telecomunicaciones.

En el apartado tres se exponen notas características del actual regulador en telecomunicaciones del Estado Mexicano, esto es, el Instituto Federal de Telecomunicaciones, respecto del que se abordan cuestiones que van desde su naturaleza jurídica, integración y descripción de sus facultades regulatorias, administrativas y jurisdiccionales.

Todo ello para finalizar con una visión global del estatus que guarda el nuevo orden digital en el Parlamento Europeo, el cual avanza en la regulación de lo relativo a los procedimientos de evaluación de la conformidad a los que deberán sujetarse proveedores que pretendan comercializar sistemas de inteligencia artificial en la Unión Europea, con lo que se culmina señalando el rol regulatorio que debe desempeñar de forma urgente el Estado mexicano, con acciones que impliquen la adecuada armonización de la normativa mundial al marco jurídico mexicano.

Aproximación al concepto Estado regulador

El Estado es, para doctora María Elena Mansilla y Mejía, “tanto una creación humana como una institución vinculada estrechamente con la naturaleza social del hombre”.¹

Dicha concepción nos obliga a tener presente los orígenes y evolución del ser humano y la manera en que ha decidido, a través del tiempo, organizarse, creando la que quizás sea la institu-

¹ María Elena Mansilla y Mejía, *Derecho internacional privado*, Iure Editores, Colección Textos Jurídicos, México, 2019, p. 30.

ción más importante que se ha dado a sí misma la humanidad: el Estado.

Como bien lo indica Mansilla y Mejía:

...el Estado participa en todas las actividades del ser humano, al propiciarlas, protegerlas y regularlas. [...] Así, el Estado, si bien es una forma de organización de una comunidad de seres humanos, debe estar regulado por normas; en otras palabras, el Derecho regula y limita la actividad del Estado mediante la Constitución; esto lo convierte en un Estado de Derecho. Por su parte, la Constitución determina las funciones del Estado, crea los órganos, las instituciones que lo conforman y las atribuciones que debe cumplir.²

La anterior es una visión integral de lo que es y le corresponde al Estado; de qué y cómo lo regula. Así, el Estado se autorregula y regula. Sin embargo, en cuanto al aspecto organizativo, nuestra autora delimita las funciones del Estado en la tradición moderna de su división o, parafraseando a Bartolomé Clavero, en el contexto de la trinidad constitucional. En líneas posteriores destacaremos que, si bien el Estado conserva la regulación de actividades específicas, también es cierto que la realiza a través de órganos que no forman parte de los poderes legislativo, ejecutivo ni judicial.

Para efectos de este artículo, por *regulación* entenderemos:

[la] función pública encomendada a órganos de la administración directa o a comisiones o agencias independientes, que comprende la aprobación de normas relativas a mercados o sectores económicos concretos, la supervisión y vigilancia de su cumplimiento por las empresas que operan en dichos mercados, especialmente para asegurar la libre competencia y la adopción, en su caso, de las medidas correctoras que procedan, incluida la imposición de sanciones.³

² *Ibidem*, p. 31.

³ “Regulación”, en Santiago Muñoz Machado (Dir), *Diccionario Panhispánico del Español Jurídico* —obra en la que participó la doctora Mansilla y Mejía—, Volumen II, Real Academia Española, la Cumbre Judicial Iberoamericana y el Consejo General del Poder Judicial, España, 2017, p. 1788.

De lo anterior podemos identificar que, en adición a la función legislativa, entendida como la capacidad para expedir las leyes que rigen y se aplican dentro de un territorio específico, el Estado se arroga la función regulatoria; esto es, emitir, a través de instancias estatales, las normas que aplicarán sobre mercados o sectores económicos concretos, con el propósito de garantizar los derechos fundamentales de libre concurrencia y libre competencia, buscando en todo momento la mayor satisfacción y protección de los consumidores o usuarios de tales sectores o mercados; manteniendo el Estado la imposición de las sanciones correspondientes.

En ese contexto, coincidimos con algunas premisas que plantea Gonzalo Sánchez de Tagle, quien señala que el Estado regulador parte de dos notas distintivas: 1) la primera implica la intervención del Estado para remediar fallas en el mercado o con el propósito de proteger intereses públicos que corresponden a la regulación económica y a la regulación social; esta intervención se da a través de órganos de la administración pública o de órganos con autonomía constitucional, y aquí la regulación se manifiesta en disposiciones administrativas de carácter general, cuyo soporte está en facultades específicas y asunción de competencias originarias; y 2) en el caso mexicano, según Sánchez de Tagle, las entidades reguladoras no asumen funciones jurídicas preponderantes, sino que ejecutan facultades de producción, aplicación y adjudicación, situación última que, en el caso del Instituto Federal de Telecomunicaciones, órgano regulador de las telecomunicaciones en México, no coincidimos por las razones que se señalarán en su oportunidad. Concluye el autor que la nota que caracteriza al Estado regulador es su fuente de legitimidad consistente en la eficiencia y deferencia técnica.⁴

Sánchez de Tagle plantea que la diferencia entre el Estado de bienestar, o benefactor, y el Estado regulador consiste en que, en

⁴ Cfr. Gonzalo Sánchez de Tagle P.S., *El Estado regulador en México*, Instituto Belisario Domínguez-Senado de la República, México, 2018, p. 11.

el primero, “el Estado es el encargado de proveer los bienes y servicios a los ciudadanos y, el segundo, parte de la premisa básica de la existencia de mercados libres en donde existen competidores que proveen bienes y servicios. De tal forma que el Estado regulador es un instrumento de la rectoría económica, y esta del Estado social, bajo el supuesto que implica el control estatal sobre las decisiones económicas del país”.⁵

Para el autor en análisis, el Estado regulador es una evolución institucional que deriva de la construcción conceptual de la rectoría económica del Estado, como parte del Estado social de derecho. Así, a través de la emisión de normas administrativas generales, el Estado regulador corrige o previene deficiencias en el mercado y protege intereses públicos a través de normas administrativas generales que usualmente son expedidas y ejecutadas por agencias autónomas y especializadas, bajo el principio de eficiencia técnica.⁶

Como aportación doctrinal consideramos que el Estado regulador es la organización del Estado en la que éste tiende a la aprobación y emisión, a través de órganos con cierto nivel de autonomía, de disposiciones administrativas de carácter general, especializadas y técnicas, relativas a mercados o sectores económicos concretos, que consideran la supervisión y vigilancia de su cumplimiento por los agentes económicos que operan en dichos mercados, especialmente para asegurar las libertades de concurrencia y de competencia, así como la adopción, en su caso, de las medidas correctoras que procedan, incluida la imposición de sanciones, todo ello enmarcado en la protección y satisfacción plena de los consumidores o usuarios de tales mercados o sectores.

⁵ *Ibídem*, pp. 14 y 18.

⁶ *Ibídem*, p. 21.

Esbozo del Estado regulador en México

El establecimiento y evolución del modelo de Estado regulador en México, desde nuestra perspectiva, se configura con mayor distinción durante la administración del presidente Miguel De la Madrid Hurtado, específicamente con las reformas constitucionales que definieron la rectoría económica del Estado, y tendrá uno de sus momentos más trascendentes con la reforma constitucional de 2013 en materia de telecomunicaciones y competencia económica, con la creación del Instituto Federal de Telecomunicaciones y la Comisión Federal de Competencia Económica, como órganos constitucionales autónomos y reguladores en sus respectivas áreas.

Los cambios importantes, y en algunos casos radicales, que ha sufrido nuestro marco constitucional y legal desde 1917 hasta la fecha, han atendido, desde la perspectiva de distintos autores, al proceso de globalización económica y al necesario redimensionamiento del Estado y su aparato gubernamental.

Para nuestro análisis, tomaremos en consideración las aportaciones de tres autores expertos en el tema y quienes destacan la inclusión de la regulación como un elemento fundamental en el cambio de visión e implementación en las políticas públicas, entre ellas, las relacionadas con el sector de telecomunicaciones: Soledad Loaeza, María del Carmen Pardo y José Roldán Xopa.

Soledad Loaeza parte de la premisa siguiente:

Al cumplirse la primera década del siglo *xxi*, el Estado había perdido los rasgos jacobinos que le imprimió la versión original de la Constitución de 1917: la autoridad centralizadora y la capacidad para tomar decisiones de manera unilateral.⁷

⁷ Soledad Loaeza, La metamorfosis del Estado: del jacobinismo centralizador a la fragmentación democrática, en S. Loaeza, y J. F. Prud'homme, (coords.), *Los grandes problemas de México*, tomo XIV Instituciones y procesos políticos, El Colegio de México, México, 2010, p. 24.

En palabras de la misma autora, el jacobinismo “significa, en primer lugar, centralización del poder y, luego, intervencionismo en la economía”.⁸

Esto es, la configuración de un Estado mexicano centralizado que tomaba las decisiones de manera unilateral e intervenía de manera directa en la economía del país. Y, como se verá más adelante, las decisiones recaían en el titular del Poder Ejecutivo Federal, es decir, el presidente de la República.

De acuerdo con Loaeza, distintos factores llevaron al redimensionamiento del Estado mexicano, destacando los siguientes:

- Loaeza afirma que “la finalidad de los instrumentos y de los atributos del Estado autoritario, definidos en la Constitución de 1917, era garantizar su autonomía en relación con los actores internos y la soberanía frente al exterior; ambas características —autonomía y soberanía— eran vistas como condiciones inexcusables para que el Estado pudiera cumplir sus objetivos de transformación social”.⁹
- Nuestra autora indica que la eficacia del modelo jacobino podía medirse por la capacidad que tenía el Estado, en particular el Poder Ejecutivo y el presidente de la República, para someter la voluntad o la autoridad de los actores políticos y tomar decisiones que afectaban el desarrollo general del país, sin previa consulta o negociación con la sociedad como ocurrió en septiembre de 1982.¹⁰
- El 1 de septiembre de 1982, el presidente José López Portillo (1976-1982) hizo el anuncio de la expropiación de la banca que, de acuerdo con Loaeza, aceleró la caída del Estado jacobino, porque provocó una amplia reacción opositora que fue mucho más allá del rechazo a la persona del Presidente y se amplió para cuestionar la autoridad del

⁸ *Ibidem*, p. 39.

⁹ *Ibidem*, p. 35.

¹⁰ *Ibidem*, p. 41.

Estado y la legitimidad de sus atribuciones económicas y de sus funciones políticas. La movilización de rechazo que empezó a articularse a partir de septiembre de 1982 no se limitó a criticar el intervencionismo, sino que, en nombre de la democracia, cuestionó dos de los instrumentos fundamentales del poder estatal: su papel como referente central de las identidades políticas y la centralización de la autoridad en el Presidente de la República y en el gobierno federal.¹¹

- Entre los esfuerzos que hizo el presidente Miguel De la Madrid (1982-1988) para reconstruir las relaciones entre el Estado y los empresarios habría que destacar las reformas constitucionales que definieron la rectoría económica del Estado, con la intención de crear reglas que limitaran el intervencionismo estatal —y limitar la incertidumbre que podía acompañarlo—, que no modificaron esencialmente el carácter mixto de la economía o la estructura del poder económico.¹²
- Con el presidente Carlos Salinas de Gortari (1988-1994), el eje era la reducción del intervencionismo estatal con el argumento de que así se fortalecería el Estado. En ese sentido, el modelo económico que se implantó a partir de los años noventa debía contrarrestar el deterioro del Estado. Así, las principales estrategias del gobierno del presidente Salinas fueron: redefinición del intervencionismo, la liberalización de los mercados, la privatización de empresas públicas, la instalación de la gobernanza como una estrategia de gobierno y la internacionalización de la economía.¹³
- La globalización fue un desafío a la autoridad tradicional del Estado por tres razones: 1) porque era la manifesta-

¹¹ *Ibidem*, p. 39.

¹² *Ibidem*, p. 44.

¹³ *Ibidem*, p. 25.

ción de la expansión extraterritorial de intereses, grupos y empresas que podían desplazarse de una ciudad a otra, de un país a otro, según su conveniencia, y así escapar a la autoridad estatal; 2) la globalización impulsó la ampliación de la agenda internacional hacia terrenos en los que hasta entonces privaba el principio de no intervención, pues, en adición a los temas comerciales o financieros, se incorporaron asuntos como la promoción de la democracia y del bienestar social, el monitoreo de los derechos humanos y la protección del medio ambiente, y 3) la globalización trajo consigo un novedoso fenómeno: la irrupción en el escenario internacional de organizaciones no gubernamentales y de redes sociales comprometidas con la promoción de causas políticas.

- En ese orden, según Loaeza, México no pudo resistir las presiones de la globalización y, en los años noventa, el gobierno del presidente Carlos Salinas comenzó la construcción de un modelo de economía abierta al exterior, cuyos ejes eran la inversión extranjera directa y los mercados internacionales. La participación de agentes externos en la economía mexicana fue mucho más allá de la liberalización comercial, porque se extendió a la reconstrucción estatal. A manera de ejemplo, señala Loaeza, que en los años ochenta y noventa los programas de rescate financiero del Fondo Monetario Internacional y del Banco Mundial estuvieron detrás del diseño de los primeros pasos hacia la reforma del Estado, pues incluían condiciones de cambio estructural relativas a la descentralización, a la autonomía regional, a la privatización de empresas y servicios públicos y a la desregulación del sector financiero.¹⁴

Entre las conclusiones de Loaeza, destaco, para efectos de este artículo, dos:¹⁵

¹⁴ *Ibidem*, p. 52.

¹⁵ *Cfr.* Loaeza, *op. cit.*, pp. 64-65.

- Si bien en los últimos veinte años del siglo xx y la primera década del siglo xxi, el Estado mexicano experimentó una profunda transformación, lo cierto es que no se ha consolidado la capacidad institucional que caracteriza a un Estado moderno como un conjunto de instituciones centrales y radiales que penetran en un territorio delimitado y, por la otra, fracturas sociales profundas han obstaculizado el desarrollo de una sociedad civil fuerte y cohesiva con capacidad para vincularse con el Estado y, así, controlarlo.
- Contrariamente a lo que propusieron los primeros gobiernos del siglo xxi, la clave del fortalecimiento del Estado no se encuentra en lo exterior, sino en la reconstitución de sus vínculos con la sociedad, en la disposición de esta última de apropiarse del Estado, para a partir de ahí fortalecerse ella misma.

De lo anterior se desprende la idea de cómo se ha venido transitando de un Estado jacobino (centralizado e intervencionista en la economía), en palabras de la autora, a un Estado fragmentado o debilitado, principalmente en los aspectos de intervención en la economía nacional y su impacto en la reestructura de la administración pública, resaltando la creación de órganos descentralizados (o autónomos).

No obstante, cabría señalar que los órganos autónomos, como el Instituto Federal de Telecomunicaciones, son órganos del Estado que coadyuvan al cumplimiento de sus fines y podríamos señalar que ayudan a su fortalecimiento bajo un claro marco constitucional y legal, así como su obligación de rendir cuentas a la sociedad mexicana por conducto del Congreso General.

Ahora bien, de acuerdo con María del Carmen Pardo, podríamos señalar que el Estado mexicano ha transitado de un Estado intervencionista a un Estado regulador, atendiendo a los aspectos siguientes:

- La crisis económica que enfrentó México a partir de 1976, y que alcanzó su nivel más crítico en 1982, hizo visibles los

límites del modelo adoptado, sobre todo al haber hecho del Estado el eje central del desarrollo, lo que obligó a un fuerte y creciente endeudamiento y a la búsqueda de financiamiento externo para sostener la inversión y un abultado gasto público.

- La política económica que protegió de la competencia a empresas nacionales otorgándoles, por ejemplo, subsidios indiscriminados y precios preferenciales, no generó los incentivos necesarios para que tuvieran, salvo excepciones, el aliciente de participar en los mercados internacionales. Esto comprometió también la importación de bienes de capital intermedios pues, aunque había empresas que podían contar con el financiamiento necesario, existía una preocupante escasez de divisas de los mercados financieros.¹⁶
- El Estado mexicano adoptó a partir de 1982 el llamado “modelo neoliberal”, que implicaba favorecer los mecanismos de mercado en actividades económicas, reduciendo su participación, regulación y tamaño. Se consideraba que su excesiva presencia en la economía limitaba la competitividad de los mercados. La apertura económica, que comenzó con el ingreso del país al Acuerdo General sobre Aranceles Aduaneros y Comercio en 1986, quedó consolidada con la negociación y firma del Tratado de Libre Comercio de América del Norte, que entró en vigor en 1994.
- En el periodo de 1982 a 2000 empezó un proceso de reformas económicas, que redundaron en una importante reducción del papel del Estado en la economía, a partir de la puesta en marcha de políticas de liberalización comercial, desregulación, privatización y reducción en el gasto público, entre

¹⁶ María del Carmen Pardo, *El Estado mexicano: ¿de la intervención a la regulación?*, en S. Loaeza y J. F. Prud’homme, (coords.), *Los grandes problemas de México*, tomo XIV Instituciones y procesos políticos, El Colegio de México, México, 2010, p. 78.

otras. Con el nuevo modelo, el Estado ya no sería el agente de desarrollo, sino que se encargaría más bien de lograr el equilibrio macroeconómico y la libre competencia. La adopción del modelo neoliberal en México exigió también un importante redimensionamiento del aparato estatal que, se argumentó, había absorbido, con su enorme burocracia, muchos de los recursos fiscales y había sido incapaz de satisfacer las demandas sociales.¹⁷

- En ese orden, el redimensionamiento del Estado se planteó como un insumo de programas de reforma de la administración pública, puesto que se requerían nuevas formas de organización del aparato gubernamental que permitieran superar los problemas fiscales y los de eficiencia entre ingreso y gasto público para dar respuesta a las demandas sociales. En este aspecto, desempeñaron un papel importante las privatizaciones de empresas paraestatales y las reformas regulatorias.¹⁸
- De esta forma, en las últimas dos décadas del siglo xx, el gobierno transformó y redefinió sus funciones y su ámbito de intervención en la economía, y enfatizó que sus acciones debían estar encaminadas de manera mucho más decidida hacia los ciudadanos. Con una economía en su mayor parte liberalizada, el gobierno empezó de manera gradual a asumir funciones de regulador y vigilante, para lo cual se crearon o reformaron diversas dependencias especializadas, las que, como se mencionó, desde sus diseños originales contaron con autonomía técnica y operativa y funcionaron según la figura jurídica de órganos desconcentrados o descentralizados. Su propósito fundamental fue regular un sector específico de la actividad económica o proteger a los

¹⁷ *Ibidem*, p. 82.

¹⁸ *Ibidem*, p. 83.

consumidores de las asimetrías de información o riesgos del mercado.¹⁹

De los anteriores aspectos, podemos identificar la transición de un Estado mexicano intervencionista a un Estado que ha optado por la regulación. Para Kliksberg, citado por Pardo:

[...] la regulación abarca muchos ámbitos de acción y tiene finalidades diversas. En algunos casos, busca asegurar la competitividad en algún sector; en otros, eliminar las asimetrías de información o externalidades a favor de los ciudadanos o bien asegurar los derechos de propiedad. Lo cierto es que la regulación, en todas sus formas (regulaciones antimonopolios, de protección de los consumidores, de estándares de calidad, de protección del medio ambiente, etcétera) aparece como imprescindible para limitar los vicios posibles del mercado.²⁰

Para José Roldán Xopa las reformas constitucionales de 2013, entre las que se encuentra la de telecomunicaciones, incorporaron la regulación como una función particularmente considerada en la Constitución, además de que se las acompañó de una organización estatal igualmente específica. A tal ordenación constitucional de lo económico se le vincula con el denominado “Estado regulador”.²¹

La idea del Estado regulador, indica Roldán, se relaciona con el entendimiento de la función que el Estado debe tener frente al mercado; tal función es la regulación, concebida originalmente desde la economía de mercado. De tal forma que si bien, desde la perspectiva de la economía de mercado éste se autorregula y, por tanto, debe estar libre de interferencias públicas, la regulación, en cambio, consiste en intervenciones públicas ante los fallos del mercado (externalidades, problemas de competencia —monopolios,

¹⁹ *Ibidem*, pp. 85-86.

²⁰ *Ibidem*, p. 87.

²¹ Cfr. José Roldán Xopa, *La ordenación constitucional de la economía. Del Estado regulador al Estado garante*, Fondo de Cultura Económica, México, 2018, p. 117.

monopolio natural, competencia destructiva., déficits de información, bienes públicos, decisiones equivocadas—).²²

Pero la regulación no solamente tiene una explicación en cuanto a su funcionalidad frente a fallos del mercado, sino también a atender las necesidades del desarrollo y la calidad de vida de las personas, lo que obliga a considerar las libertades económicas, así como a los derechos prestacionales y a los bienes públicos o comunes.

De acuerdo con Roldán Xopa:

la función reguladora tiene sus antecedentes normativos en la legislación, de manera que, formalmente, las reformas produjeron la constitucionalización de una función existente en el ordenamiento y cuya gestión se encontraba en la organización pública. El diseño normativo y la gestión administrativa fueron los ámbitos del ejercicio del gobierno en los que se diseña y se gestiona la política regulatoria. El derecho, como herramienta de intervención, y la organización pública son las piezas institucionales de acción pública centrales del Estado regulador. Es una recomposición de las funciones y posiciones del Estado y las administraciones públicas.²³

Como un último registro de las aportaciones de Roldán Xopa, cabe destacar que, para el autor, el servicio público arranca del Estado social y de la satisfacción de necesidades sociales; la regulación de la libertad de mercado y de la necesidad de limitación u orientación basada en el interés público.²⁴

Con el apoyo de las referencias de los tres autores mencionados, podemos identificar la transición en México del Estado jacobino o intervencionista al Estado regulador.

Aunado a ello, cabe tener presente el pronunciamiento que nuestro máximo tribunal ha realizado en el sentido de que en el ordenamiento constitucional y jurídico mexicano ha quedado

²² *Ídem.*

²³ *Ibidem*, p. 120.

²⁴ *Ibidem*, p.124.

plasmada la idea del Estado regulador vinculado, en particular, al sector de las telecomunicaciones, mediante la tesis de jurisprudencia P./J. 46/2015, cuyo rubro es *ESTADO REGULADOR. EL MODELO CONSTITUCIONAL LO ADOPTA AL CREAR A ÓRGANOS AUTÓNOMOS EN EL ARTÍCULO 28 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS*,²⁵ y con el contenido siguiente:

De la exposición de las razones del Constituyente Permanente en relación con la reforma constitucional publicada en el *Diario Oficial de la Federación* el 11 de junio de 2013, se observa que el modelo constitucional adopta en su artículo 28 la concepción del *Estado Regulador, entendido como el modelo de diseño estatal insertado para atender necesidades muy específicas de la sociedad postindustrial (suscitadas por el funcionamiento de mercados complejos), mediante la creación de ciertas agencias independientes –de los órganos políticos y de los entes regulados para depositar en éstas la regulación de ciertas cuestiones especializadas sobre la base de disciplinas o racionalidades técnicas*. Este modelo de Estado Regulador, por regla general, exige la convivencia de *dos fines: la existencia eficiente de mercados, al mismo tiempo que la consecución de condiciones equitativas que permitan el disfrute más amplio de todo el catálogo de derechos humanos con jerarquía constitucional*. Ahora, la idea básica del Estado Regulador, busca preservar el principio de división de poderes y la cláusula democrática e innovar en la ingeniería constitucional *para insertar en órganos autónomos competencias cuasi legislativas, cuasi jurisdiccionales y cuasi ejecutivas suficientes para regular ciertos sectores especializados*

²⁵ Esta tesis jurisprudencial se refiere a las razones aprobadas por nueve votos, contenidas en la sentencia dictada en la controversia constitucional 117/2014, publicada en el *Semanario Judicial de la Federación* del viernes 27 de noviembre de 2015 a las 11:15 horas y en la *Gaceta del Semanario Judicial de la Federación*, Décima Época, Libro 24, Tomo I, p. 382 y, por ende, se considera de aplicación obligatoria a partir del lunes 30 de noviembre de 2015. Énfasis añadido.

de interés nacional; de ahí que a estos órganos se les otorguen funciones regulatorias diferenciadas de las legislativas, propias del Congreso de la Unión, y de las reglamentarias, concedidas al Ejecutivo a través del artículo 89, fracción I, constitucional. Este diseño descansa en la premisa de que esos órganos, por su autonomía y aptitud técnica, son aptos para producir normas en contextos de diálogos técnicos, de difícil acceso para el proceso legislativo, a las que puede dar seguimiento a corto plazo para adaptarlas cuando así se requiera, las cuales constituyen reglas indispensables para lograr que ciertos mercados y sectores alcancen resultados óptimos irrealizables bajo la ley de la oferta y la demanda. Pues bien, *al introducirse el modelo de Estado Regulador en la Constitución, se apuntala un nuevo parámetro de control para evaluar la validez de los actos y normas de los órganos constitucionales autónomos, quienes tienen el encargo institucional de regular técnicamente ciertos mercados o sectores de manera independiente únicamente por referencia a racionalidades técnicas especializadas, al gozar de una nómina propia de facultades regulatorias, cuyo fundamento ya no se encuentra en la ley ni se condiciona a lo que dispongan los Poderes clásicos.*

De lo expuesto, se refleja la existencia en nuestro país de un Estado regulador y, para el análisis de este trabajo, se encuentra plasmado claramente en la Constitución, a partir del 11 de junio de 2013, que también implica un reflejo de la redimensión del Estado mexicano y la administración pública, principalmente en la materia de telecomunicaciones.

Breves notas sobre el órgano autónomo regulador de las telecomunicaciones en México

Mediante 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, en materia de telecomunicaciones* (Decreto constitucional), publicado el 11 de junio de

2013 en el *Diario Oficial de la Federación* (DOF), se creó el Instituto Federal de Telecomunicaciones (IFT) como órgano constitucional autónomo, regulador de los sectores de telecomunicaciones y radiodifusión, y autoridad en materia de competencia económica; además se previeron los aspectos siguientes:

- Los servicios públicos de interés general de telecomunicaciones deben ser prestados en condiciones de competencia, calidad, pluralidad, cobertura universal, interconexión, convergencia, continuidad, acceso libre y sin injerencias arbitrarias (artículo 6o., apartado B, fracción II de la Constitución).
- El servicio público de interés general de radiodifusión debe ser prestado en condiciones de competencia y calidad y brinde los beneficios de la cultura a toda la población, preservando la pluralidad y la veracidad de la información, así como el fomento de los valores de la identidad nacional, contribuyendo a los fines establecidos en el artículo 3° constitucional (artículo 6°, apartado B, fracción III de la Constitución).
- Se prevé que las concesiones para el uso, aprovechamiento y explotación en materia de radiodifusión y telecomunicaciones serán otorgadas por el Instituto (artículo 27 constitucional).
- Se crea al Instituto como un órgano autónomo, con personalidad jurídica y patrimonio propio, cuyo objeto es el desarrollo eficiente de la radiodifusión y las telecomunicaciones, conforme a lo dispuesto en la propia Constitución y en los términos que fijen las leyes respectivas. El Instituto tiene a su cargo la regulación, promoción y supervisión del uso, aprovechamiento y explotación del espectro radioeléctrico, las redes y la prestación de los servicios de radiodifusión y telecomunicaciones, así como el acceso a la infraestructura activa, pasiva y otros insumos esenciales, garantizando lo establecido en los artículos 6° y 7° constitucionales (artículo 28, párrafo décimo quinto de la Constitución).

- El IFT también es la autoridad en materia de competencia económica de los sectores de radiodifusión y telecomunicaciones, por lo que en dichos sectores ejercerá en forma exclusiva las facultades que el propio artículo 28 constitucional y las leyes establecen a la Comisión Federal de Competencia Económica. Así, el Instituto regula de forma asimétrica a los participantes en estos mercados con el objeto de eliminar eficazmente las barreras a la competencia y la libre concurrencia (artículo 28, párrafo décimo sexto de la Constitución).
- El IFT impondrá límites a la concentración nacional y regional de frecuencias, al concesionamiento y a la propiedad cruzada que controle varios medios de comunicación que sean concesionarios de radiodifusión y telecomunicaciones que sirvan a un mismo mercado o zona de cobertura geográfica, y debe ordenar la desincorporación de activos, derechos o partes necesarias para asegurar el cumplimiento de estos límites, garantizando lo dispuesto en los artículos 6° y 7° de la Constitución (artículo 28, párrafo décimo sexto de la Constitución).
- Corresponde al IFT el otorgamiento, la revocación, así como la autorización de cesiones o cambios de control accionario, titularidad u operación de sociedades relacionadas con concesiones en materia de radiodifusión y telecomunicaciones. Además, el Instituto fijará el monto de las contraprestaciones por el otorgamiento de las concesiones, así como por la autorización de servicios vinculados a éstas (artículo 28, párrafo décimo séptimo de la Constitución).
- Las concesiones del espectro radioeléctrico serán otorgadas mediante licitación pública, a fin de asegurar la máxima concurrencia, previendo fenómenos de concentración que contraríen el interés público y asegurando el menor precio de los servicios al usuario final; de acuerdo con la Constitución, en ningún caso el factor determinante para definir al ganador de la licitación será meramente económico. Las

concesiones para uso público y social serán sin fines de lucro y se otorgarán bajo el mecanismo de asignación directa conforme a lo previsto por la ley y en condiciones que garanticen la transparencia del procedimiento.

- La ley establecerá un esquema efectivo de sanciones que señale como causal de revocación del título de concesión, entre otras, el incumplimiento de las resoluciones que hayan quedado firmes en casos de conductas vinculadas con prácticas monopólicas (artículo 28, párrafo décimo octavo de la Constitución).
- El IFT podrá emitir disposiciones administrativas de carácter general exclusivamente para el cumplimiento de su función regulatoria en los sectores de su competencia (artículo 28, párrafo vigésimo, fracción IV, de la Constitución).
- El Instituto está facultado para promover controversias constitucionales (artículo 105, fracción I, inciso I) de la Constitución).

Ahora bien, para dar cumplimiento a lo previsto en el artículo Sexto transitorio del Decreto constitucional, el 10 de septiembre de 2013 el pleno del Senado de la República ratificó a los primeros comisionados del Instituto,²⁶ con lo que dicho órgano autónomo quedó constitucionalmente constituido e integrado.

²⁶ Los primeros comisionados del IFT fueron Luis Fernando Borjón Figueroa (10/09/2013 al 28/02/2016). Ernesto Estrada González (10/09/2013 al 28/02/2017). Adriana Sofía Labardini Inzunza (10/09/2013 al 28/02/2018). María Elena Estavillo Flores (10/09/2013 al 28/02/2019). Gabriel Oswaldo Contreras Saldívar (10/09/2013 al 29/02/2020, designado por el Senado como Presidente del IFT, del 10/09/2013 hasta el 9/09/2017, y reelecto para el periodo del 3/10/2017 hasta el 29/02/2020. Mario Germán Fromow Rangel (10/09/2013 al 28/02/2021), y Adolfo Cuevas Teja (10/09/2013 al 28/02/2022). En sustitución de Borjón fue designado Javier Juárez Mojica (18/10/2016 al 28/02/2025); en lugar de Estrada fue designado Arturo Robles Rovalo (25/04/2017 al 28/02/2026); en lugar de Labardini fue designado Sóstenes Díaz González (25/04/2018 al

De igual manera, para cumplir con lo previsto en el decreto constitucional, el 14 de julio de 2014, en edición vespertina, se publicó en el DOF el *DECRETO por el que se expide la Ley Federal de Telecomunicaciones y Radiodifusión, y la Ley del Sistema Público de Radiodifusión del Estado Mexicano; y se reforman, adicionan y derogan diversas disposiciones en materia de telecomunicaciones y radiodifusión*.

De tal manera que, en adición a lo previsto en la Constitución, con lo establecido en la Ley Federal de Telecomunicaciones y Radiodifusión (LFTR) quedó configurado el órgano autónomo regulador de las telecomunicaciones en México, destacándose, entre otras, las facultades regulatorias, administrativas y jurisdiccionales siguientes:

Regulatorias

- Expedir disposiciones administrativas de carácter general, planes técnicos fundamentales, lineamientos, modelos de costos, procedimientos de evaluación de la conformidad, procedimientos de homologación y certificación y ordenamientos técnicos en materia de telecomunicaciones y radiodifusión (artículo 15, fracción I de la LFTR).
- Emitir disposiciones, lineamientos o resoluciones en materia de interoperabilidad e interconexión de las redes públicas de telecomunicaciones, a efecto de asegurar la libre competencia y concurrencia en el mercado (artículo 15, fracción IX de la LFTR).
- Emitir lineamientos de carácter general para el acceso y, en su caso, uso compartido de la infraestructura activa y pasiva (artículo 15, fracción XI de la LFTR).
- Imponer límites a la concentración nacional y regional de frecuencias, al concesionamiento y a la propiedad cruzada

28/02/2027), y en lugar de Estavillo fue designado Ramiro Camacho Castillo (1/03/2019 al 29/02/2028).

que controle varios medios de comunicación y ordenar la desincorporación de activos, derechos o partes necesarias para asegurar el cumplimiento de estos límites (artículo 15, fracción XIX de la LFTR).

- Determinar la existencia de agentes económicos con poder sustancial en los mercados relevantes que correspondan, así como agentes económicos preponderantes en los sectores de radiodifusión y de telecomunicaciones; e imponer las medidas necesarias para evitar que se afecte la competencia y la libre concurrencia en los mercados materia de la LFTR (artículo 15, fracción XX de la LFTR).
- Declarar la existencia o inexistencia de condiciones de competencia efectiva en el sector de que se trate y, en su caso, la extinción de las obligaciones impuestas a los agentes económicos preponderantes o con poder sustancial (artículo 15, fracción XXI de la LFTR).
- Establecer las medidas e imponer las obligaciones específicas que permitan la desagregación efectiva de la red local del agente económico preponderante en el sector de las telecomunicaciones o del agente que a nivel nacional tenga poder sustancial en el mercado relevante de servicios de acceso al usuario final, de manera que otros concesionarios puedan acceder a los medios físicos, técnicos y lógicos de conexión entre cualquier punto terminal de la red pública de telecomunicaciones y el punto de acceso a la red local pertenecientes a dichos agentes, entre otros elementos (artículo 15, fracción XXII de la LFTR).

Administrativas

- Otorgar las concesiones previstas en LFTR y resolver sobre su prórroga, modificación o terminación por revocación, rescate o quiebra, así como autorizar cesiones o cambios de control accionario, titularidad u operación de sociedades

relacionadas con concesiones (artículo 15, fracción IV de la LFTR).

- Llevar a cabo los procesos de licitación y asignación de bandas de frecuencias del espectro radioeléctrico en materia de telecomunicaciones y radiodifusión, y de recursos orbitales con sus bandas de frecuencias asociadas (artículo 15, fracción VII de la LFTR).
- Fijar tanto el monto de las contraprestaciones por el otorgamiento de las concesiones, así como por la autorización de servicios adicionales vinculados a éstas, previa opinión no vinculante de la Secretaría de Hacienda y Crédito Público (artículo 15, fracción VIII de la LFTR).
- Ejercer las facultades en materia de competencia económica en telecomunicaciones y radiodifusión, en términos del artículo 28 de la Constitución, la LFTR, la Ley Federal de Competencia Económica y demás disposiciones aplicables (artículo 15, fracción XVIII de la LFTR).
- Imponer sanciones por infracciones a las disposiciones legales, reglamentarias o administrativas, o por incumplimiento a lo dispuesto en los títulos de concesión o a las resoluciones, medidas, lineamientos o disposiciones emitidas por el Instituto, dictar medidas precautorias y declarar, en su caso, la pérdida de bienes, instalaciones y equipos en beneficio de la Nación (artículo 15, fracción XXX de la LFTR).

Jurisdiccionales

- Resolver y establecer los términos y condiciones de interconexión que no hayan podido convenir los concesionarios respecto de sus redes públicas de telecomunicaciones conforme a lo previsto en la LFTR (artículo 15, fracción X de la LFTR).

- Resolver los desacuerdos de compartición de infraestructura entre concesionarios, conforme a lo dispuesto en la LFTR (artículo 15, fracción XII de la LFTR).
- Resolver los desacuerdos que se susciten entre concesionarios de redes públicas de telecomunicaciones, entre comercializadores, entre concesionarios y comercializadores o entre cualquiera de éstos con prestadores de servicios a concesionarios, relacionados con acciones o mecanismos para implementar o facilitar la instrumentación y cumplimiento de las determinaciones que emita el Instituto, conforme a lo dispuesto en la LFTR (artículo 15, fracción XIII de la LFTR).

Por último, es de destacarse que las normas generales, actos u omisiones del Instituto podrán ser impugnados únicamente mediante el juicio de amparo indirecto y no serán objeto de suspensión (artículo 28, párrafo vigésimo, fracción VII, de la Constitución); tales juicios de amparo serán sustanciados por jueces y tribunales especializados en materia de competencia económica, radiodifusión y telecomunicaciones (artículos 28, párrafo vigésimo, fracción VII y 94, párrafo sexto de la Constitución).

El nuevo orden digital institucional

En abril de 2024 fue aprobada por el Parlamento Europeo la actualización (corrección de errores) del Reglamento de Inteligencia Artificial de la Unión Europea,²⁷ normativa que sin duda marcará un hito mundial en el tema, al igual que lo fue el Reglamento General de Protección de Datos.

Entre los aspectos que se destacan de ese Reglamento de Inteligencia Artificial es, para efectos de este artículo, el relativo a los procedimientos de evaluación de la conformidad a los que debe-

²⁷ Reglamento de Inteligencia Artificial en la Unión Europea, en https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_ES.pdf.

rán estar sujetos los proveedores de los diversos sistemas de inteligencia artificial que pretenda ser comercializados en la Unión Europea.

Como es sabido, los procedimientos de evaluación de la conformidad refieren al cumplimiento irrestricto de las especificaciones y características técnicas que deben cumplir equipos, productos, dispositivos, sistemas, procesos, y, en ese tenor, se requiere, en principio, el establecimiento de dichas características y especificaciones técnicas, sin perjuicio del respectivo tema de las disposiciones propias para la importación, comercialización y distribución de los equipos, productos, dispositivos, sistemas, procesos.

De ahí que el rol que debe asumir el Estado mexicano exige inmediata atención y acciones que impliquen la adecuada armonía de México en el actuar mundial o, por lo menos, respecto de los socios comerciales.

En ese tenor, y a manera de prolegómenos, se sugieren las acciones siguientes:

- *Del poder legislativo*: la discusión, análisis y aprobación del marco legal relativo a los sistemas de inteligencia artificial.
- *Del poder ejecutivo*: el rediseño institucional administrativo para crear la Secretaría de Tecnologías y Digitalización, que entre otros aspectos tenga a su cargo la política digital de inclusión digital, así como fortalecer las atribuciones de la Secretaría de Economía y a la Procuraduría Federal del Consumidor en cuanto a la expedición de Normas Oficiales Mexicanas (importación, comercialización y distribución), y de protección más específica a los consumidores mexicanos de los sistemas de inteligencia artificial.
- *Del Instituto Federal de Telecomunicaciones*: derivado de la expedición del ordenamiento legal respectivo por parte del Congreso General, expedir las disposiciones técnicas correspondientes y establecer un sistema efectivo de laboratorios de prueba para el cumplimiento de las especificaciones y características técnicas respectivas; fortalecer sus atribuciones

técnicas para atender en la inmediatez todo lo relativo a los sistemas de inteligencia artificial.

CONCLUSIONES

En el presente artículo hemos señalado que el Estado regulador es la organización del Estado en la que éste tiende a la aprobación y emisión, a través de órganos con cierto nivel de autonomía, de disposiciones administrativas de carácter general, especializadas y técnicas, relativas a mercados o sectores económicos concretos, que consideran la supervisión y vigilancia de su cumplimiento por los agentes económicos que operan en dichos mercados, especialmente para asegurar las libertades de concurrencia y de competencia, así como la adopción, en su caso, de las medidas correctoras que procedan, incluida la imposición de sanciones, todo ello enmarcado en la protección y satisfacción plena de los consumidores o usuarios de tales mercados o sectores.

El modelo de Estado regulador en México se refleja en el artículo 28 constitucional con, entre otros elementos, la creación del Instituto Federal de Telecomunicaciones como órgano constitucional autónomo y órgano regulador de las telecomunicaciones.

Así, el Instituto es una autoridad del Estado, pues surge como un órgano constitucional autónomo y un objeto específico; es un regulador, pues expide las disposiciones administrativas de carácter general en los sectores de telecomunicaciones y radiodifusión; es una autoridad administrativa, ya que realiza y ejecuta actos administrativos (concesión) y de autoridad (administra el espectro radioeléctrico y sanciona); es una autoridad jurisdiccional, puesto que resuelve desacuerdos entre agentes económicos regulados, y es una autoridad con deferencia técnica y especializada por los sectores que regula y vigila.

Sin duda, hay un nuevo orden mundial en el que los sistemas de inteligencia artificial cobrarán cada día mayor importancia e impacto en el ejercicio de derechos fundamentales, en la econo-

mía, en la sociedad en general, y en el diseño de los Estados en el mundo. De ahí la necesidad de fortalecer las instituciones del Estado mexicano para responder en la inmediatez a dichos escenarios disruptivos.

A manera de corolario, recupero una de las últimas aportaciones académicas de Mansilla y Mejía, quién al definir la Razón de Estado, indicaba:

el Estado es un organismo cuya fuerza no se mantiene plenamente, más que si le es posible desenvolverse y crecer, la razón de Estado indica también los caminos y las metas de este crecimiento.²⁸

En ese orden el Estado regulador debe cumplir con las metas de crecimiento del Estado mexicano trazadas en nuestro texto constitucional.

REFERENCIAS BIBLIOGRÁFICAS

Constitución Política de los Estados Unidos Mexicanos. DOF del 5 de febrero de 1917. Última reforma publicada el 6 de marzo de 2020.

Contreras Bustamante, Raúl, y de la Fuente Rodríguez, Jesús (coords.), *Diccionario Jurídico*, Facultad de Derecho, UNAM y Tirant Lo Blanch, México, 2019.

Decreto por el que se expiden la Ley Federal de Telecomunicaciones y Radiodifusión, y la Ley del Sistema Público de Radiodifusión del Estado Mexicano; y se reforman, adicionan y derogan diversas disposiciones en materia de telecomunicaciones y radiodifusión. DOF del 14 de julio de 2014.

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, en materia de telecomunicaciones. DOF del 11 de junio de 2013.

²⁸ María Elena Mansilla y Mejía, “Razón de Estado”, en Raúl Contreras Bustamante y Jesús de la Fuente Rodríguez (Coords.), *Diccionario Jurídico*, Facultad de Derecho, UNAM y Tirant Lo Blanch, México, 2019, p. 1501.

Diccionario Panhispánico del Español Jurídico, II volúmenes, dirigido por Santiago Muñoz Machado, Real Academia Española, la Cumbre Judicial Iberoamericana y el Consejo General del Poder Judicial, España, 2017.

Ley Federal de Telecomunicaciones y Radiodifusión. DOF del 14 de julio de 2014. Última reforma publicada el 24 de enero de 2020.

Loaeza, Soledad, La metamorfosis del Estado: del jacobinismo centralizador a la fragmentación democrática, en Loaeza, S. y Prud'homme, J. F. (coords.), *Los grandes problemas de México*, tomo XIV Instituciones y procesos políticos, El Colegio de México, México, 2010.

Mansilla y Mejía, María Elena, *Derecho internacional privado*, Iure Editores, Colección Textos Jurídicos, México, 2019.

Pardo, María del Carmen, El Estado mexicano: ¿de la intervención a la regulación?, en Loaeza, S. y Prud'homme, J.F (coords.), *Los grandes problemas de México*, tomo XIV Instituciones y procesos políticos, El Colegio de México, México, 2010.

Reglamento de Inteligencia Artificial en la Unión Europea, visible en: https://www.europarl.europa.eu/doceo/document/TA-9-2024-0138-FNL-COR01_ES.pdf.

Roldán Xopa, José, *La ordenación constitucional de la economía. Del Estado regulador al Estado garante*, Fondo de cultura Económica, México, 2018.

Sánchez de Tagle P.S., Gonzalo, *El Estado regulador en México*, Instituto Belisario Domínguez-Senado de la República, México, 2018.

Legaltech: la tecnología a disposición del Derecho, una nueva oportunidad de negocios, el cambio en la prestación de servicios jurídicos o la inédita forma de aprender, enseñar, ejercer, comercializar y crear el Derecho

SONIA VENEGAS ÁLVAREZ¹

INTRODUCCIÓN

El presente artículo de investigación jurídica acerca del *legaltech* aborda desde una amplia perspectiva lo que para muchos únicamente se trata del uso de ordenadores y algunas tabletas por abogados modernizados que confrontados con la vieja escuela y sus arcaicos métodos se encuentran insertos en la Era Digital. Para sorpresa de ese sector de la población y de otros tantos quizá un poco más versados en la materia, el sector de la tecnología digital amenaza con romper nuestra visión sobre múltiples campos del Derecho: enseñanza, aprendizaje, ejercicio profesional, creación, aplicabilidad etcétera, aparte de que no existe prácticamente resquicio del mundo jurídico que se haya escapado a la eclosión de la inédita forma de comprender la relación entre el Derecho y la tecnología.

¹ Directora de la Facultad de Derecho de la Universidad Nacional Autónoma de México.

Desde la metodología aquí propuesta dos aristas sostienen una incompreensión del fenómeno: acepción y contemporaneidad. Tras un trajinar de definiciones y concepción entre vocablos afines es posible decantarse (de la mano de los especialistas en la materia) por una voz que aluda a la misma realidad que se trata de nombrar y describir, lo que a su vez conlleva retrotraerse en el tiempo e identificar los fenómenos del día a día que dan cuenta del cambio en la realidad y del cómo ha terminado por manifestarse en el fenómeno que actualmente conocemos como *legaltech*.

Después de esa reveladora parte, se puede acceder a una descripción de los quehaceres otrora reservados a personas peritas en el Derecho que en nuestros días son desempeñados no sólo con mayor eficacia y eficiencia sino a un menor costo y tiempo por algoritmos, los cuales, no obstante, siguen nutriéndose de seres humanos, cuyos conocimientos jurídicos resultan aún vitales: creación de redes de negocios, cuestiones operativas y de análisis son los sectores de mayor relevancia para el *legaltech*. Esos quehaceres adquieren una naturaleza prístina sí los podemos ligar a la producción de productos y servicios legales cercanos al común de los abogados: redacción de contratos, recordatorio de citas con los clientes, organización de documentos en función de su relevancia, resolución de disputas, corrección de errores, predicción de resultados en el litigio, y qué puede decirse acerca del diseño de sistemas operativos de máquinas y herramientas respetuosas del ordenamiento jurídico o instrumentos que solucionen nuestras empantanadas problemáticas fuera de los juzgados. Alguno de nosotros ¿ha pensado en la posibilidad de ejercer el Derecho en una realidad virtual o en el metaverso? Ésas son tan sólo algunas de las muchas promesas y realidades que abraza el fenómeno *legaltech*.

Porque tal como se repetirá hasta la saciedad, el *legaltech* cambió prácticamente cada rubro del Derecho desde su aprendizaje y enseñanza, el ejercicio profesional, su comercialización, la forma en que nos empleamos, la dinámica de cumplimiento del orden

jurídico, el modo de hacer negocios a través de lo jurídico y, quizá lo más acuciante, el modo en que tasamos el valor de nuestros conocimientos como profesionistas legales.

Nociones esquivas

Legaltech es uno de los temas cuya popularidad tanto ha empantanado el panorama que su alrededor circundan nociones de contenido tan errado que amenazan incluso su propia naturaleza; a juicio del autor, de las muchas que podrían abordarse dos son fundamentales: la supuesta modernidad y la inocente explicación de lo que el *legaltech* implica.

Ahondar en la inocente explicación sobre *legaltech* busca sobre todo desarraigar de los lectores la idea del uso de tecnologías (mayoritariamente internet) por parte de los abogados en el desempeño de su quehacer cotidiano como única explicación acerca del tema en cuestión, porque se trata principalmente de una disrupción en el ejercicio del Derecho, pero también en la adquisición de servicios jurídicos y el proceso de enseñanza-aprendizaje de éste.

La reflexión del cómo se crea el conocimiento jurídico es el punto ideal frente al *legaltech*: los servicios jurídicos son intensivos en conocimiento, ello quiere decir que el principal recurso para la creación de valor es el capital humano de los profesionales del Derecho, es decir, el trabajo y no tanto el capital económico; debido a ello la mayoría de los despachos de abogados han basado sus modelos de negocio en la venta de asesoramiento jurídico especializado por horas. Por otro lado, en la Administración Pública o el Poder Judicial cada funcionario o juez tiene que verificar la realidad de los hechos en las normas, seleccionando e interpretando el Derecho aplicable al caso, y emitir los oportunos pronunciamientos para resolver, conforme al ordenamiento jurídico la pretensión ejercitada, cuidándose también la ejecución de la resolución. Ese cúmulo de operaciones deben realizarlas los operadores jurídicos de carne y hueso, desplegando las correspondientes

capacidades intelectivas y volitivas que conforman el núcleo de la función de administrar o juzgar.²

Y, sin embargo, esa forma de trabajo, que aprendimos en las universidades y replicábamos hasta hace algunos días, ha sido trastocada de una forma que, al principio, se asumió sutil y que a la postre terminó por transformarla: desde hace algún buen tiempo se fueron gestando nuevas formas de prestar servicios jurídicos, en las que los nuevos proveedores se afianzaran con firmeza en el mercado y el funcionamiento de nuestros tribunales se transformara. A menos que se adapten, muchos negocios jurídicos tradicionales fracasarán. Por otro lado, se presentará un conjunto completo de nuevas oportunidades a jóvenes emprendedores y creativos abogados. De ese cambio tres son los motores: el desafío más por menos, la liberalización y la tecnología de la información.

Bajo esa postura, el dilema *más por menos* engloba a la totalidad de las realidades que no pueden costear los servicios de un abogado: desde los directores jurídicos en las corporaciones, presionados en la reducción del personal y el aumento de la carga de trabajo, hasta el ciudadano promedio enfrentan la realidad sin saber, bien a bien, las implicaciones legales de su actuar. Todos coinciden en que los servicios jurídicos están reservados a las minorías que pueden pagarlos. El segundo frente, la liberalización —que no es lo mismo que la desregulación—, describe la irrupción en el mercado de los servicios jurídicos de nuevos agentes competidores que, sin ser necesariamente abogados, proveen de servicios jurídicos a los clientes, no sólo de formas más eficaces sino también más económicas, sin que estén comprometidos con las formas tradicionales de trabajo; se han divorciado de la idea del servicio jurídico realizado por abogados, cuyos costosos honorarios se pagan en función de las horas que trabajan. Por el contrario, al centrarse

² Moisés Barrio Andrés, *Legal Tech y la transformación del sector legal, La transformación digital de la abogacía*, España, 2003, p. 16.

en la fuerza del proveedor mayorista, el cálculo de los honorarios ha terminado por desvincularse del tiempo invertido. De esa liberación, un aspecto central es la apertura del mercado a actores no abogados que, sin importar su instrucción académica, suministran asistencia legal.

En última instancia, se ubica la tecnología y el uso que se ha pronosticado que tendrá en la provisión de servicios jurídicos. No se trata de la simple informatización y racionalización de procesos manuales e ineficientes; el cambio va más allá de la automatización, porque es, sobre todo, innovación, o sea, la realización de tareas jurídicas que resultaban inimaginables. De allí el apelativo de tecnologías disruptivas, aquellas que han desafiado y cambiado el funcionamiento de una empresa o de un sector: tecnologías que ayudan a desbancar y provocan la desaparición, incluso de empresas líderes en un sector del mercado; en cuyas primeras etapas de gestación los líderes del mercado y sus clientes descartan esos nuevos sistemas al calificarlos de superficiales y con pocas probabilidades de éxito, aun cuando más tarde reconocen su gran aceptación sin ya poder recuperar el terreno perdido; ese escenario es el ideal para una oferta de servicios jurídicos más amplia, eficiente y a menor costo.³

Actualmente muchos abogados ejercen el Derecho de la misma forma que lo han ejercido sus colegas durante siglos ofreciendo a sus clientes soluciones a medida, altamente personalizadas y diseñadas a las necesidades particulares de cada uno, cuyo costo es alto y, por tanto, con una cartera de clientes limitada. Esa situación se enfrenta, por un lado, a la disrupción de la tecnología, pero, sobre todo, al cambio del factor clave en el mercado: la demanda. Ciertamente, el consumidor, que la pandemia covid-19 dejó tras de sí, solicita habilidades compaginadas al trabajo remoto, migrando hacia la virtualidad, y el incremento de las

³ El ejemplo que permite ilustrar esta idea remite a Kodak, cuyo negocio se vio interrumpido por las cámaras digitales; Richard Susskind, *El abogado del mañana. Una introducción a tu futuro*, 2017, España, p. 1.

expectativas en servicios jurídicos más rápidos y responsables. Es claro que la tecnología ha sido usado como una forma de intervención en la búsqueda de solventar retos propios del quehacer jurídico en el orbe.⁴ Adicionalmente conviene recordar que la tecnología ha tenido un impacto especial en tareas destinadas a la agregación, organización e información, precisamente las que los abogados promedio realizan: bibliotecas, base de datos jurisprudenciales y cursos de Derecho o asesorías y redacción de documentos. El panorama es, pues, otro.

Y frente a cualquier atisbo de duda, los clavos del ataúd han sido puestos por la autorrepresentación judicial: tradicionalmente el sistema de impartición de justicia se ha construido sobre un modelo adversarial de dos partes, dos abogados y un juez. Sin embargo, la incidencia de personas que deciden representarse por sí solas y las legislaciones que lo permiten muestra claros signos de incremento. Eso implica que incluso el propio sistema judicial está siendo obligado a tomar acciones que *nivelen la cancha* para aquellas personas que prescinden de un experto en Derecho que los represente (la estandarización y simplificación de formatos y procesos es uno de esos esfuerzos).⁵

De tal suerte, sin importar mucho lo que, en términos de conceptos y definiciones pueda decirse sobre *legaltech*, no puede continuarse entendiendo como el uso de internet en la prestación de algunos servicios complementarios a la asesoría jurídica- El *legaltech* es, en su forma más simple, la nueva forma de ejercer, prestar y adquirir los servicios jurídicos tradicionales y, en su forma más acabada, la creación de otros que no hemos ni siquiera vislumbrado.

⁴ Siddharta Peter de Souza, The Spread of Legal Tech Solutionism and the Need for Legal Design, *European Journal of Risk Regulation*, N° 13, 2002, p. 374.

⁵ *Illinois State Bar Association's, Report and Recommendations of the Illinois State Bar Association's Task Force on the Future of Legal Services*, 2016, p. 4.

Legaltech vs. lawtech

En la bibliografía disponible no se observa una disputa férrea sobre lo oportuno o inoportuno que pueda resultar el intercambio indiscriminado de locuciones como el *legaltech* y *lawtech*.⁶ Instituciones de arraigado reconocimiento en el *common law*, como la Law Society conciben desde una misma perspectiva al *legaltech* y *lawtech*: en términos amplios, son las tecnologías, cuyo objetivo es apoyar, complementar o reemplazar métodos tradicionales de entrega, prestación o transacciones legales o, bien, mejorar la operación del sistema de justicia. Como sector, el *lawtech* abraza a las compañías que proporcionan servicios legales mediante mecanismos tecnológicos, y vendedores que desarrollan y proveen soluciones tecnológicas a esas empresas o negocios.⁷

Sin embargo, con el ánimo de dar a conocer tantos enfoques como sea posible, cabe la distinción entre ambos términos, considerando, por un lado, que el término *legaltech* suele asociarse a tecnologías propias de la oficina, como pueden ser los sistemas contables, y se vinculan mucho menos a las nuevas tecnologías jurídicas, pero, desde otra mirada, es el término adecuado que describe las actividades del sector, puesto que *legal* alude a la industria legal, al mercado legal y al sector también legal pensando en la tecnología que se emplea justamente por ese sector de la economía. Por el contrario, *lawtech* recuerda al ejercicio del Derecho, o al campo de conocimiento que se enseña y se aprende en las universidades o al entramado jurídico que regula a la sociedad. En todo caso, ese término resulta adecuado únicamente si se habla de un subgrupo específico enfocado al Derecho: redacción de documentos o quizá ayuda en el entendimiento de asuntos jurídicos.⁸

⁶ Que sin ser las únicas son las más socorridas.

⁷ The Law Society, *Introduction to LawTech. A Practical Guide to Legal Technology*, 2019, p. 9.

⁸ Conforme a lo consultado en el portal electrónico *Legal Geek* programa especializado en el apoyo a *star ups* del sector *legaltech* o *lawtech*, en #LegalTech v #LawTech-WTF?—Legal Geek.

Es posible también analizar el contenido del *legaltech* a través de la atomización de sus componentes, por un lado, acotando el contenido de lo jurídico y de lo tecnológico. Lo primero se relaciona siempre con planes sociales, cuya materialización son normas jurídicas, ordenamientos, principios, es decir, todo aquello que comúnmente se conoce como Derecho. De allí que, para ser tecnología jurídica, ésta debe relacionarse con esas normas u ordenamientos jurídicos, pero esa interacción ha de desenvolverse en el corazón del Derecho en sí mismo, por lo que válidamente puede señalarse que se estará frente al fenómeno del *legaltech* cuando se hable de todo tipo de dispositivos capaces de ser empleados como medios para interactuar con el núcleo del Derecho o, bien, para asistir a esa interacción, así como las habilidades y técnicas que empleamos para echar mano de ellos.⁹

El pujante sector de la academia española especializada define a la tecnología legal como la adopción de tecnología y *software* innovadores para racionalizar y mejorar los servicios jurídicos: herramientas, aplicaciones y plataformas que han sido desarrolladas específicamente para el sector legal. Las empresas *legaltech* son generalmente *startups* fundadas con el propósito específico de disrumpir la práctica de las profesiones jurídicas.¹⁰ O el conjunto de empresas y de proyectos que ofrecen soluciones y servicios jurídicos, cuyo objetivo común es, por medio de tecnología novedosa, aportar un valor añadido frente a las soluciones jurídicas tradicionales aprovechando, en particular, todas las posibilidades, medios y herramientas tecnológicos y digitales que ofrece la sociedad de la información, o que son implícitas a ésta. En un sentido amplio, estas soluciones se pueden ofrecer a todo tipo de empresas y empresarios individuales, tanto si están supervisadas como si no. De esta forma, comprenderían a la

⁹ Ryan Whalen, Defining Legal Technology and its Implications, *International Journal of Law and Information Technology*, 2022, pp. 4-6.

¹⁰ Barrio, *op. cit.*, pp. 31-ss.

prestación innovadora de servicios legales dirigidos a satisfacer las necesidades de la actividad clásica de cualquier despacho de abogados o de cualquier equipo legal interno, o departamentos de cumplimiento normativo y de auditoría interna: dirigidos a simplificar la redacción de contratos o escritos procesales o extraprocesales, autenticación de escritos, acceso a bases de datos o espacios de *marketing*, mientras que, en el sentido estricto, se alude al conjunto de empresas y proyectos digitales dirigidos a la renovación y transformación, esencialmente digital, de los agentes que integran el sector de asesoramiento legal, lo que no sólo afecta a los abogados sino también a otros colectivos, asistiendo todos ellos a una auténtica revolución en los códigos que hasta hace uno años regían su actividad.¹¹

Igualmente complejo es el enfoque de la academia alemana, profundamente interesada en el estudio de temas afines al *legal-tech*. Para ellos el término describe el uso de tecnologías digitales en la identificación, interpretación y aplicación del Derecho y, en algunas instancias, para su creación. Como resultado, en su forma tradicional el Derecho está siendo ejercido en nuevas formas y, en algunos casos, ha sido reemplazado.¹²

Y, desde una última postura, *legal technology* se refiere al empleo de la información digital y las tecnologías de la comunicación para automatizar la totalidad o parte del trabajo que implica un proceso legal, para ofrecer apoyo a los productores de servicios jurídicos, así como proveer información jurídica y asesorar directamente a clientes y consumidores. Sin que pueda dejar de mencionarse otras tecnologías como el procesamiento, e-mail, internet, herramientas de manejo y distribución de labores reconociéndose en todo caso, la adopción de herramientas jurídicas

¹¹ José Eduardo Delgado Larena-Avellaneda, *Legal Tech y Fin Tech, La transformación digital de la abogacía*, España, 2003, pp. 4-5.

¹² Wolfgang Riem-Hoffmann, *Legal Technology/Computational Law. Preconditions, Opportunities and Risks*, *Journal of Cross-Disciplinary Research in Computational Law*, November, 2020.

más complejas y específicas como parte de un cambio cualitativo en la forma en que el conocimiento y la pericia jurídica es usada y compartida en la sociedad.¹³

De la supuesta contemporaneidad del *legaltech*

Una vez aclarado el panorama conceptual en torno a *legaltech*, una segunda cuestión queda por puntualizar: la supuesta contemporaneidad de las tecnologías aplicadas al quehacer jurídico. La obvia tentación es imaginar al *legaltech* como un fenómeno contemporáneo, y en cierta forma lo es. La explosión de su aplicabilidad únicamente puede entenderse a sazón de nuestro tiempo. Sin embargo, conviene tener en cuenta tres etapas sucesivas y acumulativas que explican el estado del arte.

El antecedente primigenio puede retrotraerse a los años sesenta, con los primeros intentos de los europeos y americanos de crear sistemas de búsqueda de información jurídica automatizada que, si bien en su mayoría no trascendieron de lo experimental, hubo avances significativos en el diseño de dichos sistemas: con *Lexis* y *Westlaw* como marcas insignes en el mercado de búsqueda de información jurídica. Paralelamente, tuvo lugar la implosión de los sistemas expertos diseñados de un modo demasiado específico y aplicables a pequeñas áreas del conocimiento jurídico o enfocados a la resolución de cuestiones burocráticas, y no a la solución de problemáticas legales.

La segunda etapa puede ubicarse entre 1991 y 2012, marcada según los expertos por el cambio en el mercado, bajo el mandato de la tecnología digital: la masificación del ordenador portátil y personal y su consecuente abaratamiento, la amplificación de los diseños tecnológicos, y la creación de un mundo *web* donde todos participan a través de uso, pero también de su construcción,

¹³ Julian Webb, *Legal Technology: The Great Disruption?*, *Melbourne Legal Studies Research Paper Series*, N° 897, pp. 5-ss.

que en el terreno legal trascendieron de seis maneras distintas: la automatización de los documentos legales, la solución de problemáticas del Derecho por medio de herramientas tecnológicas, el desarrollo de sistemas de almacenamiento de información legal y la democratización en su acceso, el desarrollo de esquemas *on line* por parte de las empresas —dirigidos a sus potenciales clientes, en los cuales se comparten información y recursos relevantes, hasta el diseño de portales electrónicos interactivos, retroalimentativos—, el diseño de manejo de casos y la creación de redes de trabajo digitales, y, por último, la digitalización del sistema de justicia (y, en todo caso, el denominado “gobierno electrónico”), son características distintivas de esta época.

El tercer periodo, que comienza en 2012 y se extiende a nuestros días, se distingue por la aplicación de la inteligencia artificial al Derecho: mecanismos de aprendizaje automático, el análisis jurídico, *blockchain*, con la intención de crear sistemas integrados que combinen la provisión del manejo de proyectos, la automatización de documentos, flujos de trabajo, esquemas de cobro, la creación de portales interactivos con los clientes, y las interesantes propuestas de un sistema judicial completamente digitalizado¹⁴ que, en suma, desembocan en un ecosistema emergente, complejo, en el cual puede diferenciarse la naturaleza de las tareas que el *legal tech* ha revolucionado, no sólo en el modo en que se efectúan sino en la manera en que se crean.

El sector *legaltech* en la práctica

La forma idónea de acercarse al mundo *legal tech* más allá del devenir histórico o de las distinciones conceptuales y definiciones podría ser a través de la ejemplificación del cómo se manifiesta en la cotidianeidad jurídica; en términos extremadamente asequibles,

¹⁴ Idem.

se trata de servicios legales en línea y de plataformas de análisis de datos, mercados profesionales para abogados, soluciones para generar documentos legales y contratos, *software* de gestión especializado en oficinas profesionales, soluciones en materia de probanzas y portales electrónicos que resuelven interrogantes y cuestiones legales. A dichas actividades también puede conocerse en función de lo que pueden hacer por el Derecho: como tecnologías habilitadoras siempre que su función sea facilitar el desarrollo de procesos internos; herramientas que mejoran procesos, que promueven nuevas eficiencias en la administración de casos y procesos que abarcan desde la gestión de los recursos humanos, el *marketing*, el soporte al cliente y la cobranza, y las que hacen mayor ruido a los abogados, las enfocadas al Derecho sustantivo que implican labores de apoyo o de posible reemplazo de los peritos legales.¹⁵

Tratándose de uno de los mercados mayores y más desarrollados para las *startups*, como lo es el inglés, esas iniciativas de negocio se desdoblán en dos grandes rubros: el manejo de negocios y el desarrollo del trabajo. Si se trata de todas las actividades que solicitan operación, organización o el empleo de profesionales, se está frente al manejo de un negocio, mientras que el desarrollo de un trabajo engloba a todas las actividades que conlleva un trabajo jurídico para los clientes. De tal manera, el manejo empresarial requiere modelos de *startups* dedicadas a la gestión de recursos humanos y económicos, clientes y la organización operativa de finanzas y actividades diarias, mientras que el desarrollo del trabajo se ve reflejado por la creación de documentos y contratos, el litigio y las transacciones con los clientes.

De todo ese universo se analiza en esta primer parte lo concerniente al modelo empresarial, puesto que el desenvolvimiento del trabajo rutinario se detallara en un apartado posterior.

¹⁵ Erick Rincón Cárdenas, y Valeria Martínez Molano, *Legaltech. ABC de los servicios legales en la era digital*, Universidad del Rosario y la Cámara de Comercio de Medellín para Antioquia, 2000, Rosario, pp. 7-8.

Manejo de recursos humanos. Previo al advenimiento de los diversos modelos de contratación laboral, las consternaciones de las firmas consistían en la caza y firma de talentos, no obstante, ese modelo está superado. Actualmente los modelos de negocio no operan más con un número de personal fijo e inamovible sino a través de proveedores y plataformas flexibles.

Manejo operativo y finanzas. En el corazón de cada despacho jurídico o en el departamento legal de cada empresa existe un equipo de especialistas enfocados en los asuntos financieros de la empresa (bien, analizando el cómo está siendo gastado el dinero, analizando su rentabilidad, bien, el valor creado por cada departamento, elaborando planes a futuro por citar algunos), la tendencia apunta hacia la adopción de soluciones digitales que permitan almacenamiento en la nube, el análisis de datos e incluso el diseño de sistemas híbridos entre el gobierno corporativo y el equipo legal que reconocer la utilidad de emplear los mismos datos en diferentes modos.

Manejo de clientes. Un adecuado manejo de clientes es la llave hacia el éxito: el uso del *marketing* digital es la nueva herramienta para ganar clientes cuyo especial obstáculo es el cumplimiento de la normativa en materia de protección de datos personales, por lo que el mercado actual se basa en el desarrollo de herramientas diseñadas sólo para empresas legales.

Manejo de conocimiento. Las soluciones digitales se enfocan desde la correcta colocación de los expertos en las áreas en que mejor se pueden desempeñar al interior de las empresas, hasta el manejo de los emails, extracción de información de contratos y documentos o bien el identificar, crear, organizar, buscar y compartir conocimiento.

Manejo de posibles problemáticas. Dentro del sistema del *common law* existe una obligación a cargo de las empresas y los profesionistas dedicadas al Derecho de contar con instrumentos que respondan y respalden a sus clientes frente a posibles quebrantos e infracciones en el desempeño de sus servicios, por lo cual el sector de las *startups* se ha enfocado en la elaboración de soluciones ante posibles escenarios de insolvencia, mala práctica o consejo profesional.¹⁶

¹⁶ Cfr. Thomson Reuters, *Legaltech Startup Report 2019. A Maturing Market*, 2019, pp. 6-ss.

Otro acercamiento puede intentarse dividiendo el campo del *legaltech* en cuatro cuadrantes: 1) redes de trabajo especializadas en la operación de personas, servicios y agencias; 2) conocimiento: inteligencia, información, realización de contenidos y procesos; 3) *software*: elaboración de programas de apoyo, complemento o reemplazamiento de peritos, y 4) plataformas: puntos de encuentro entre la demanda y la oferta y proveeduría de servicios legales genéricos.¹⁷ Asimismo, pueden considerarse las áreas en cuales el *legaltech* brinda soporte: negocio-consumidor; empresa-empresa y otras aplicaciones internas. Las aplicaciones enfocadas al impulso de la interacción entre los abogados y sus clientes, como los *chatbots* que responden dudas jurídicas simples y remiten al usuario a la empresa de tornarse complicada una solución, mercados digitales en los cuales es posible concentrar y comparar precios y opiniones sobre la calidad de los servicios prestados o la solución de controversias digitales entre vendedores y consumidores, se habla de aplicaciones *empresa-cliente*. Por otro lado, algunas apps han sido diseñadas para facilitar la comunicación entre empresas, la transmisión segura y eficaz de documentos hacia otros despachos, tribunales, oficinas gubernamentales o sus propios clientes. Incluso algo tan sencillo y problemático, como la generación de facturas y cuentas de cobro, son vivos ejemplos de las aplicaciones *negocio-negocio*. En última instancia, la expresión de la tecnología jurídica en la *aplicación interna* alude a las funciones que apoyan e incentivan la ejecución del proceso legal que no requiera de una interacción directa con el cliente, como la detección de pagos de procedencia ilícita, y la cuantificación de las acciones intentadas por los reclamantes, por mencionar algunas.¹⁸

¹⁷ Archil Chochia, *et al*, Legal Technology for Law Firms: Determining Roadmaps for Innovation, *Croatian International Relations Review*, May 2018, p. 95.

¹⁸ Ciaran Harper, y Sarah Zhang, *Legal Tech and Lawtech: Towards a Framework for Technological Trends in the Legal Services Industry*, pp. 1-ss, en

El mundo que conocíamos a través de la lente *legaltech*

Todo lo que órbita alrededor de la tecnología jurídica posee, en su justa medida, relevancia probada: desde la distinción conceptual, el devenir histórico, hasta la aplicación práctica, son aspectos esenciales que, vistos en su conjunto, permiten hacerse una idea cabal del fenómeno. Sin embargo, el aspecto *clave* de la investigación no es otro sino la disrupción en el mercado laboral de las tecnologías digitales, del cómo el ejercicio del Derecho ha sido modificado de manera sigilosa pero certera. Para ello, la visión no ya tan futurista de Richard Susskind es toral. La vena principal de su argumento descansa en la división y disección del trabajo jurídico, la concepción, desde una nueva perspectiva, de las negociaciones y las controversias legales, en las cuales la totalidad del trabajo ha sido diseccionada y asignada al personal más capacitado para ello, a menudo abaratando los costos, y realizado por personas no necesariamente peritas en Derecho: la revisión de documentos, investigación legal, gestión de proyectos, asistencia procesal, comunicación electrónica, estrategia, táctica, negociación y la defensa, son vivos ejemplos de las actividades que los despachos jurídicos no necesariamente han de llevar a cabo por ellos mismos, sino echando mano de tecnologías disruptivas. Pero incluso la etapa hasta hace mucho imposible de atomizar se ha demostrado que no es así. Se está hablando del procedimiento, de tareas necesarias para el litigio liberalizadas para muchos otros competidores: investigación legal, gestión de transacciones, selección de plantillas, negociación, redacción personalizada, gestión de documentos, asesoría jurídica y evaluación de riesgos.

En síntesis, vale decirse que en el pasado, cuando se afrontaba un caso, el cliente tenía un simple elección: llevarlo a un bufete de abogados. Ese mundo ha cambiado. Ahora hay nuevas fuentes alternativas de servicios jurídicos.

A continuación se da cuenta de algunos de ellos:

- *Insourcing*. Esta forma de trabajo tiene lugar cuando los abogados desarrollan la totalidad del trabajo jurídico sin acudir a otros peritos en la materia para el asesoramiento externo.
- *Delawyring*. El *coyote* es el nombre con el que coloquialmente conocemos en México a la persona que, sin ser experto en Derecho, presta servicios legales; la innovación descansa en que ahora esos servicios son prestados por aplicaciones y no por personas.
- *Relocalización*. El modo de producción de moda, caracterizado por el traslado de parte del trabajo a lugares donde la mano de obra y la propiedad son menos gravosos, como los *call centers* o las funciones financieras de las empresas, a países, como India o Malasia.
- *Outsourcing*. Un fenómeno en el cual tareas jurídicas rutinarias para las empresas de servicios jurídicos les son asignadas a otras firmas, cuyo costo es mucho más accesible.
- *Cosourcing*. Una especie de sinergia de organizaciones prestadoras de servicios legales que, en una especie de combo, terminan por cumplir con sus obligaciones por medio del trabajo en conjunto.
- *Leasing*. Conforme a esta nueva forma de hacer negocios, ciertas aplicaciones digitales ponen a disposición de grandes despachos jurídicos, abogados únicamente contratados por periodos cortos a menudo relacionados con el incremento en la demanda de sus servicios o el desarrollo de proyectos específicos; así, las empresas no absorben el elevado costo de una nómina fija, pues la contratación de este modo resulta evidentemente menos onerosa.
- *Homesourcing*. La pandemia vino a revelar la posibilidad de trabajar en asuntos jurídicos desde casa: es decir, talento legal que sin estar disponible en el lugar de trabajo puede

desempeñarse a tiempo parcial y compaginar con ello labores de crianza.

- *Opensourcing*. La forma ideal de acceder a una fuente ilimitada de material legal (documentos estandarizados, opiniones, directrices, respuestas a consultas, procedimientos explicados) sin coste alguno.
- *Crowsourcing*. Como forma de contratación en masa se trata de la consulta digital respecto del enfoque del asunto por resolver, creándose una comunidad jurídica abierta al debate y la consulta.
- *Solosourcing*. A partir de la atomización tanto de los procedimientos de negociación como procesales, es posible contratar peritos en Derecho enfocados a la realización de una única parte de la gran tarea global.
- *Kmsourcing*. Partiendo del anglicismo *know how*, implica el empleo del conocimiento como fuente de retroalimentación que en la prestación de servicios jurídicos garantiza que los abogados echen mano de fórmulas probadas y exitosas.
- *Nosourcing*. Más que una estrategia de negocios aparece como estrategia procesal; al decidir no emprenderse acción legal alguna ponderando los posibles costes y los resultados así obtenidos.

La sentencia final respecto al trabajo legal es que, para cualquier asunto jurídico sustancial, se convertirá en una práctica común dividir el asunto en tareas fáciles de gestionar, identificando la forma más eficiente de realizar cada tarea, y adoptando de forma conjunta diferentes enfoques y medios alternativos de proveer los servicios, sin que ello implique una suerte de modelo de producción en masa para este tipo de servicios, pues las circunstancias de los clientes nunca son las mismas. Sin embargo, tampoco puede decirse que siempre se necesiten profesionales humanos en todas las etapas del ciclo de vida de un proyecto ju-

rídico, incluso si el resultado final es personalizado.¹⁹ De cara a estas nuevas circunstancias es acuciante la adquisición de nuevas habilidades que, para algunos, no les fueron enseñadas en las facultades de Derecho o en las universidades y que, para otros que aún se encuentran en la etapa de instrucción profesional, aún no se encuentran previstas por las respectivas mallas curriculares: el *marketing* como el arte de atraer nuevos clientes; tecnología para usar y considerar el empleo efectivo de herramientas; análisis para el incremento de la eficiencia y la rentabilidad; el análisis de datos con el propósito de evaluar estrategias exitosas y establecer precios adecuados por los servicios prestados; y el manejo de cadenas de suministro que les permitan relocalizar tareas a bajo costo.²⁰

***LawTech startups* y su peculiar desempeño en el terreno jurídico**

En los apartados anteriores se ha abordado cómo el *lawtech* se manifiesta en la práctica a través de las tareas que desempeña en el sector de los servicios legales. No obstante, lo hasta entonces apuntado es un acercamiento general que da cuenta de grandes rubros de trabajo que el empleo de determinadas tecnologías ha permitido digitalizar, mientras que lo que aquí se propone es una perspectiva mucho más puntual y explícita.

El primer campo lo constituyen los documentos legales con especial énfasis en los contratos en un mercado que se muda a los datos portátiles, la digitalización del sistema judicial y del gobierno electrónico. Empero, la innovación consiste en la prestación de servicios que les permita a los abogados la redacción personalizada de documentos legales (*drafting*), así como su revisión y manejo. Aunado a los avances en materia de inteligencia artificial, promete crear instrumentos digitales que automaticen la extrac-

¹⁹ Susskind, *op. cit.*, pp, 30-ss.

²⁰ *Illinois State Bar Association's, Report and Recommendations of the Illinois State Bar Association's Task Force on the Future of Legal Services*, 2016, p. 4.

ción de datos, el análisis de textos y cláusulas como requisitos para una exitosa negociación contractual.

Un segundo rubro lo abarca el litigio caracterizado por sistemas de impartición de justicia en línea o por la incursión de experiencias disruptivas como la asistencia para la autorrepresentación procesal, el manejo de demandas, la resolución de controversias y la presentación de la carga probatoria *online*. La necesaria presencia física en la Corte está siendo rápidamente erosionada por la posibilidad de realizar videoconferencias y audiencias digitales apoyado por sistemas de reconocimiento facial y sistemas de protección de datos y, en última instancia, el servicio al cliente en cuyo seno se encuentran servicios a particulares, empresas y organizaciones, los cuales en ocasiones facilitan mecanismos de flujo de trabajo sin la necesaria intervención de un abogado. En algunos supuestos detrás de esas aplicaciones pueden verse personas especializadas en el mundo del Derecho, pero recientemente la experiencia ha demostrado que ello no es una condición indispensable para su puesta en marcha exitosa.²¹

Una mirada más atenta permite distinguir a las *startups* en función del trabajo jurídico que amenizan, reemplazan y en otros casos innovan:

- *Redes de trabajo entre abogados*. Por medio del impulso de estrategias de *outsourcing* y la creación de conexiones entre la sociedad y el sector de trabajo legal.
- *Automatización de documentos*. Estas aplicaciones acogen el diseño de sistemas y redes de trabajo que asisten en la creación de documentos electrónicos, lo que incluye sistemas de datos que echan mano de textos o información preexistente para la elaboración de nuevos documentos electrónicos. Se

²¹ Thomson Reuters, *Legaltech Startup Report 2019. A Maturing Market*, 2019, en Legaltech: ¿Qué es y cómo contribuye con el mercado jurídico? | Thomson Reuters (thomsonreutersmexico.com).

trata de sistemas que generan borradores de documentos relativamente pulidos y personalizados que responden a preguntas formuladas por los usuarios o la elaboración de lo que en México conocemos coloquialmente como “machotes”.

- *Administración práctica.* Los sistemas digitales de gestión y manejo proveen a los abogados de convenientes métodos para un manejo efectivo de sus clientes, información relevante de sus asuntos, contactos, calendarios, citas y reuniones, información en general, documentos por mencionar algunos.
- *Búsqueda jurídica.* El servicio que las *startups* proporcionan en el área de búsqueda jurídica se enfoca al diseño de criterios de búsqueda avanzada provenientes de la inteligencia artificial, y el procesamiento del lenguaje sin que sea una herramienta homologada. Para ello existe un catálogo con características diferenciables.
- *Análisis predictivo y litigación basada en datos.* El análisis predictivo consiste en el estudio de la información proveniente de los casos por medio de técnicas estadísticas o matemáticas, detectándose los posibles errores. Esos resultados pueden, a su vez, emplearse para una mejor predicción de eventos futuros y una mejor toma de decisiones. Si los abogados emplean modelos de predicción en el litigio obtienen información indispensable desde el inicio de un procedimiento jurisdiccional, lo que desemboca en un mejor desempeño procesal. Quizá más apasionante sea el estudio predictivo sobre el comportamiento de los tribunales, es decir, el razonamiento jurídico que han desarrollado: agregándose conjuntos de datos muy pronto será posible conocer las preocupaciones de la población (por ende, los temas que serán legislados), vaticinar el grado de cumplimiento y los riesgos jurídicos latentes.
- *Descubrimientos electrónicos.* Es el campo de la tecnología digital avocada a tareas como la identificación, recolección

y producción de información a solicitud de una específica investigación jurídica. Aquí pueden incluirse *e-mails*, documentos, presentaciones, haces de datos, videos, redes sociales y portales electrónicos.

- *Solución electrónica de controversias.* Usando tecnología, especialmente internet, se trata de resolver conflictos fuera de la Corte siempre que se trate (en este caso) de medios alternativos de solución de controversias. Existen básicamente dos áreas: la primera, basada plenamente en la tecnología, se refiere a esos sistemas donde la innovación desempeña un rol activo en la conducción de la controversia al emplearse múltiples algoritmos que les permiten a las partes llegar a las mejores soluciones; la segunda gran área consiste en el empleo de la tecnología como asistente en la solución del conflicto, cuyo proceso se lleva de manera independiente a los avances digitales.
- *Seguridad de datos personales.* Esa parte de la tecnología se enfoca en la protección de la confidencialidad de los datos que son intercambiados entre los clientes y los profesionistas, tomando forma de algoritmos encriptados.
- *Conectividad ininterrumpida.* Por medio de estos sistemas y dispositivos, se evita la interrupción del contacto entre los clientes y los abogados: los ordenadores, tabletas y cualquier dispositivo inalámbrico con acceso a la internet facilitan la celebración de videoconferencias, consulta de mensajería, redes sociales y correo electrónico, por lo que existe un acceso inmediato a los clientes y colegas del gremio jurídico.
- *Mercado jurídico electrónico.* Estas tecnologías impulsan la creación de puntos de reunión virtuales en los cuales se comparan puntos de vista sobre los servicios obtenidos, niveles de satisfacción, comparación de precios y tarifas, subastas de servicios legales por mencionar algunos. Un cambio de paradigma, si se piensa en la imposibilidad de romper el cerco informativo acerca de otras opciones para los clientes.

- *E-learning*. Un campo poco estudiado cuando se habla del *legaltech* es la disrupción en el método de enseñanza y aprendizaje del Derecho que ha trascendido a las clases en línea o las videoconferencias: la práctica jurídica y entornos de aprendizaje jurídico virtual y el denominado “metaverso legal”.
- *Orientación jurídica online*. Por medio de internet es posible no sólo proporcionar (generar, compartir, buscar y encontrar) información jurídica sino también orientación jurídica e incluso asesoramiento personalizado a bajo costo.
- *Legal open-sourcing*. Con la liberación del conocimiento jurídico y la posibilidad de publicarlo masivamente, la idea consiste en crear cantidades ingentes de materiales jurídicos, cuyo acceso sea irrestricto al público y a la comunidad.
- *Conocimiento jurídico integrado*. Sin duda alguna, una de las áreas de mayor interés en el futuro venidero. Involucra el profundo arraigamiento del orden jurídico dentro de los sistemas y procesos, sin que ello requiera más el conocimiento previo y meticuloso de las personas acerca de aquello que les está permitido hacer, puesto que serán las máquinas, instrumentos y herramientas las que lo *sepan* (un magnífico ejemplo son los automóviles que ante la detección en sus conductores de niveles de alcohol fuera del rango permitido por ley quedarán inmovilizados hasta la disminución del grado de alcohol).
- *Externalización de procesos legales*. Valerse de las tecnologías digitales entraña la participación de empresas externas que no trabajan para los usuarios finales, sólo para abogados, despachos o departamentos jurídicos cuyo trabajo es la evaluación de las solicitudes, sin que se pierda de vista que la tecnología se aplica únicamente cuando clientes y sus abogados intercambian información usando plataformas electrónicas.

Algunas apps del sector *legaltech* en la realidad

No es aventurado afirmar que los impuestos (por ser ésta la figura más cercana al ciudadano común) encarnan la animadversión general al Derecho. Se trata de un tema complejo manejado por autoridades agresivas y un terreno donde impera el terrorismo fiscal pues están en juego los recursos económicos de los gobernados y la posible pérdida de la libertad. .

En ese fértil terreno surge *Taxdown* una aplicación que proporciona cinco diferentes tipos de servicios jurídicos para la gestión de contribuciones en México: 1) asesoría acerca de cómo hacer una declaración anual; 2) información en torno al impuesto sobre la renta; 3) mejora en la gestión de deducciones; 4) trámites ante el Servicio de Administración Tributaria, y 5) asesoría jurídica en materia de impuestos en México, domicilio fiscal, enajenación de bienes inmuebles sin el enterero de impuestos y otros. La operación de la plataforma electrónica parte de la necesidad de la mayoría de los ciudadanos de contar con asesoría jurídica fiscal a través de dos esquemas: uno gratuito y otro por suscripción. Por medio de un acceso general, los interesados pueden consultar si es posible contar con un saldo a favor ante el Servicio de Administración Tributaria, pero si lo que se busca es la presentación de una declaración anual, el costo de ese servicio asciende a únicamente quinientos pesos anuales —si se busca una asesoría más detallada el costo es de menos de mil pesos anuales—; y simulando esquemas de trabajo ideados por los propios abogados existe la posibilidad de trabajar por iguala: sin erogar por adelantado ni un centavo el cliente recibe el monto de la devolución y será hasta ese momento que *taxdown* cobre algún porcentaje sobre lo depositado a la cuenta del contribuyente.

Sin la necesidad de emprender una sinuosa búsqueda del especialista en Derecho fiscal, que puede o no derivar en el contacto del perfil adecuado no sólo a las necesidades del contribuyente sino a su bolsillo y evitando trasladarse a la oficina (ubicada, en ocasiones, en las antípodas), se puede presentar la declaración anual, o llevar a cabo el seguimiento al proceso de devolución y

de los requerimientos del Servicio de Administración Tributaria, con asesoría legal disponible los 365 días del año, resolución de dudas en menos de 24 horas por medio de un *chat*, planeación del próximo año fiscal e incluso asesoría fiscal con sólo usar una computadora personal.

Lawtech Software Group

Desde el mercado de *lawtech* más consolidado en el orbe, —la plaza tecnológica del Reino Unido—, *Lawtech Software Group* emerge como un revolucionario grupo encargado del diseño de programas dirigidos a la solución de problemáticas propias del Derecho: el empleo de la inteligencia artificial para el cumplimiento y la comprobación de datos biométricos, las tecnologías de verificación capaz de revisar más de 15 mil documentos provenientes de más de doscientas naciones, el manejo de casos eficiente por medio de un análisis de datos avanzado y eficiente o construyendo puentes de comunicación entre el cliente y el abogado.

Lawyer 365 es una de las marcas disponibles que permite resolver disputas desde lo familiar, penal, migración, corporativo, laboral, enajenación de bienes inmuebles, negligencia médica, responsabilidad civil, arrendamientos, redacción de documentos legales por medio de la selección de un abogado y la consecuente recepción de asesoría legal.

Jurimetría

Jurimetría es uno de los más claros ejemplos de la función clave que el profesional del Derecho tiene en el diseño de las herramientas del *legaltech*, al ser una plataforma que analiza cuestiones relevantes en los litigios: probable duración, resultado posible, trazado de la trayectoria del juez y su línea argumentativa y, por si ello no fuera suficiente, la posible línea argumentativa de la contraparte tomando como referencia la participación en algunos otros litigios. Lo que pudiera pensarse como una proyección

anecdótica deviene en la construcción de una estrategia a cargo de la parte consultora.

El funcionamiento de *Jurimetría* está habilidosamente ilustrado en su portal electrónico: el sistema se nutre de más de 10 millones de resoluciones judiciales, la estadística judicial y otras fuentes de datos, los cuales son analizados empleándose algoritmos de inteligencia artificial, enriquecimiento jurídico y, evidentemente, la mano humana encarnada por el control de calidad de los juristas españoles. El resultado es tan asombroso como amplio: *Jurimetría* del caso, del magistrado, del abogado, del organismo público, de la empresa y del tribunal, todo lo cual puede consultarse con un periodo de prueba gratuito temporal.

CONCLUSIONES

El anglicismo *legaltech* es el vocablo adecuado acorde con la opinión de los especialistas para designar el empleo de la tecnología digital en prácticamente cualquier recoveco del Derecho. Un fenómeno que no es reciente, con una amplia trayectoria trazable desde los primeros intentos de búsqueda automatizada de información jurídica y que, en nuestros días, culmina con la ambiciosa tarea de crear sistema de aprendizaje que permite emular una decisión judicial que los operadores del Derecho realizan, en ocasiones, a velocidad paquidérmica.

El tema aquí expuesto puede abordarse desde múltiples áreas: como oportunidad de negocios inaudita (aquí uno de los nichos que el emprendimiento jurídico está explotando), un reto para la enseñanza y el aprendizaje del Derecho (la posibilidad del ejercicio de prácticas profesionales en la realidad virtual o el metaverso); el diseño y nutrición de los algoritmos que habrán de moldear la decisión y la operatividad de las herramientas y servicios en los cuales el Derecho estará integrado.

La amplitud de los servicios potenciales que ofrece el *legaltech* abarca desde lo más sencillo, como la gestión rutinaria del trabajo

de un despacho o un litigante particular, la redacción personalizada de documentos legales, la desconcertante predicción del razonamiento de los que intervienen en un litigio, hasta la posible resolución de conflictos sin intervención humana (ciertamente es bastante interesante la posible replica de sesgos discriminatorios en algoritmos provenientes de los seres humanos que los diseñaron).

Sin duda alguna, ha quedado demostrado que el sector de la tecnología digital es mucho más que el simple uso de ordenadores, móviles, tabletas e internet por los operadores jurídicos.

REFERENCIAS BIBLIOGRÁFICAS

- Barrio Andrés, Moisés, *Legal Tech y la transformación del sector legal, La transformación digital de la abogacía*, España, 2003.
- Chochia, Archil *et al*, Legal Technology for Law Firms: Determining Roadmaps for Innovation, *Croatian International Relations Review*, May 2018.
- De Souza, Siddharta Peter, The Spread of Legal Tech Solutionism and the Need for Legal Design, *European Journal of Risk Regulation*, N° 13, 2002.
- Delgado Larena Avellaneda, José Eduardo, Legal Tech y Fin Tech, *La transformación digital de la abogacía*, España, 2003.
- Harper, Ciaran, y Zhang, Sarah, *Legal Tech and Lawtech: Towards a Framework for Technological Trends in the Legal Services Industry*, (PDF) Legal Tech and Lawtech: Towards a Framework for Technological Trends in the Legal Services Industry (researchgate.net).
- Illinois State Bar Association's, Report and Recommendations of the Illinois State Bar Association's Task Force on the Future of Legal Services*, 2016.
- Riem Hoffmann, Wolfgang, Legal Technology/Computational Law. Preconditions, Opportunities and Risks, *Journal Of Cross-Disciplinary Research in Computational Law*, November, 2020.
- Rincón Cárdenas, Erick, y Martínez Molano, Valeria, *Legaltech ABC de los servicios legales en la era digital*, Universidad del Rosario, Cámara de Comercio de Medellín para Antioquia, 2000, Rosario.
- Susskind, Richard, *El abogado del mañana. Una introducción a tu futuro*, 2017.
- The Law Society, *Introduction to Lawtech. A Practical Guide to Legal Technology*, 2019.

Thomson Reuters y *Legal Geek*, *Legaltech Startup Report 2019. A Maturing Market*, 2019.

Thomson Reuters, *Legaltech Startup Report 2019 A Maturing Market*, 2019, Legaltech: ¿Qué es y cómo contribuye con el mercado jurídico? | Thomson Reuters (thomsonreutersmexico.com).

Webb, Julian, Legal Technology: The Great Disruption?”, *Melbourne Legal Studies Research Paper Series*, N° 897.

Whalen, Ryan, Defining Legal Technology and its Implications, *International Journal of Law and Information Technology*, 2022.

Los datos personales en entornos digitales: herramientas para su protección

ROSA ALEJANDRA AZUARA MALAGÓN¹

INTRODUCCIÓN

En los tiempos que corren, marcados por la digitalización de gran cantidad de aspectos de la vida cotidiana y por el nítido aumento del uso de las tecnologías de la información y comunicación, los datos personales se han posicionado como elementos informativos de un importante valor, y, a su vez, se han convertido en el objetivo de gran cantidad de amenazas y riesgos derivados de su utilidad y potencial en el ámbito comercial y económico.

En ese sentido, en el trabajo que aquí se presenta pueden encontrarse diversas consideraciones relacionadas con los aspectos conceptuales de la privacidad, los entornos digitales y los datos personales con especial referencia a los fenómenos y dinámicas de circulación virtual de dicha información.

Por otra parte, en estas páginas se establecen diversas reflexiones relacionadas con los riesgos, problemáticas y desafíos que trae consigo la circulación masiva de los datos personales en entornos digitales, como internet, en tanto que, desde una perspectiva de

¹ Doctora en Derecho, especialista en transparencia y rendición de cuentas, catedrática durante más de siete años en las facultades de Derecho y Contaduría y Administración de la Universidad Nacional Autónoma de México (UNAM). Actualmente, es profesora de carrera tiempo completo en la Facultad de Derecho de la UNAM.

interdependencia e indivisibilidad de los derechos humanos a la protección de datos personales y a la privacidad, la vulneración de ellos deriva en consecuencias perniciosas para la garantía y protección de otros derechos.

Finalmente, en esta colaboración se da cuenta de las herramientas e instrumentos disponibles para la salvaguarda de los derechos a la protección de datos personales y a la privacidad desde una perspectiva individual, a la luz de los vacíos normativos prevaletentes en México y en las omisiones de promoción de estos derechos imputables a diversos actores.

Los datos personales y la privacidad con referencia a los entornos digitales

En la actualidad, los derechos a la privacidad y a la protección de datos personales se encuentran profundamente enlazados con las evoluciones tecnológicas referidas a entornos digitales, como internet. Lo anterior trasciende del ámbito informático al ámbito jurídico en tanto que influye en cuestiones de auténtica relevancia para el Derecho; pensemos por ejemplo en la certeza y seguridad que las personas titulares de dichos datos requieren respecto de la manera en que se gestiona dicha información.²

Ahora bien, para dilucidar estas complejas relaciones estimamos pertinente establecer diversas consideraciones de carácter conceptual en torno a nociones como privacidad, datos personales y entornos digitales. En ese sentido, señala Meraz, que podemos entender a la privacidad a partir de los siguientes tres sustratos:

En primera instancia está la cosmovisión o “visión del mundo” de cada individuo, pues “gran parte de los bienes jurídicos tutelados por los derechos de la personalidad son bienes que requieren una

² A. I. Meraz Espinoza, Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales, IUS. *Revista del Instituto de Ciencias Jurídicas de Puebla*, 12(41), 2017, p. 294.

interpretación subjetiva: el honor, la privacidad y la imagen en cuanto atributo". El segundo es el relativo a "los conflictos entre derechos de la personalidad, como por ejemplo el derecho a la información, especialmente el derecho de informar, y el derecho a la privacidad. Por último, el tercer sustrato, y considerado el más importante, es el relativo al cruce entre el derecho a la privacidad e internet. Aquí, se encuentran los conflictos éticos, bioéticos y el uso propiamente dicho de la red de redes.³

Derivado de dichas reflexiones, podríamos retomar la aproximación de Meraz consistente en que la privacidad puede ser entendida como "algo que cada ciudadano tiene derecho de decidir sobre su persona e intimidad y donde nadie más puede intervenir"⁴ y con base en ello resulta imperativo centrar el análisis de estas cuestiones sobre las relaciones entre las personas titulares de los datos personales y los actores de Derecho privado que almacenan y manejan dichos datos en los entornos digitales.

Por cuanto hace a una aproximación conceptual a la noción de datos personales con relación a los entornos digitales, podemos retomar lo expuesto por Jervis, quien refiere que a partir de tecnologías como el Internet de las Cosas (IoT, por su acrónimo en inglés), se ha comprometido la seguridad y la privacidad de las personas, en tanto que:

Se trata de un avance tecnológico que permite, por ejemplo, determinar cuál es el comportamiento de manejo por parte de un conductor y con ello elegir qué prima de seguro automotriz es eficiente cobrar conforme el nivel de riesgo que presenta en base a un historial de comportamientos; registrar los movimientos de los pacientes dentro de la urgencia de una clínica u hospital para mejorar sus flujos y restringir accesos conforme sus perfiles; contar con hogares inteligentes que permitan regular la temperatura y la

³ Ibídem, 299. Asimismo, véase V. Drummond, *Internet, privacidad y datos personales*. Reus, 2004.

⁴ Meraz Espinoza, *op. cit.*, p. 299.

luz según sus preferencias y horarios o evitar robos o accidentes domésticos con sistemas de monitoreo y alarmas apropiadas [...].⁵

La referencia a esta tecnología se estima pertinente en tanto que, a partir de la exploración de la gran cantidad de alcances que ésta tiene, resulta indispensable reformular la concepción de los datos personales, pues estamos ante algo que va mucho más allá de lo que la doctrina y el material normativo disponible han referido como información a partir de la cual se identifica o se hace identificable a una persona. De tal manera que, como ha señalado la Agencia Española de Protección de Datos, es importante configurar una definición lo suficientemente amplia para anticiparse a las posibles evoluciones de la tecnología que incluya los procedimientos y técnicas para el tratamiento de la información que permitan singularizar a una persona o usuario.⁶

Ahora bien, otra de las encrucijadas relevantes para comprender las complejidades de estos fenómenos es la relacionada con la intersección entre datos personales y entornos digitales, respecto de lo cual tomaremos como punto de partida la histórica confrontación entre beneficios y riesgos de dichas tecnologías. Al respecto, destacan los planteamientos de Peshard, quien refiere que desarrollos como las redes sociales significaron una revolución en la forma de comunicarnos, en tanto que ofrecieron oportunidades de muy diversa índole, como el conocimiento, el entretenimiento, la diversión y la socialización, pero, al mismo tiempo, esta constante y pública exposición de la información personal trajo consigo importantes

⁵ P. Jervis Ortiz, Internet de las cosas y protección de datos personales. *Revista Chilena de Derecho y Tecnología*. 4(2), 2015, p. 11. <https://doi.org/10.5354/0719-2584.2015.37509>.

⁶ *Legal Today*, Cambia el concepto de “dato personal”. *Legal Today*, 3 de marzo de 2011, en <https://www.legaltoday.com/actualidad-juridica/noticias-de-derecho/cambia-el-concepto-de-dato-personal-2011-03-03/>.

riesgos como la explotación indebida con fines comerciales o la violencia, del tal manera que:

[E]l papel del Estado es garantizar la convivencia y el balance adecuado entre ambos derechos, es decir, de la libertad de expresión y de la protección a los derechos de la privacidad, estableciendo con claridad que el Internet no es un espacio sin ley. En consecuencia, el propósito de las autoridades de protección de datos y otras instituciones deberá ser el de garantizar una navegación segura a través de un conjunto de normas y políticas públicas que fomenten el pleno conocimiento de las consecuencias que conlleva la participación en redes sociales.⁷

Así las cosas, puede advertirse la trascendencia jurídica de la circulación y el almacenamiento de los datos personales en internet en tanto que una inadecuada gestión de ellos puede llevar a consecuencias indeseables que afectan de múltiples maneras la esfera jurídica de las personas, trastocando su dignidad, libertad e intimidad, entre otros valores fundamentales y derechos.

Riesgos y desafíos en la circulación virtual de los datos personales

Uno de los puntos de arranque para explorar la gran cantidad de retos y desafíos en esta materia es lo que se ha señalado como dominio de las empresas gigantes del internet, tales como Google, Apple, Facebook y Amazon, que han sido señaladas de tal manera que:

[E]n primer lugar, se encuentran en una situación de posición dominante dentro de diferentes mercados digitales; en segundo lugar, porque estas multinacionales poseen varios mercados conexos en

⁷ J. Peschard Mariscal, Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos en C. Gregorio, y L. Ornelas (Comps.), *Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorándum de Montevideo*, Instituto de Investigación para la Justicia, Instituto Federal de Acceso a la Información y Protección de Datos, 2011, pp. 21-25.

internet, que subsisten gracias a la venta de publicidad, que constituye el mayor ingreso de estas empresas.⁸

Al respecto, la problemática persistente y central consiste en la comercialización o explotación económica de los datos personales de los que estos gigantes de internet se allegan, provocado en la mayoría de las ocasiones por la promoción con una gratuita campaña por la cual se atraen a las personas usuarias que ponen a su disposición información personal de muy diversa índole sin conocer adecuadamente el alcance de la autorización del uso que media en todo ello, lo que a su vez financia el acceso gratuito a los servicios que se ofrecen, derivado de la venta de dichos usuarios, y que, posteriormente, sirve, por ejemplo, para ofrecer publicidad dirigida o personalizada.⁹ Dicha dinámica, con especial referencia al caso de Google es sintetizada por Cubillos Vélez de la siguiente manera:

Por una parte, Google propone una serie de servicios gratuitos a los internautas, quienes confían sus datos personales a esta empresa, y por otra, Google monetiza la audiencia gracias a la venta de espacios publicitarios basados en los datos de los internautas y en la instalación de *cookies* para orientar los resultados. De esta manera, el modelo de gratuidad es doblemente aparente, porque Google genera ingresos con los datos personales de los internautas y con la publicidad.¹⁰

Otra de las problemáticas en este ámbito tiene que ver con el uso de las *cookies*, las cuales pueden ser entendidas como “informaciones instaladas en el disco duro del computador por el servidor del sitio que visita el titular de la información; ellas contienen

⁸ Ángela Cubillos Vélez, (2017). La explotación de los datos personales por los gigantes de internet, *Estudios en Derecho a la Información*, 1 (3), 2017, p. 28, en <https://doi.org/10.22201/ijj.25940082e.2017.3.10823>.

⁹ Ibídem, p. 29, en <https://doi.org/10.22201/ijj.25940082e.2017.3.10823>.

¹⁰ Ibídem, p. 37, en <https://doi.org/10.22201/ijj.25940082e.2017.3.10823>.

el nombre del servidor que la deposita, una identificación con un número único y eventualmente con una fecha de expiración”.¹¹

Lo anterior constituye un tratamiento de datos personales, en tanto que esta información permite identificar a la persona titular de datos personales muy diversos, sobre todo si se considera que la cantidad de *cookies* que se instalan durante un periodo de navegación en internet puede llegar a ser muy alta, y existen *cookies* que distan de cumplir con las exigencias de un consentimiento, libre expreso e informado; o existen algunas otras que recurren a métodos aún menos prolijos, como limitarse a informar al titular de los datos personales que se instalarán *cookies* mediante una ventana emergente, condicionando la navegación en el sitio en razón de la aceptación de su instalación.¹²

Finalmente, otro de los retos más agudos identificados en esta materia es el relacionado con la manera en la que dejamos en nuestros recorridos y pasos por la red datos biométricos diversos que sirven a los gigantes de internet de manera muy importante para la identificación de las personas titulares, a través de la voz o los rasgos del rostro en las fotografías que compartimos en redes sociales, por ejemplo. Lo anterior cobra relevancia por cuanto existen casos documentados en los que se evidencia la venta dichos datos a compañías aseguradoras o farmacéuticas.¹³

Ahora bien, este ciclo completo de circulación y apropiación de información personal es ilustrado de manera sintetizada por Cubillos Vélez, quien señalaba, respecto del caso de Facebook, a manera de ejemplo lo siguiente:

1) Este gigante de internet tiene acceso a datos sensibles que gozan de especial protección, y conoce la tendencia política, orientación sexual de sus usuarios y puede, incluso, realizar reconocimiento facial. Esta compañía debería indicar cuál será la finalidad del tratamiento para cada dato personal recopilado, respetando la

¹¹ Ibídem, p.38, en <https://doi.org/10.22201/ijj.25940082e.2017.3.10823>.

¹² Ibídem.

¹³ Ibídem.

obligación de información y la naturaleza del dato; 2 Esta red social debería informar a sus usuarios sobre la transferencia de datos que efectúa a Estados Unidos. No obstante, la información no se encuentra disponible en la política de datos de Facebook; 3) Facebook instala, igualmente, cookies espías, conocidas como *cookies* DATR en los computadores o aparatos móviles; estas *cookies* memorizan todas las visitas a páginas dotadas de un botón “me gusta” y recopilan la información de los internautas, incluso de aquellos que no son usuarios de la red. Todo lo anterior se realiza sin el consentimiento informado del usuario; 4) Esta compañía conserva, asimismo, por un largo periodo la dirección IP del usuario que realiza la conexión en su red, sin su autorización.¹⁴

La dificultad en el ejercicio y diseño de mecanismos adecuados de control para los gigantes de internet consiste en que estamos ante una interconexión de mercados diversos que facilita el tratamiento ilimitado de los datos, dado que en la medida en la que se ofrecen servicios de muy diversa índole, estas empresas se hacen de la mayor cantidad de clientes posibles.¹⁵

Los vacíos y retos normativos en la materia

Son diversas las posturas que sostienen la necesidad de replantear los contenidos normativos vigentes en nuestro país en los que se establecen los procedimientos a partir de los cuales se puede acceder a la información de personas usuarias, procesarla y resguardarla, así como las sanciones para aquellos particulares que incumplan con lo establecido, a saber: la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP), promulgada el 5 de julio de 2010.¹⁶

¹⁴ Ibidem, p. 40.

¹⁵ Ibidem.

¹⁶ C.A. Lara-Nino, M. Morales-Sandoval, y A. Díaz-Pérez, Los retos para proteger los datos del usuario en México, *Revista Internacional de Investigación e Innovación Tecnológica*, 10 (56), 2022, p. 25.

En ese sentido, y conforme a lo establecido en dicho ordenamiento, pueden advertirse diversas deficiencias para la adecuada protección de la información personal. En ese sentido, podemos retomar lo referido por Lara, Morales y Sandoval, de que aunque el principal requisito a satisfacer para que un particular pueda almacenar y hacer uso de los datos personales de las personas usuarias es la presentación de un documento denominado “aviso de privacidad”, dicho instrumento presenta, la mayoría de las ocasiones, una gran carga de falibilidad, pues:

¿cuántas personas realmente se toman el tiempo de leer estos documentos? En este tema, la Ley establece que quien recopila los datos debe permitir al usuario solicitar que estos no sean usados o almacenados, es decir, el espíritu de la Ley no es en realidad proteger al usuario, sino reglamentar el uso de los datos personales.¹⁷

Otra de las deficiencias de la normatividad actual señaladas por las voces citadas se encuentra vinculada con la definición de datos personales consistente en “cualquier información concerniente a una persona identificada o identificable”, lo que a juicio de dichas voces presenta importantes vacíos, ya que:

Primero, es posible argumentar que toda persona es identificable si se cuenta con suficientes datos disponibles. Además, como se evidencia en el mismo reporte, se podría discutir que los datos no conciernen a una persona física, sino a un ordenador que es propiedad de la persona. Este tipo de definiciones que carecen de precisión pueden dar pie a la defensa de actividades ilícitas.¹⁸

Otro de los vacíos identificados por estos autores está relacionado con el consentimiento de las personas titulares de los datos personales para su tratamiento, pues, aun cuando en el artículo 8 de la ley se establece que existe un consentimiento expreso cuando la voluntad del usuario se manifieste “verbalmente, por escrito, por medios electrónicos, ópticos o por cualquier otra tecnología, o por signos inequívocos”, puede ser problemático en virtud de

¹⁷ Ibidem, p. 25.

¹⁸ Ibidem, p. 26.

que existe una gran cantidad sitios electrónicos que muestran la leyenda “Al permanecer en esta página acepta nuestros términos y condiciones, lo que, a juicio de estos autores, implica que: “Realmente no hay un requerimiento estricto de que los terceros soliciten de forma expresa el consentimiento del usuario para recopilar y procesar sus datos”.¹⁹

Además, el mismo precepto normativo señala que “Se entenderá que el titular consiente tácitamente el tratamiento de sus datos, cuando habiéndose puesto a su disposición el aviso de privacidad, no manifieste su oposición”, lo que trae consigo que válidamente los terceros pueden recopilar y tratar la información del usuario a menos que dicha persona consulte el aviso de privacidad y siga el mecanismo establecido para manifestar su oposición.²⁰

Finalmente, Lara, Morales y Díaz identifican como riesgos derivados de vacíos normativos los relacionados con un componente de impunidad generalizada en nuestro país, pues en una gran cantidad de casos no se sanciona efectivamente a los responsables, así como se sufre el lacerante fenómeno de robos de identidad, además de que, desde una perspectiva interdisciplinaria, se puede advertir la falta de tipificación como delito de dicha conducta en el ámbito penal federal.²¹

A manera de conclusión: herramientas tecnológicas de salvaguarda y protección de la privacidad en entornos digitales

Asentadas estas reflexiones de carácter conceptual, teórico y normativo, consideramos relevante establecer la importancia de diversas herramientas que pueden implementarse para la adecuada salvaguarda y protección de los datos personales en el contexto de los vertiginosos cambios y avances de entornos digitales como internet.

¹⁹ Ibidem.

²⁰ Ibidem, p. 26.

²¹ Ibidem, p. 27.

Al respecto, destacan herramientas como 1) la encriptación de la información; 2) la detección de brechas de seguridad; 3) la utilización de firmas electrónicas, y 4) la gestión de contraseñas que satisfagan los parámetros de seguridad. Dichos instrumentos cuentan con diversas ventajas, entre las que destaca, naturalmente, la posibilidad de ser implementadas de manera independiente por las personas usuarias de los entornos digitales, lo que subsana las deficiencias presentadas por una legislación que ha quedado rebasada por los avances tecnológicos.

En relación a la primera de las herramientas señaladas, la encriptación de la información en los entornos digitales puede ser entendida como “[L]a utilización de un algoritmo matemático que ‘envuelve’ un mensaje de manera que sólo el receptor legítimo pueda abrirlo y hacerse de su contenido, mediante la utilización de una llave o clave única que ‘desenvuelve’ el mensaje”.²² De ahí que aplicaciones, como WhatsApp, que cumplen con una función trascendental en las tecnologías de nuestros días, como lo es la comunicación instantánea, se valgan de dicha herramienta con la finalidad de inspirar confianza y seguridad en sus usuarios.

Respecto de la segunda de las herramientas referidas, la Agencia Española de Protección de Datos (AEPD), ha referido:

[E]l responsable de tratamiento debe estar preparado para esta posibilidad, debe establecer quién y qué acciones se ejecutarán en caso de producirse. Para ello, lo primero es ser consciente de qué datos personales se están tratando, con qué medios y los riesgos que puede haber.²³

²² D. Álvarez Valenzuela, Algunos aspectos jurídicos del cifrado de comunicaciones, *Derecho PUCP*, (83), 2019, p. 243, en <https://doi.org/10.18800/derechopucp.201902.008>.

²³ Agencia Española de Protección de Datos, *Brechas de seguridad de datos personales: qué son y cómo actuar*, Agencia Española de Protección de Datos. 18 de septiembre de 2019, en <https://www.aepd.es/prensa-y-comunicacion/blog/brechas-de-seguridad-de-datos-perso->

Por ello, señala la propia AEPD, resulta por demás importante implementar mecanismos que permitan detectar las brechas de seguridad de datos personales.

La tercera de las herramientas cuenta con importantes virtudes con relación a la protección de los datos personales en entornos digitales, en tanto que una firma electrónica puede hacer frente de manera ágil y garantista a una de las problemáticas más relevantes en esta materia, como el punto clave del consentimiento en el tratamiento y la utilización de los datos personales, en tanto que, a través de esta herramienta, se deja registro y se “sella” la actividad de los usuarios conforme a la regulación aplicable.²⁴

Por último, es importante señalar que una de las herramientas de alcance más inmediato y eficiente —pero de la cual desafortunadamente no siempre se tiene conciencia plena de su importancia— es el uso de contraseñas seguras, pues a partir de ellas pueden resistirse ataques informáticos. Al respecto, la Comisión Económica para América Latina y el Caribe (CEPAL) ha referido como algunas de las claves para crear contraseñas seguras las siguientes:

- Crear contraseñas largas.
- Utilizar mayúsculas, minúsculas, signos de puntuación y caracteres no alfabéticos.
- Utilizar contraseñas únicas para cada servicio.
- Utilizar el enfoque XKCD, que consiste en utilizar cuatro palabras escogidas al azar; y,

nales-que-son-y-como-actuar#:~:text=Una%20brecha%20de%20seguridad%20es,digitalmente%20o%20en%20forma%20papel.

²⁴ Tecalis, RGPD: *Firma electrónica para cumplir con el Reglamento General de Protección de Datos*. Tecalis. 6 de marzo de 2023, en <https://www.tecalis.com/es/blog/rgpd-reglamento-general-proteccion-datos-firma-electronica-digital-lopd-ley-empresas-gdpr>.

- Utilizar un gestor de contraseñas, *software* que genera y maneja contraseñas únicas y encriptadas, ofreciendo mayores garantías de seguridad y evitando el problema de crear y recordar múltiples contraseñas.²⁵

Por otra parte, podemos retomar lo expuesto por Lara, Morales y Díaz, quienes recomiendan a las personas usuarias, frente a los escenarios de riesgo marcados por procesos delictivos cada vez más complejos, lo siguientes:

- Evitar proporcionar datos personales a través de sitios de internet o medios electrónicos a menos que sean absolutamente necesarios.
- Evitar exponer documentos con información sensible a través de basura, correspondencia no atendida, servicios de papelería, entre otros.
- Evitar hacer uso de plataformas digitales que carecen de autenticidad, así como aplicaciones móviles que solicitan acceso a servicios que realmente no necesitan.
- Conocer los derechos con los que goza el usuario ante las políticas de recolección y tratamiento de los datos por terceros, así como los medios de revocación de autorización.²⁶

Sin duda, la legislación en la materia presenta necesidades urgentes de actualización derivado de los avances tecnológicos cada vez más complejos y la consecuente vulnerabilidad de las personas usuarias en entornos digitales ante complejos procesos delictivos con consecuencias cada vez más agudas. Sin embargo, como han referido Lara, Morales y Díaz, es importante reconocer la necesidad de concientizar a la ciudadanía en torno a la importancia de resguardar su información personal y las potenciales consecuencias

²⁵ Comisión Económica para América Latina y el Caribe, *Gestión de datos de investigación. Uso de contraseñas seguras*, Biblioteca de la CEPAL, en <https://biblioguias.cepal.org/c.php?g=495473&p=4398100>.

²⁶ Lara-Nino, *et al*, *op. cit.*, p. 28.

que traen consigo un uso inadecuado de dichos datos, pues aunque pudiera ser sugerente la impresión de que la tecnología ha rebasado a la humanidad en cada vez más ámbitos al encontrarnos rodeados de medios digitales, es cierto que con la correcta capacitación y concientización de dichos riesgos, podemos vigilar y hacer frente a las distintas amenazas que pudieran presentarse.²⁷

REFERENCIAS BIBLIOGRÁFICAS

- Agencia Española de Protección de Datos, *Brechas de seguridad de datos personales: qué son y cómo actuar*, Agencia Española de Protección de Datos, 18 de septiembre de 2019, en <https://www.aepd.es/prensa-y-comunicacion/blog/brechas-de-seguridad-de-datos-personales-que-son-y-como-actuar#:~:text=Una%20brecha%20de%20seguridad%20es,digitalmente%20o%20en%20forma%20papel>.
- Álvarez Valenzuela, D., Algunos aspectos jurídicos del cifrado de comunicaciones. *Derecho PUCP*, (83), 2019, pp. 241-262, en <https://doi.org/10.18800/derechopucp.201902.008>.
- Comisión Económica para América Latina y el Caribe, Gestión de datos de investigación. Uso de contraseñas seguras, Biblioteca de la CEPAL, en <https://biblioguias.cepal.org/c.php?g=495473&p=4398100>.
- Cubillos Vélez, Ángela, La explotación de los datos personales por los gigantes de internet, *Estudios En Derecho a La Información*, 1(3), 2017, pp. 27-55, en <https://doi.org/10.22201/ijj.25940082e.2017.3.10823>.
- Drummond, V., *Internet, privacidad y datos personales*. Reus, 2004.
- Legal Today, Cambia el concepto de “dato personal”. Legal Today, 3 de marzo de 2011, en <https://www.legaltoday.com/actualidad-juridica/noticias-de-derecho/cambia-el-concepto-de-dato-personal-2011-03-03/>.
- Meraz Espinoza, A. I., Empresa y privacidad: el cuidado de la información y los datos personales en medios digitales, *ius. Revista del Instituto de Ciencias Jurídicas de Puebla*, 12 (41), 2017, pp. 293-310.
- Jervis Ortiz, P., Internet de las cosas y protección de datos personales, *Revista Chilena de Derecho y Tecnología*, 4 (2), 2015, pp. 9-51, en <https://doi.org/10.5354/0719-2584.2015.37509>.

²⁷ Ibidem, p. 29.

- Lara-Nino, C. A., Morales-Sandoval, M., Díaz-Pérez, A., Los retos para proteger los datos del usuario en México, *Revista Internacional de Investigación e Innovación Tecnológica*, 10 (56), 2022, pp. 14-33.
- Peschard Mariscal, J., Protección de las niñas, niños y adolescentes en el ámbito digital: responsabilidad democrática de las instituciones de gobierno y de las agencias de protección de datos, en Gregorio, C. y Ornelas L. (comps.), *Protección de datos personales en las redes sociales digitales: en particular de niños y adolescentes. Memorándum de Montevideo*, Instituto de Investigación para la Justicia, Instituto Federal de Acceso a la Información y Protección de Datos, 2011, pp. 21-25.
- Tecalis, RGPD: *Firma electrónica para cumplir con el Reglamento General de Protección de Datos*, Tecalis, 6 de marzo de 2023, en <https://www.tecalis.com/es/blog/rgpd-reglamento-general-proteccion-datos-firma-electronica-digital-lopd-ley-empresas-gdpr>.

El derecho digital: un rubro necesario en el ciberespacio, el quinto dominio en operaciones militares

EMILIO VIZARRETEA ROSALES¹

A MANERA DE INTRODUCCIÓN

Como una necesaria reflexión para impulsar y fortalecer una legislación en materia digital, valgan los siguientes alegatos que configuran los conceptos del ciberespacio, de la ciberseguridad, los ciberataques y la necesaria resiliencia estratégica en infraestructuras críticas. A lo largo del texto se mencionan autores y factores que todo derecho digital debe considerar, y a partir del ciberataque a la Secretaría de la Defensa Nacional (SEDENA) se especifican los elementos que en la vida social, económica, política y militar, nacional e internacional, tanto en la forma y los contenidos, deben ser contemplados en la normatividad mexicana.

El análisis y la deliberación de la información se tejen en los actuales horizontes del desarrollo y las seguridades nacional, pública e interior, con su vinculación global y con una multidimensionalidad

¹ Emilio Vizarratea Rosales es profesor-investigador en la UNAM, el CESNAV-ININVESTAM de la SEMAR; del CEEFA, CODENAL y la Escuela Superior de Guerra de la SEDENA. Analiza tópicos de Política Nacional e Internacional; Filosofía y Teorías Políticas; Inteligencia, Desarrollo, Seguridad y Defensa Nacionales, así como de Ciberpolítica, Democracia, Gobernabilidad y Política Electoral. Entre sus obras destacan: *Repensar México, una introducción a la seguridad y defensa nacionales* (2020); *Sobre el Discurso Estratégico* (2016); *El saber político: Platón y Aristóteles* (2014) y diversos ensayos.

que se caracteriza por la situación determinada por la resonancia de la epidemia de covid-19, la guerra de Rusia contra Ucrania, los problemas ligados a la energía, la alimentación, el medio ambiente y el cambio climático, los ataques a la infraestructura crítica de la SEDENA y a otras dependencias y empresas mexicana y del mundo, los problemas vinculados a la democracia, las batallas al interior de los poderes y los gobiernos, así como sus pesos y contrapesos y, la tensión entre México y Estados Unidos por las dificultades en materia de seguridad, migración, energías limpias y el T-MEC, desde luego porque ambos países celebraron elecciones presidenciales en 2024.

México ha resuelto su proceso electoral estableciendo una continuidad de sus políticas, por lo que el registro de estos asuntos de interés nacional, como lo es el derecho digital y sus alcances y límites en el ciberespacio, estarán pendientes en la agenda pública gubernamental.

Contexto conceptual ciberespacial

El *ciberespacio* es observado por las fuerzas armadas como el quinto ámbito de operaciones, después de la tierra, el mar, el aire y el espectro radioeléctrico; el ciberespacio es un entorno conceptual en el que se produce la comunicación a través de redes informáticas.²

Partiendo de los aspectos de un campo de información y conocimiento relativamente nuevo y con una gran dinámica en su desarrollo, como el ciberespacio, registramos algunos elementos de la jerga lingüística que se emplea cotidianamente y que nos permite homogeneizar el uso de las palabras, y que nos permite hacer cosas. Así, el prefijo *ciber*, y todo lo relacionado con su dominio, no tiene un consenso unificado. Sin embargo, se refiere a

² Vid la Cumbre de la OTAN en Varsovia, 2016, así como la referencia del *Diccionario Oxford*.

lo cibernético, informático, virtual o digital. En estos usos, la *ciberseguridad* es concebida como un conjunto organizado de medidas para prevenir, evitar y minimizar potenciales daños a personas, equipos, redes y sistemas de información o infraestructuras críticas, públicas o privadas.³

Asimismo, se articulan los conceptos de *ciberamenazas*, como una fuente potencial de perjuicio, externa o interna, a algún activo de la organización que se materializa a través del ciberespacio. Un *ciberataque* es concebido como uso deliberado de una *ciberarma*, por una persona o de manera automática, para causar un daño o perjuicio a un elemento del ciberespacio de un adversario, pudiendo tener efectos indirectos en los ámbitos de operaciones convencionales; el *ciberriesgo* es la probabilidad de que una *ciberamenaza* aproveche una vulnerabilidad para causar un daño a un activo que tiene un valor y una criticidad relevante.

Internet y los *sistemas aislados*, como redes, sistemas y dispositivos de almacenamiento de información no conectados a internet representan dos partes fundamentales que componen el ciberespacio. La conectividad global y cierto aislamiento en términos de confidencialidad se vinculan al ámbito de la ciberseguridad y la ciberdefensa.

Internet es una red de redes, un dispositivo que configura y materializa al ciberespacio: Es abierta e independiente en su forma de operar en el mundo, dirigida por organizaciones sin ánimo de lucro. Frente a la internet convencional, en la internet oculta (*deep web*), profunda o invisible, existen una colección de sitios *web* y bases de datos que un buscador común, como Google, Yahoo o Bing, no pueden indexar. Es, por ello, un terreno idóneo para realizar transacciones y actividades sin dejar rastro, lo cual puede tener un uso malicioso o delictivo vinculado a organizaciones criminales. Esta internet oculta usa navegadores, como TOR (*The*

³ Fundamental para orientarse en la familia de palabras *ciber*, resulta la *Guía de Ciberdefensa* publicada por la Junta Interamericana de Defensa, en Canadá en 2020.

Onion Router), difíciles de rastrear o identificar en su origen. Por ello, la *deep web* se analiza en los ámbitos de la ciberdefensa y la ciberseguridad.

El *ciberspacio* posee singularidades determinantes como *artificialidad, imperceptibilidad, dinamismo, ubicuidad, inmediatez y transversalidad*. Así, el *ciberspacio* ha sido creado por el hombre; es invisible e intangible; cambia constantemente; actúa en lo inmediato; tiene fronteras, y posee relacionalidad presencial e influencia, con los otros cuatro dominios; por ello requiere de capacidades específicas para su atención.

Estos elementos significativos del lenguaje ciber, las palabras, sus significados, la forma de su relacionalidad, constituyen los discursos de los diversos actores que nos orientan al describir las acciones que despliegan y que permiten construir, en la teoría y la práctica, las reflexiones y maneras de ser de los comportamientos legales e ilegales —mientras no tengamos un derecho digital que los articule jurídicamente en un proceso completo—, en la generalidad analógica del Derecho positivo de México y del mundo. Es un aspecto central en los elementos de la ciberseguridad que convergen en los temas de la seguridad y el desarrollo y que, desde el punto de vista teórico, epistemológico y metodológico, puede aprovechar el esfuerzo realizado por la denominada Escuela de Copenhague y algunas instituciones, como el CESNAV de la SEMAR.⁴

La mecánica de la dinámica entre ciberspacio y ciberseguridad

El entorno del *ciberspacio* resuena en lo que ocurre a nivel presencial, y, desde luego, tiene un sentido ampliado debido al uso de dispositivos tecnológicos renovados con una gran dinámica de evolución, cambio y desarrollo. Si bien la información

⁴ Barry Buzan, Jaap de Wilde y Ole Waever, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, UK, 1997, 190p; CESNAV-CODENAL, *Glosario de Términos en materia de seguridad en el ciberspacio*, 2021, 210p.

genera un cierto tipo de poder, en realidad puede conducir a cierto tipo de conocimiento que, conforme a un uso adecuado y en determinadas circunstancias, puede lograr poder. El análisis de la información ha devenido un proceso estratégico, crítico y complejo —puesto que quien analiza información, la política o el poder atiende las circunstancias que le rodean—, atisba en las fuentes de información que constituyen la estimación en un enunciado, afirmación o hipótesis, de un discurso que emite un actor relevante, hace sus reflexiones, análisis e interpretaciones, y propone ciertos cursos de acción posible para el logro de fines determinados. El análisis de la información y su seguridad son la aurora de la ciberseguridad actual.

El análisis de información matiza, ubica y reconstruye acontecimientos, datos, hechos, fenómenos; los ubica espacial y temporalmente, establece secuencias lógicas encadenadas, racionaliza la información con relación a sus fines y medios, busca apoyar la toma de decisiones, de manera objetiva, realista y factible. Eso lo hace cotidianamente y siempre a contrapelo de la necesidad. Es un trabajo de noria, de búsqueda de minero, constante, sistemático, sin fatiga, sin prefectos vigilantes que valgan, hasta que logra encontrar la pepita de oro, el hilo de Ariadna, que lo lleva a la gran veta dorada de la información, que le muestra la salida del laberinto de la ignorancia o del exceso de información, que le da comprensión y la explicación del fenómeno en estudio. Por ello es un activo que debe protegerse adecuadamente.

Los creadores y usuarios de información relevante requieren conocimiento, compromiso y responsabilidad profesional, convicción, sensibilidad, intuición, medida y sentido sobre los alcances y límites de lo que hace. Es un proceso de formación y de experiencia que lleva largo tiempo, en ocasiones muchos años. Saben que el trabajo de información es una herramienta indispensable. Quiere saber siempre más y mejor, porque la demanda es siempre para ayer. A pesar de la organización del trabajo o, mejor, precisamente por el tipo de organización, no siempre previsora ni con

prospectiva formal, siempre la demanda de información es alta, urgente, y mucho más; es un leviatán informativo, devorador e insaciable.

El análisis de información, político o de inteligencia, es una herramienta fundamental en la vida gubernamental y empresarial cotidiana. Distingue lo que diversos actores proponen y desean. Es un catalizador del instinto político de quienes han hecho de la información y la inteligencia una profesión, un campo de conocimientos estratégicos adscrito a la seguridad nacional, un acto de fe voluntaria.⁵

La construcción de infraestructuras críticas se apoya recíprocamente en los sistemas de información y de inteligencia, gubernamentales o privados, están atentos a la dinámica global, de competencia a ultranza, de lucha por sobrevivir en un mercado de capitalismo salvaje, con uso de recursos extremos, con una innovación tecnológica minuto a minuto, que obliga a una apertura mental del cambio y la innovación que, muchas veces, choca con el sueño de los justos, del pensar que ya se llegó. El tirarse a la hamaca de la conformidad es otorgar al adversario la oportunidad del éxito, frente a nuestra derrota en los diversos campos, político, económico, social, militar, exterior y de desarrollo tecnológico.

Un derecho digital debe atender, en primer lugar —y sólo con motivo de análisis— tanto el contexto doméstico, con actores y factores, aliados y adversarios, congruentes e intransigentes, que constituyen la dinámica cotidiana de la política y la economía nacionales, con el binomio de desarrollo y de seguridad que se complementan y guían, con los intereses particulares, amenazantes o delincuentes violentos y organizados y de cuello blanco, que muchas veces predominan frente a los intereses nacionales.

⁵ Vid Emilio Vizarratea, La importancia de la información y la inteligencia en los modelos geopolíticos contemporáneos, *Inteligencia estratégica; retos y oportunidades para México*, CESNAV, 2014, pp. 215-239.

Y, enseguida, en paralelo, desde luego, tenemos el contexto externo, globalizador y competitivo, intensamente demandante de canonjías y prebendas, interesado en colocar sus intereses globales externos por encima de los intereses nacionales, seductor de virtudes gubernamentales y de empresarios incompetentes, promotor de vicios que deterioran el propio desarrollo nacional en la inercia del poder nacional.

La prevención y la prospectiva son elementos que acompañan a la información y la inteligencia estratégicas. Los diagnósticos, estrategias, políticas, planes y programas, gozan de las estimaciones que surgen de dichos sistemas de información e inteligencia y, cuando no los tienen, no sólo sufren los actores, sino los autores y participantes, observadores o no del proceso en ciernes. Una planeación y una gestión estratégicas de las infraestructuras críticas construyen la ciberseguridad.

Hoy día, ante la actual difusión pública de acciones de investigación y espionaje, de ciberataques constantes, nos han mostrado no sólo situaciones-límite en el mundo virtual, sino también las situaciones de realidad y demanda en un mundo en competencia que requiere de mayor y mejor información, de organizarla en un eficaz sistema de inteligencia, de adjetivarla como estratégica, para acuñar la relevancia que poseen en los tiempos que vivimos, de impulsar políticas de ciberseguridad y defensa que trasciendan los ámbitos exclusivamente militares, manteniendo el respeto al Estado de Derecho y, en particular, a los derechos humanos de todos.

En suma, sin un derecho digital, sin recurso humano, sin inteligencia humana, la inteligencia estratégica está penca, tunca, chimuela, tuerta, coja, débil e incompleta y, las más de las veces, disfuncional de los fines, objetivos y metas de seguridad nacional. Y cuando no existen recursos para la ciberseguridad disminuye la visión que afirma que sin seguridad no hay desarrollo..

Sin inteligencia tecnológica, la inteligencia estratégica está disminuida, no amplía su radio de acción, el alcance de los sentidos pierde su fortaleza, se pierde la complejidad evolutiva e innovado-

ra del todo, desaparecen oportunidades, se vuelve menos competitiva. Los recursos económicos, públicos o privados, para invertir en tareas de inteligencia y seguridad no debieran escatimarse. Es la incomprensión del sentido de lo estratégico. Es la presencia ineludible de la ciberseguridad.

Papel de la información, la inteligencia de la ciberseguridad.

La evolución de la información y de las áreas de inteligencia, desde el paradigma que emerge durante la Segunda Guerra Mundial hasta el fin de la Guerra Fría, su cuidado y resguardo han desarrollado una tipología sobre el tratamiento de la información, de la seguridad de la información a la ciberseguridad, del *plus* agregado en la inteligencia y la contrainteligencia, desde la versión humana hasta la tecnológica, pasando por una inteligencia virtual para conquistar el ciberespacio. Los dispositivos han cambiado, pero las formas y los contenidos permanecen. Son los factores que deben considerarse desde un derecho digital.

La actual difusión pública de acciones de investigación y espionaje, en México y el mundo, nos ha mostrado no solo situaciones-límite en el mundo virtual, sino las situaciones de realidad y demanda en un mundo en competencia, que requiere de mayor y mejor información, de organizarla en un eficaz sistema de inteligencia, de adjetivarla como estratégica, para acunar la relevancia que poseen. De estar bajo el cuidado de la ciberseguridad.

Estos actos, de espionaje y robo de información han expuesto la debilidad del imperio en las tareas de información e inteligencia, los descuidos en la seguridad de la información y la contrainteligencia de nuestros vecinos del norte, y en el mundo en general, así como de las debilidades en la ciberseguridad.

La atención a los problemas del desarrollo tecnológico tiene que ver con las ventajas y afectaciones para la estabilidad y el desarrollo social y económico. Los problemas globales están asociados al terrorismo internacional, al crimen cibernético, al crecimiento

de mercados globales, al incremento de organizaciones criminales nacionales y transnacionales, al desarrollo de armas químicas, biológicas y de destrucción masiva, a la degradación del medio ambiente, al descontrol del cambio climático, al narcotráfico, la piratería, la biopiratería, el espionaje económico e industrial y a la tecnología de uso delincuencia. Todo ello implica mayor presupuesto, más y mejor personal, mayor preparación preventiva y prospectiva, mejor evaluación y eficaz capacidad de respuesta. La seguridad y la ciberseguridad representan el blindaje de las tareas tecnológica para mantener el desarrollo y seguridad nacionales. Bajo este contexto, resulta fundamental caracterizar, para su posible tipificación en los derechos digitales, algunos aspectos relevantes del ataque a la infraestructura crítica de la Secretaría de la Defensa Nacional.

Ciberespacio

Los ejércitos del mundo han encontrado la fórmula adecuada para aprovechar los avances que han desarrollado las distintas guerras. O cuando ha habido desastres naturales o eventos terroristas o *hackeo* a instituciones financieras y estratégicas, así las fuerzas armadas han aprendido de errores, fallas o derrotas y logran mantenerse ahora en la batalla de lo virtual.

Las Fuerzas Armadas Mexicanas definen al ciberespacio como el “entorno o ámbito intangible de naturaleza global, soportado por las Tecnologías de la Información y Comunicaciones, en el que se comunican e interactúan las entidades públicas, privadas y la sociedad en general, coadyuvando al desarrollo nacional y garantizando el ejercicio de los derechos y libertades como en el mundo físico”. El ciberespacio, un pluriverso de vida en el mundo cotidiano, es el quinto entorno operacional para proporcionar seguridad y defensa.

Este quinto dominio que opera en lo táctico, operacional y estratégico, es de vital importancia, debido a que comprende las infraestructuras críticas de los Estados-nación y, si se comprometen,

afectan las tareas y asuntos públicos, así como de las empresas privadas, los organismos e instituciones nacionales e internacionales. Habitan la competencia tecnológica internacional por conquistar su dominio. Su impacto en el desarrollo, así como el desafío que representa para brindar la seguridad requerida. La importancia de la seguridad informática consta de políticas estrategias, herramientas tecnológicas para garantizar a los usuarios un ambiente digital seguro, para brindar esa ciberseguridad a los Estados.

El *ciberespacio* se ha vuelto indispensable en la vida cotidiana, debido a la digitalización de las actividades y a los procesos mediante los cuales las tecnologías de la información transforman los ámbitos de la producción, así como el procesamiento e intercambio de información. Esa interacción ha facilitado los procesos, actividades que se hacían de manera personal y mecánica, pero también se han presentado diversos problemas cibernéticos. Estos problemas en la seguridad de la información se tienen que abordar desde la ciberseguridad, dadas las dificultades que caracterizan al ciberespacio, de identidad, flexibilidad y anonimato.⁶

Ciberseguridad

La ciberseguridad es concebida como la colección de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, enfoques de gestión de riesgos, acciones, capacitación, mejores prácticas, garantía y tecnología que se pueden utilizar para proteger el entorno cibernético y los activos de la organización y del usuario (Unión Internacional de Telecomunicaciones, ITU).

Pretende prevenir el daño causado por interrupciones, fallas o mal uso de las TICs y para reparar el daño si ha ocurrido. Una

⁶ El tratamiento del ciberespacio en la vida cotidiana, sus relaciones de poder y los conceptos de la discusión actual nos los brindan los textos de Byung-Chul Han, *Infocracia*, Taurus, México, 2022, 103p.

puesta en marcha de la resiliencia necesaria. La ciberseguridad se contempla en el ámbito de la seguridad nacional, por lo cual los gobiernos ponen en marcha estrategias que deben considerar los distintos sectores de las esferas social, pública y privada.

La forma en que se materializan las ciberamenazas son: el ciberespionaje, el robo masivo de información y de datos personales; los ciberataques dirigidos, cada vez más complejos por medio de la inteligencia artificial, el ciberterrorismo, el sabotaje físico; nuevas formas de delinquir por los grupos criminales organizados, sean de carácter nacional o transnacional, así como mediante campañas de manipulación, desprestigio y desestabilización a través de las redes sociales, por actores no estatales y grupos antagónicos.

El ciberespacio es un nuevo universo, intangible, atemporal, con simultaneidad; ha demandado un conocimiento que tiende a especializarse, pues posee una versión técnica que denota una jerga lingüística, que se desarrolla mediante la codificación, la decodificación, el cifrado y el descifrado de grandes cantidades de información (*Big Data*) a una velocidad extraordinaria, por medio de infraestructuras tecnológicas compuestas por equipos de cómputo y redes informáticas, e integradas mediante diseños y arquitecturas específicas. Evoluciona constantemente, con un alto crecimiento y en una renovación que vuelve obsoletos equipos y procesos en poco tiempo, articulando una comunidad de producción y consumo tecnológica y de conocimiento, que facilita la difusión de sus avances por muy pequeños que sean. El ejemplo de los celulares de Apple, que cada seis meses lanzan al mercado sus novedades, es mostrar el avance de los computadores en las TICs.

El ciberespacio es la piedra angular para el funcionamiento y desarrollo de los Estados, gobiernos y sociedades, así como para infraestructuras de comunicaciones, el comercio, el comando y control militar, los servicios de emergencia, el tránsito masivo, la distribución de plantas de energía y, entre éstas, las infraestructuras críticas de información, como sistemas que

brindan apoyo o servicios, o procesan productos esenciales para una nación para habilitar y sostener la sociedad del siglo XXI.

El avance de las infraestructuras críticas —que integran activos físicos que en la computadora era el *hardware*, junto con los activos cibernéticos, el *software*— induce una reflexión sobre la importancia del lugar de los actores que atienden dichas infraestructuras críticas y establecen un rango de debilidad, riesgo, o amenaza la actividad, o el servicio que realiza esta entidad gubernamental o empresarial, para adaptarse a un nivel cada vez más tecnificado, previendo la futura evolución o la migración de procesos a instancias mucho más avanzadas en la tecnología y el conocimiento de los procesos, que influyen en los productos y servicios bajo su responsabilidad. La ciberseguridad cuenta con un lugar, usuarios y consumidores, procesos y productos, que son valorados cotidianamente.⁷

De manera que, así como existen personas preocupadas por la evolución y cuidado del ciberespacio y de las infraestructuras críticas que lo habitan, que lo emplean con fines productivos, educativos, y de seguridad y para el desarrollo, también existen algunos actores estatales y no estatales que le dan un empleo negativo y perjudicial al ciberespacio, van de lo lesivo hasta actos criminales. En consecuencia, al ciberespacio también se puede considerar como un dominio interactivo, virtual, complejo, y ubicuo, a partir del cual emerge una interacción dinámica entre personas, *software*, y redes informáticas interconectadas mediante dispositivos tecnológicos a través de la red, con fines diversos, tales como la transmisión, la comunicación, la aproximación, o interacción. De ahí que esta interacción entre los actores y factores mencionados debe hacerse en un ambiente seguro, por lo que este dominio virtual debe ser protegido, derivando en lo que se concibe como

⁷ Vid, Alberto Ramos Toxtle, Gestión estratégica de la ciberseguridad en las infraestructuras críticas para fortalecer la seguridad nacional de México, tesis de Doctorado en Defensa y Seguridad Nacional, CESNAV, agosto 23, 2022, 193p.

la ciberseguridad, encargada de brindar salvaguarda y protección a la información, frente a todo tipo de antagonismo relacionado con las amenazas que transcurren por el ciberespacio.

El ciberespacio comenzó a incluirse en las estrategias militares de seguridad nacional a partir de 1998, primero, para la protección de infraestructura crítica, la detección de ciberamenazas, la guerra de la información y la ciber-resiliencia, hasta que Estados Unidos definió al ciberespacio formalmente en 2006 como el quinto entorno operacional, al mismo nivel que la tierra, el aire, el mar y el espacio ultraterrestre, lo que impulsó la investigación, el desarrollo y la innovación tecnológica para desarrollar capacidades de seguridad en el ciberespacio, como son: seguridad de la información, ciberseguridad, ciberdefensa, ciberinteligencia, entre otras, para que el Estado-nación haga frente a toda la gama de amenazas tradicionales y emergentes en y a través del ciberespacio.

Amenazas y riesgos

La ciberseguridad debe prevenir y minimizar los efectos que producen la intrusión, la manipulación e interrupción de los sistemas o las redes que pueden afectar su funcionamiento generando consecuencias catastróficas. De manera que los medios, herramientas y aplicaciones que se emplean actualmente para vulnerar los sistemas, engañar a las personas, dañar redes y bases de datos son cada vez más sencillas y fáciles de usar, lo que ha hecho más vulnerable al ciberespacio, en la medida en que intervienen más actores. Y esto se deriva de la exposición en la que se encuentra el ciberespacio, sujeto a expensas de las habilidades de personas que aprenden fácilmente a manipular herramientas de cómputo y *software* en perjuicio del objetivo de quienes hacen presencia legal en el ciberespacio: son los ciberdelincuentes.

La tecnología ha cambiado la forma en que vivimos, trabajamos y convivimos en y con la sociedad, en paralelo ha generado el despliegue de un amplio número de amenazas en el ciberespacio. Tales

amenazas se pueden materializar en el cuidado para aprobar los accesos y los niveles en cada uno de los peldaños de las infraestructuras críticas. Adecuar las medidas de protección ante estas amenazas tiene por objetivo la protección de todos los activos de información y, por supuesto, de los procesos de las infraestructuras críticas.

El incremento exponencial de ciberataques que se ha observado en los últimos años incluye los riesgos y amenazas no tradicionales, las cuales tienen a las infraestructuras y a los individuos por objetivos principales, con implicaciones que repercuten en la vulnerabilidad del Estado y pueden producir graves afectaciones en el funcionamiento de la sociedad. Y así se considera que la información para el Estado mexicano es un activo invaluable, toda vez que es la materia prima para la toma de decisiones y operación de infraestructuras en diferentes áreas, desde el nivel estratégico hasta el nivel táctico, pasando por el operacional. Además, en la operación de las infraestructuras críticas, la información que se transmite en forma de datos es vital. Por ello, cualquier forma que ésta adquiera, ya sea escrita, almacenada electrónicamente, transmitida por correo o por medios electrónicos, presentada en imágenes, expuesta en una conversación o distribuida por cualquier medio, siempre debe protegerse en forma adecuada y preservar sus características fundamentales de disponibilidad, autenticidad, confidencialidad e integridad. En ese sentido, la intromisión de los hackeractivistas de *Guacamayas Leaks* a los servidores de la SEDENA generó un gran daño.

Lo anterior muestra los matices, dimensiones y las características de la ciberseguridad. Por ello, la previsión de los incidentes en la ciberseguridad afectan a las propiedades básicas de la información desde lo físico hasta lo intangible, lo que implica reiterar que la confidencialidad, integridad y disponibilidad de la información, así como los sistemas de información, servicios o redes, que influyen sobre uno o más activos de información, representan los factores que deben ser asegurados.

Así, los incidentes de ciberseguridad pueden ser provocados por fallas en los propios sistemas, en los recursos humanos que laboran *in situ* y por actores externos. El factor humano es el eje fundamental de los riesgos en ciberseguridad. Por ello es necesario conocer cómo se relacionan las ciberamenazas con los diferentes actores; sus objetivos e intereses.

Las Infraestructuras Críticas de Información son las de los sectores del Petróleo, Telecomunicaciones, Financiero, Energía, y Militar, las cuales, en caso de un ciberataque, pueden sufrir consecuencias catastróficas para la Seguridad Nacional. A su vez, las empresas privadas ponen atención sobre otros sectores que suministran servicios, como los de salud, transporte, los de las industrias química, de la alimentación, telecomunicaciones, administración, finanzas, e incluso investigación.

Así, este crecimiento del ciberespacio, causado por la evolución tecnológica, representa, al mismo tiempo, una gran vulnerabilidad. Los ciberdelincuentes buscan permanentemente la oportunidad de obtener beneficios con sus actividades criminales, o de dañar las infraestructuras críticas de información de los Estados. La hostilidad se remonta al origen del internet, y actualmente es más refinada, lo cual demanda una capacidad de respuesta similar, o superior, para prever este tipo de actividades delictivas.

Los ciberdelincuentes pueden ser actores estatales o no estatales. Cada ciberataque dimana de un ciberdelincuente, que trata de violentar la seguridad de una infraestructura crítica.

En síntesis, podemos observar que el ciberespacio, considerado como el quinto de los dominios de la guerra, posee una multidimensionalidad que nos conduce a nuevos riesgos y amenazas, por lo que es necesario prever áreas especializadas en ciberseguridad, que protejan las infraestructuras críticas de un país.⁸

⁸ Vid el alegato sobre ciberespacio y lo aeroespacial, los nuevos campos del poder operacional de las fuerzas armadas, después de la tie-

Como los ciberataques siempre pueden ser replicados, hay que aprender de tales acontecimientos. Muchas compañías y gobiernos han sufrido ataques en años recientes. Prácticamente no hay ámbito que no los hayan sufrido. Estos incluyen fraudes, ataques dirigidos, secuestro de computadoras, hacktivismo, robo de información pública y privada, y de identidad (especialmente en el sector financiero). Toda una gama de acciones que amerita la intervención jurídica.

Los ciberataques nos muestran el alcance y el límite de los riesgos y amenazas a la que se exponen las infraestructuras críticas de una nación. Sin embargo, los grupos delictivos, actores estatales o no estatales, valoran los procesos que conducen a los bienes y servicios de carácter estratégico, para las industrias claves de un país, por lo que la ciberseguridad implica una atención siempre inmediata. La teoría y la práctica de la ciberseguridad abarca en su actual transversalidad todos los ámbitos en la vida de la sociedad, y nos lleva a afirmarla como el elemento central para avanzar en el desarrollo y seguridad de nuestra nación en el presente y futuro inmediato.

Esto implica que las infraestructuras críticas de información deben tener un nivel máximo de protección en todos los ámbitos y, si bien puede diagnosticarse que existe un vacío respecto a una política o estrategia de Ciberseguridad Nacional, que proporcione los lineamientos, procedimientos, normas y mecanismos que constituyan una arquitectura robusta, hay conciencia en algunos grupos de trabajo que para su fortalecimiento se requiere de la mayor voluntad política y de los recursos para su impulso.

También debe considerarse de vital importancia para la sobrevivencia de estas infraestructuras que se gestione la ciberseguridad

rra, el mar, el aire y el espectro radioeléctrico en Emilio Vizarratea, *El ciberespacio y su relación con el desarrollo aeroespacial*, presentado en el Colegio de Defensa Nacional, en el Seminario “El ámbito aeroespacial, en la defensa y seguridad nacional del Estado Mexicano”, celebrado el 15 al 17 de junio de 2015.

de manera estratégica, de tal forma que la coordinación facilite la función preventiva, sentido último de toda planeación estratégica, permitiendo que los recursos (humanos y materiales) relacionados con citadas infraestructuras actúen de manera proactiva, con el objetivo de que el nivel de riesgo se minimice y se obtenga un nivel adecuado de seguridad.

El presupuesto favorece la actualización y mejora en el equipo y, junto a la profesionalización del personal. Pero la prevención de los ciberataques debe ser cada vez más inteligente y constante, de modo de que dichos equipos consumen y demandan recursos, dado que la tecnología avanzada está disponible a los ciberdelinquentes y ellos cuentan con mayor cantidad de recursos y financiamiento.

Mucho de lo que hemos anotado arriba, tiene correlatos en la praxis del ciberespacio, la ciberseguridad y la ciberdefensa, de modo que requiere un ejercicio de reflexión que se articule en una legislación al respecto, y contemple los diversos actores, estructuras, procesos, infraestructuras críticas, elementos delin cuenciales y que sea preventivo y punitivo. El caso que se expone a continuación colocó en una situación de alto riesgo a las instituciones gubernamentales mexicanas, más allá de la secrecía de su tratamiento. Por el riesgo y la amenaza a la seguridad nacional, debe valorarse para lograr la necesaria resiliencia y la prevención.

Ciberataque a la SEDENA⁹

A finales de 2022, la Secretaría de la Defensa Nacional (SEDENA) sufrió un ataque a su infraestructura tecnológica, en la cual se vulneró información de sus actividades, la cual fue ampliamente

⁹ En 2023, impartí un curso sobre tópicos de inteligencia y seguridad nacional en el CEEFA de la SEDENA. Estaba muy reciente el ciberataque de Guacamayas a la SEDENA. Las siguientes notas son la resonancia de esa reflexión académica, donde se ubican alegatos de la ciberseguridad, los derechos digitales y la necesaria resiliencia

publicitada por los medios de comunicación y redes sociales. Esta situación representa un problema mayor, no sólo para la SEDENA, sino para el Estado mexicano en su conjunto.

Debido a que se reflejan las vulnerabilidades de sistemas y equipos, esta situación se debió a una falta de leyes, reglamentos y normatividad —no sólo acerca de derechos digitales, sino también de ciberseguridad, que impulse y coordine a las instancias para que articulen la detección oportuna de amenazas y riesgos contra la seguridad nacional y las instituciones públicas y privadas—, además de sanciones para este tipo de delitos, ya que, desafortunadamente, representan un enemigo intangible, sin fronteras o límites, que está tomando ventajas sobre muchos países.

Este hackeo vulneró la seguridad cibernética de la SEDENA e impactó en las fuerzas armadas y en el Gobierno mexicano en su totalidad, pues fueron afectadas algunas comunicaciones oficiales, de carácter privado, confidencial y de seguridad.

Aun con las dificultades de asegurar fuentes de información creíbles, en el ambiente del ciberespacio es necesario registrar los elementos que los propios autores aceptan como parte de sus acciones, de sus responsabilidades, y, obviamente, de las consecuencias que provocaron. La tipología delictiva no está plenamente desarrollada, pero existen elementos analógicos, como la Ley de Seguridad Nacional.

Asumió la responsabilidad del ciberataque el grupo *Guacamaya Leaks*, *hackers* activistas que se autoproclaman como “un colectivo contra la militarización de la región latinoamericana”. Durante 2022, aprovecharon vulnerabilidades en ciberseguridad en las fuerzas armadas de Guatemala, Chile, Colombia y Perú y filtraron información de sus servidores a medios de comunicación. Este grupo aprovechó una vulnerabilidad del

estratégica en infraestructuras críticas. Agradezco las voces de los participantes de ese curso, que acompañan al texto.

correo institucional de la Secretaría de la Defensa Nacional, el cual se empleaba para el intercambio de mensajería instantánea con dependencias civiles y militares, de donde se extrajo información relacionada con actividades operativas, administrativas, logísticas y de inteligencia.¹⁰

Por otro lado, cabe destacar que el ataque cibernético a la SEDENA duró aproximadamente veinte días, el cual comenzó a gestarse a finales de agosto del 2022 y fue detectado a principios de septiembre del mismo año. Al tomar conciencia del hecho, se tomaron acciones para contener la extracción de información, evaluar el daño causado, verificar qué información se vulneró y determinar cómo se realizó el evento.

Cabe mencionar que la SEDENA no es la primera institución del Estado mexicano que ha sufrido ataques de esta naturaleza, ya que, en 2019, se extrajeron y secuestraron alrededor de 180 mil archivos de Pemex, por los cuales se pidieron 4.9 millones de dólares; otras instancias han sido la Lotería Nacional y la Plataforma Nacional de Transparencia, así como BANJERCITO.

Según un estudio de Sophos, una empresa británica de *software* y *hardware* de seguridad, de doscientas organizaciones en México, 74 por ciento fue víctima de *ransomware*, pagando un promedio de casi 500 mil dólares; además, dio a conocer que en 2021 este tipo de ataques creció 600 por ciento en nuestro país.

Guacamaya Leaks es una organización internacional de *hackers* que ha publicado en diferentes medios de comunicación, informes anónimos y documentos filtrados con contenido sensible en materia de interés público. En sus manifiestos se define como anticolonialista y antiimperialista, actúa contra las Fuerzas Armadas de varios países y contra empresas extractivistas y petroleras, en defensa de los territorios y la naturaleza de *Abya Yala*.

¹⁰ Vid los diversos comentarios en su página oficial de IDT Consulting,

Los hacktivistas explican aquí sus motivaciones:

Los ejércitos de *Abya Yala* (el término indígena que usan para referirse al continente americano) han garantizado y facilitado la entrada de empresas extractivistas provenientes del Norte Global. Son los guardaespaldas. El ejército armado es el que ejerce el trabajo sucio de los Estados, de las empresas, de la delincuencia organizada como el narcotráfico.

Su nombre comenzó a resonar a partir del 19 de septiembre de 2022, en pleno Día de las Glorias del Ejército en Chile, al difundir 400 mil correos electrónicos del Estado Mayor Conjunto de ese país, que contienen análisis de los países vecinos, la crisis migratoria, el conflicto mapuche, el estallido social de 2019 y el trabajo de activistas.

El grupo anuncio más filtraciones de datos en Perú, El Salvador, Colombia y México. Así, en Colombia filtraron alrededor de 275 gigabytes de información de las Fuerzas Armadas, y casi 5 terabytes de la Fiscalía; en Perú difundieron 35 gigabytes de datos del Comando Conjunto de las Fuerzas Armadas y 70 gigabytes del Ejército.

Al revisar los documentos filtrados por *Guacamaya*, un grupo de 65 periodistas descubrió que el conglomerado Suizo-Ruso-Solway, controlador de *Fénix*, tenía planes para incendiar cultivos de subsistencia, comprar líderes locales y pagar a la Policía Nacional; sin embargo, de los hackeos a empresas *Guacamaya* pasó a los ejércitos latinoamericanos, a los que acusa de cómplices del extractivismo. A la última filtración de correos de militares latinoamericanos la llamaron “Operación Fuerzas Represivas”.

El 19 septiembre de 2022, *Guacamaya Leaks* se adjudicó el ataque a la Secretaría de la Defensa Nacional, donde extrajeron aproximadamente 6 terabytes de información, compartida a la prensa. La comenzó a publicar el periodista Carlos Loret de Mola en su portal *Latinus*, la cual ha sido retomada por diferentes medios de comunicación y en redes sociales. De forma general hicieron referencia inicial a los temas siguientes:

- La salud del Lic. Andrés Manuel López Obrador, presidente de México.
- En las Fuerzas Armadas prevalecen acciones y prácticas ajenas a la democracia, violaciones a los derechos humanos, incluso en sus propias filas.
- Monitoreo a grupos feministas que son catalogados con el mismo grado de riesgo para la seguridad que los defensores del territorio.
- Los cárteles del narcotráfico.
- Posible colusión de militares con el crimen, personajes políticos o los gastos en lujos por cuenta de altos funcionarios castrenses.

La información extraída fue publicado ampliamente en prensa, radio, televisión y en redes sociales. Sólo registró los tópicos más relevantes, y con colocarlos en la red, aparecen los contenidos, las fuentes y algunos comentarios de periodistas y analistas:

- La familia del Presidente y sus viajes privados.
- El Hospital Central Militar al servicio de funcionarios cercanos al Presidente.
- El Ejército detectó intenciones de huachicoleros para matar al Presidente.
- Beatriz Gutiérrez Müller usa a militares para limpieza.
- Adán Augusto López entregó Tabasco a presuntos líderes del CJNG.
- Gobiernos de MORENA tendrían nexos con el narco.
- Gobierno de Veracruz apoyó al Cártel del Noroeste.
- Revelan radiografía del crimen organizado en la Ciudad de México y Estado de México.
- La batalla secreta entre CJNG y Unión Tepito en la capital.
- Los movimientos de Rafael Caro Quintero.

- Al menos veinte alcaldes de Guerrero presuntamente vinculados con narcos.
- SEDENA compró *software* de espionaje en 2019.
- El seguimiento a Ken Salazar, embajador de Estados Unidos.
- CONACYT quería probar la vacuna *Patria* en militares.
- Advierten el colapso del Tren Maya.
- Operativo para rescatar a Evo Morales (AMLO envió un operativo para rescatar al expresidente de Bolivia en 2019).
- Fiesta del narcotraficante “Mencho”.
- Espionaje militar al margen de la ley por el Centro Militar de Inteligencia.

De acuerdo con los registros anteriores, sólo anotados por su fácil ubicación en redes y medios, los servidores de la SEDENA fueron vulnerados, generando que temas diversos hayan sido expuestos a medios de comunicación locales y posteriormente a la opinión pública mundial, evidenciando la necesidad de intensificar los protocolos de ciberseguridad por la SEDENA y el resto de las instituciones públicas y privadas de México.

A corto plazo, es necesario verificar toda la información sustraída por los hacktivistas de *Guacamaya*, así como identificar las personas que tuvieron acceso, una vez que ésta fue compartida. Esto permitirá generar inteligencia e implementar medidas pasivas y activas de contrainteligencia con la finalidad de reducir el impacto de las acciones que efectúen organizaciones, actores públicos y privados desafectos a esta Secretaría, al actual Gobierno de la República.

Zamarrón señaló que “En México hacen falta 260,000 profesionales de ciberseguridad y el caso de *Guacamaya Leaks* ratificó la importancia de este sector dentro de gobiernos y empresas” (2022). Por tal motivo es necesario que, a mediano y largo plazo, el país y la SEDENA destinen mayor inversión al desarrollo del

recurso humano que atiende esta grave problemática, así como se fortalezca el sistema educativo militar, asignando a las universidades públicas y privadas la impartición de carreras, diplomados, seminarios y cursos en ciberseguridad, para combatir a los ciberdelinquentes, quienes han desarrollado métodos más avanzados e impredecibles.

CONCLUSIONES

La delincuencia, como los ciberataques emprendidos por *Guacamaya Leaks*, se desarrolla a nivel mundial, por lo que se requieren mecanismos de cooperación multilateral con el propósito de intercambiar información, métodos y técnicas que permitan hacer eficientes las medidas de ciberseguridad.

Para la SEDENA resulta fundamental fortalecer sus procesos de ciberseguridad; renovando la infraestructura, capacitando a su personal y previendo a largo plazo nuevos ataques; dichos procesos deben tener como finalidad objetivos, como incapacitar los movimientos operativos o que arriesguen la integridad del personal militar.

Esta falta de seguridad cibernética vulnera a la institución armada en el país frente a todos los mexicanos al disminuir la confianza en el Ejército, que es la “la última línea de defensa” del país; asimismo, es afectada la imagen institucional en el entorno internacional.

Para lograr resiliencia después del ataque de *Guacamaya Leaks*, se recomienda lo siguiente:

- El Centro de Operaciones del Ciberespacio (COC) de la SEDENA en coordinación con la Dirección de Informática tendrán que evaluar a fondo el incidente con el objetivo de conocer el alcance y naturaleza del ataque, así como qué sistemas fueron dañados.

- La Secretaría de la Defensa Nacional deberá realizar un estudio e implementar un nuevo procedimiento a partir de las lecciones aprendidas, dedicado exclusivamente a ciberataques y al manejo de información sensible.
- Implementar mecanismos interinstitucionales para compartir información y técnicas de atención con otras dependencias como el Centro Nacional de Respuesta a Incidentes de Seguridad Informática, la Secretaría de Marina Armada de México, Seguridad y Protección Ciudadana, Centro Nacional de Inteligencia y la Guardia Nacional.
- Revisar las políticas en materia de ciberseguridad, para determinar actualizaciones, si los procedimientos son adecuados y qué procedimientos no se realizaron para evitar el incidente.
- Acrecentar el presupuesto destinado a las Tecnologías de la Información y Comunicación (TICs), sistemas de ciberseguridad y capacitación.
- Revisión y actualización del marco legal e institucional en la materia.
- Antes del proceso de estudio de contrainteligencia, hay que difundir las lecciones aprendidas, de forma interna, y en la medida de lo posible, de forma interinstitucional.
- Gestión de riesgos y amenazas, con la capacidad de anticipar crisis.
- Necesidad de una regulación oportuna y apropiada sobre infraestructura crítica de la SEDENA, SEMAR y SSPYPC.
- Determinar las previsiones apropiadas para garantizar procesos continuos y operativos en todas las circunstancias.
- Desarrollo de ejercicios y proyectos de simulación de ciberataques y aplicación de protocolos para la ciberseguridad.
- Generar la cooperación a nivel municipal, estatal, nacional, regional, internacional y privada.

- Estudiar el concepto de “Mejora Continua” de la industria e iniciativa privada, para su posible adaptación.
- Estudiar la protección física y permanente de instalaciones donde se alojan las infraestructuras estratégicas y críticas de TIC de la institución.
- Estudiar la viabilidad del uso de *software* de código abierto basado en Linux, para reducir costos; sin embargo, esto implica mayor gasto en capacitación, aunque evita la dependencia de compañías y licencias.
- En la capacitación del capital humano se debe hacer especial énfasis, ya que los elementos profesionales y técnicos son el eslabón para el éxito en este campo de batalla.

En suma, la resiliencia cibernética ante el robo de información por *Guacamaya Leaks* implica revalorar la necesidad de contar con sistemas de ciberseguridad, robustos y actualizados, establecer políticas claras de manejo de la información, monitorear constantemente los sistemas de información, contar con un plan de respuesta inmediata y capacitar permanentemente al personal en temas de seguridad informática, ciberdefensa y manejo de la información confidencial.

Estas recomendaciones permitirán a las organizaciones gubernamentales enfrentar situaciones similares en el futuro y garantizar la Seguridad Nacional de México. La necesidad de una ciberseguridad es evidente. A partir de la relevancia del ciberespacio, la aplicación de un derecho digital muestra su necesidad en función de las características distintivas del ataque a la Secretaría de la Defensa Nacional.

BIBLIOHEMEROGRAFÍA

Ascencio, C., *Guacamaya Leaks: entre la inteligencia y el abuso estatal*, connectas.org, 2022, en <https://www.connectas.org/analisis/latinoamerica-hacktivismo-guacamaya-leaks/>.

Buzan, Barry; de Wilde, Jaap, y Waever, Ole, *Security: A New Framework for Analysis*, Lynne Rienner Publishers, UK, 1997, 190p.

Casa Blanca, National Cybersecurity Strategy, en *National-Cybersecurity-Strategy-2023.pdf* (whitehouse.gov)

CESNAV-CODENAL, *Glosario de Términos en materia de seguridad en el ciberespacio*, 2021, 210p.

Coordinación de Estrategia Digital Nacional, Coordinación de Estrategia Digital Nacional | Gobierno | gob.mx (www.gob.mx).

Diputados, Cámara de, *Iniciativa con proyecto de decreto por el que se expide la Ley Federal de Ciberseguridad 2023*, en *02_iniciativa_292_25abr23.pdf* (diputados.gob.mx)

Estrada, C., *Guacamaya Leaks: ¿Qué hacer con lo que sabemos?* Edición 491 Instituto Tecnológico y de Estudios Superiores de Occidente (ITESO), 2023, en <https://magis.iteso.mx/nota/guacamaya-leaks-que-hacer-con-lo-que-sabemos/>.

Forbes Staff, *Hackeo masivo a SEDENA evidencia vulnerabilidad de ciberseguridad; así fue el ataque*, 2022, en <https://www.forbes.com.mx/hackeo-masivo-a-sedena-evidencia-vulnerabilidad-de-ciberseguridad-asi-fue-el-ataque/>.

Gibson, W., *Neuromante*, Ace Book, Canadá, 1984.

Gómez, M., *En busca de una modelo de resiliencia cibernética basado en las experiencias de la OTAN y su posible transferencia a América del Sur*, Editorial Autores de Argentina, 2019.

Grotberg, E., *Introducción: nuevas tendencias en resiliencia*, Wisconsin: Universidad de Wisconsin, 1995.

Han Byung-Chul, *Infocracia*, Taurus, México, 2022, 103p.

ITD Consulting. (2022). *Guacamaya Leaks: el gran ciberataque a la ciberseguridad latinoamericana de 2022m* en <https://itdconsulting.com/backup-y-recovery/guacamaya-leaks-el-gran-ciberataque-a-la-ciberseguridad-latinoamericana-de-2022/>.

Junta Interamericana de Defensa, *Guía de Ciberdefensa; orientaciones para el diseño, planeamiento, implantación y desarrollo de una ciberdefensa militar*, Canadá, 2020, 113p.

Preciado, R.. *Guacamaya Leaks y la Seguridad Nacional*, Rafael Preciado Hernández, 2022, en http://frph.org.mx/bdigital/uploads/827_frph_guacamaya_leaks_y_la_seguridad_nacional_vf.pdf.

Ramos Toxtle, Alberto, *Gestión estratégica de la ciberseguridad en las infraestructuras críticas para fortalecer la seguridad nacional de México*. CESNAV, tesis de Doctorado en Defensa y Seguridad Nacional, agosto 23, 2022, 193p.

Ruido en la Red. (2022). *Guacamaya Leaks: recopilación de las revelaciones del hackeo a la Sedena*, en <https://ruidoenlared.com/que-es/guacamaya-leaks-filtracion-hackeo-sedena/>.

Senado, Cámara de, Iniciativa Ciberseguridad Sen. Miguel Ángel Mancera 2020, en Microsoft Word-IN. CIBERSEGURIDAD 30082020.docx (senado.gob.mx)

SEMAR-Sedena, *Glosario de términos en materia de seguridad en el ciberespacio*, junio 2021.

SEMAR-Sedena, *Glosario de términos unificados en seguridad nacional*, México, 2021.

UE, *Parlamento Europeo. Comunicación de la Comisión al Parlamento Europeo y al Consejo sobre “El planeamiento de la UE sobre la resiliencia y la reducción de riesgos de catástrofes en los países en desarrollo: aprender de las crisis alimentarias*, Parlamento Europeo, 2012.

Unión (2022), *Hackeo SEDENA y Guacamaya. ¿Cómo fue y qué pasó? Esto es lo que sabemos*, en <https://www.unionguanajuato.mx/2022/09/30/hackeo-sedena-y-guacamaya-como-fue-y-que-paso-esto-es-lo-que-sabemos/>.

Vizarrete, Emilio, *El saber político: Platón y Aristóteles*, SEMAR-ININVESTAM, México, 2016, 403p.

Vizarrete, Emilio, *Poder y seguridad nacional*, CESNAV, 2013, 582p.

Vizarrete, Emilio, *Repensar México, introducción a la seguridad y defensa nacionales*, SEMAR-CESNAV, 2020, 483p.

Vizarrete, Emilio, *Sobre el discurso estratégico*, SEMAR-LXIII Legislatura, Cámara de Diputados, 2016, 164p.

Vizarrete, Emilio, Estabilidad y desarrollo regional para la seguridad mexicana, *La Seguridad Nacional Integral de México; diagnósticos y propuestas*, CESNAV, 2013, pp. 61-75.

Vizarrete, Emilio, La importancia de la información y la inteligencia en los modelos geopolíticos contemporáneos, *Inteligencia Estratégica; retos y oportunidades para México*, CESNAV, 2014, pp. 215-239.

Vizarrete, Emilio, *El Ciberespacio y su relación con el desarrollo aeroespacial*, presentado en el Colegio de Defensa Nacional, en el Seminario “El ámbito aeroespacial, en la defensa y seguridad nacional del Estado Mexicano”, celebrado el 15 al 17 de junio de 2015.

Zamarrón, I., *Guacamaya Leaks evidencian brecha de profesionales de ciberseguridad*, Forbes México, 2022, en <https://www.forbes.com.mx/guacamaya-leaks-evidencia-brecha-de-profesionales-de-ciberseguridad/>.

Ciudades inteligentes: innovación tecnológica para el futuro urbano

NORA ANGÉLICA DAMIÁN SANTIAGO¹

INTRODUCCIÓN

En pleno siglo XXI hablar de Inteligencia Artificial (IA) es hablar del futuro que nos ha alcanzado: hoy vivimos en medio de la evolución continua de las tecnologías de la información y la comunicación, y la manera en que las sociedades se adaptan y responden a los desafíos y oportunidades que estas tecnologías plantean. La IA, el Internet de las Cosas, la realidad aumentada y el *blockchain*² son sólo algunas de las tecnologías emergentes que prometen seguir transformando el paisaje social, económico y cultural.

El uso de la IA como cerebro de las Ciudades Inteligentes desempeña un papel fundamental como motor de innovación y transformación, procesando y analizando vastos conjuntos de datos provenientes de sensores, cámaras, redes sociales y otras fuentes que permiten que los sistemas tecnológicos perciban su entorno, se relacionen con él, resuelvan problemas y actúen con

¹ Licenciada en Derecho y estudiante de la Especialización de Derecho Constitucional (UNAM, México), asesora del Comisionado Ciudadano en el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

² Tecnologías para los negocios, *¿Blockchain qué es y para qué sirve?*, s.f, en <https://ticnegocios.camaravalencia.com/servicios/tendencias/blockchain-que-es-y-que-ventajas-tiene/>

un fin específico, por lo que el uso de esta tecnología ha revolucionado muchos sectores de la economía y la sociedad dentro de la Administración Pública, la cual hoy ya no es ajena a esta tendencia. Estos sistemas facilitan la interacción con nuestros dispositivos móviles usando algoritmos que toman decisiones críticas en sectores como la medicina, las finanzas y la seguridad nacional, que mejoran la eficiencia, la accesibilidad y la efectividad en múltiples espacios, por lo cual la capacidad de la IA para influir en los resultados públicos y sociales, económicos y políticos es inmensa. Por tanto, se debe asegurar que los sistemas de IA operen de manera justa y transparente, mientras se minimiza el riesgo de daños en la sociedad. Asimismo, los gobiernos están adoptando el uso y aplicación de la IA, con el objetivo de transformar las ciudades en entornos más habitables, sostenibles y eficientes.

En los distintos niveles de gobierno la meta de la Administración Pública consiste en satisfacer las demandas de la población mediante la prestación de servicios públicos. Para lograr esto el Estado comunica sus acciones, proporcionando información accesible, completa y útil. No obstante, ésta enfrenta cotidianamente desafíos relacionados con la burocracia, la falta de eficiencia y las limitaciones en su capacidad de respuesta.

En el contexto mexicano, la Administración Pública ha experimentado una evolución a lo largo del tiempo, basándose en una teoría de jerarquía y autoridad clara y directa que ha perdurado por siglos. A pesar de ello, el trabajo sustancial realizado por la Administración Pública ha mostrado una creciente falta de alineación con esta visión tradicional de gobernar. Cada vez más, los administradores públicos gestionan asuntos, no a través de la autoridad directa, sino mediante diversas estrategias.

¿Qué es una Ciudad Inteligente o Smart City? Sus características y cuál es la relación con la IA

Primero definamos qué es una Ciudad Inteligente o *Smart City*. Este término comenzó a discutirse en la década de los noventa

del siglo xx cuando se relaciona la inteligencia con el funcionamiento de los mecanismos del espacio urbano mediante el uso de Tecnologías de la Información y Comunicaciones (TIC) y, más recientemente con el uso y aplicación de la IA que desempeña un papel fundamental, con el objetivo de gestionar de manera eficiente aspectos, como el uso de energía, las vías de comunicación, el transporte, los servicios públicos, el gobierno y la infraestructura urbana, el análisis de datos, la optimización de los recursos, el ofrecer servicios públicos personalizados y anticipar fallas en la infraestructura, implementar sistemas de vigilancia y combatir el crimen, una planificación urbana más eficiente y sostenible, todos estos factores que pueden amenazar el buen funcionamiento de las ciudades.

De acuerdo con la Comisión Económica para Europa de las Naciones Unidas y la Unión Internacional de Telecomunicaciones (2019) es:

Una ciudad innovadora que utiliza la tecnología de la información, la comunicación y otros medios para mejorar la calidad de vida, la eficiencia de las operaciones, los servicios urbanos y la competitividad; al tiempo que garantiza que satisfice las necesidades de las generaciones presentes y futuras con respecto a los aspectos económicos, sociales, ambientales y culturales.³

Una ciudad inteligente es un modelo de desarrollo urbano basado en la adopción de tecnologías digitales [Internet de las cosas, (IoT), redes 5G, inteligencia artificial (IA), grandes datos, cómputo en nube, vehículos autónomos y otros] para optimizar la eficiencia de las operaciones y los servicios de la ciudad a fin de aumentar la calidad de vida de sus habitantes y de contribuir a la mejora del medioambiente.⁴

³ ONU-Habitat explora el uso de la inteligencia artificial en las ciudades 13 de marzo de 2019, en <https://onuhabitat.org.mx/index.php/onu-habitat-explora-el-uso-de-la-inteligencia-artificial-en-las-ciudades>.

⁴ Comisión Económica para América Latina y el Caribe, *Tecnologías digitales para un nuevo futuro*, Naciones Unidas, 2021, en <https://repositorio.cepal.org/server/api/core/bitstreams/879779be-c0a0-4e11-8e08-cf80b41a4fd9/content>.

La deficiencia del transporte público, los elevados niveles de congestión vehicular, la contaminación del aire, la gestión de residuos y el acceso a agua potable, salud y educación, así como la inseguridad, son problemas que las políticas de desarrollo urbano deben abordar. Los modelos de ciudades inteligentes pueden ofrecer soluciones efectivas a estos desafíos.

Para fomentar el desarrollo de las ciudades inteligentes, es necesario contar con una gobernanza definida que tome en cuenta los aspectos locales, como la implementación de infraestructura tradicional (vial, sanitaria y eléctricas, entre otras) y digital, así como el fortalecimiento del capital humano. Esto debe estar alineado con un marco de gobernanza nacional que promueva el avance digital (redes 5G, Internet de las cosas, entre otros) y gestione los riesgos tecnológicos, tales como la privacidad de los datos y las amenazas a la ciberseguridad. Todo esto es crucial para generar confianza en la ciudadanía respecto del uso de las tecnologías digitales.

Las ciudades inteligentes ofrecen una variedad de beneficios que afectan positivamente la calidad de vida de los ciudadanos, la eficiencia de los servicios urbanos y la sostenibilidad ambiental.⁵ Algunos beneficios clave de las ciudades inteligentes son:

- Eficiencia en la gestión del tránsito para reducir el congestionamiento vehicular, mejorar la movilidad y minimizar la emisión de gases contaminantes.
- Mejora en la planificación y gestión del transporte público, incluyendo rutas más eficientes y horarios dinámicos, que faciliten el desplazamiento de los ciudadanos, así como el alquiler de bicicletas y la mejora de la infraestructura para ciclistas fomentan sistemas de transporte sostenible.

⁵ Business School University of Navarra, *¿Cuáles son las ciudades más “inteligentes” del mundo?*, 9 de abril de 2014, en <https://www.iese.edu/es/insight/articulos/ciudades-mas-inteligentes-mundo/>.

- Ahorro de Energía con el uso de la iluminación LED y la gestión energética avanzada, que contribuyen a la sostenibilidad ambiental.
- En el ámbito de la salud implementación de tecnologías, como registros electrónicos y sistemas de monitoreo remoto, así como mejora en la prestación de servicios de atención médica.
- Utilización de plataformas digitales y aplicaciones móviles que facilitan la participación ciudadana para que los ciudadanos se involucren más en la toma de decisiones y la resolución de problemas urbanos.
- Mejora en los sistemas de seguridad y vigilancia, para que sean más efectivos, gracias al uso de medios tecnológicos y el análisis de datos, lo cual brinda una respuesta más rápida y efectiva a situaciones de emergencia, mejorando la seguridad pública.
- Uso de sensores y sistemas de gestión permiten un uso más eficiente del agua en la irrigación, la limpieza de calles y otros servicios urbanos.
- Accesibilidad para personas con discapacidad, asegurando que los servicios y espacios urbanos sean inclusivos, a través del uso de la tecnología.
- Gobierno Electrónico y Gobierno Digital que facilitan la prestación de servicios gubernamentales en línea, simplificando procesos y mejorando la accesibilidad para los ciudadanos.

Esta implementación de tecnologías avanzadas impulsa la innovación y el crecimiento económico, atrayendo inversiones y fomentando la creación de empleo en sectores relacionados con la tecnología. Estos beneficios hacen que las ciudades inteligentes representen una propuesta atractiva para abordar los desafíos urbanos y mejorar la calidad de vida de sus residentes. Es importante abordar de manera adecuada las cuestiones relacionadas con la

privacidad, la seguridad y la equidad para garantizar una implementación exitosa y ética de estas tecnologías.

A menudo, se promueve la adopción de estas tecnologías como la base de la inteligencia en estos modelos, atribuyéndoles características progresistas y favorables que prefiguran un modelo emergente en la gestión urbana, donde el uso de las TIC's. Ahora, con las herramientas que la IA ofrece, sirven para mejorar la calidad de vida de los ciudadanos y sus habitantes, pues optimizan la eficiencia de los servicios urbanos. Así pues, es importante explorar los diversos aspectos de las ciudades inteligentes, desde sus beneficios hasta los desafíos. Las consideraciones éticas asociadas, impulsadas por el poder transformador de la tecnología, no sólo representan una tendencia global imparable, sino que se establecen como la **magnífica solución factible** para aminorar y dominar los graves resultados ambientales y socioeconómicos que la creciente urbanización está generando en nuestro planeta.

La transición hacia ciudades inteligentes requiere una responsabilidad y un compromiso conjunto de gobiernos, empresas, ciudadanos y organizaciones. Es fundamental invertir en tecnología, desarrollar marcos legales adecuados y fomentar la participación ciudadana para construir un futuro urbano más sostenible, próspero e inclusivo. Una regulación efectiva del uso de las tecnologías de la información y la inteligencia artificial (IA) será esencial para desarrollar políticas y marcos regulatorios que promuevan la inclusión digital, protejan los derechos de los usuarios y fomenten la innovación responsable.

El uso y la regulación de la IA son fundamentales, ya que, aplicada en sistemas de ciudades inteligentes, puede realizar tareas específicas sin ser consciente de ello, como los asistentes virtuales o los sistemas de recomendación. Aunque la capacidad de la IA para entender y razonar de manera autónoma, similar a la humana, sigue siendo mayormente teórica y no se ha realizado en la práctica, sus aplicaciones son amplias y variadas. Éstas abarcan desde el análisis automatizado de datos financie-

ros hasta vehículos autónomos, los diagnósticos médicos automatizados y personalización de experiencias de aprendizaje en plataformas educativas.

En el sector financiero, la IA se emplea para modelar escenarios económicos, gestionar riesgos, automatizar operaciones bursátiles y personalizar servicios para los clientes. En el ámbito de la salud, sistemas avanzados de IA están transformando el diagnóstico y tratamiento de enfermedades al interpretar grandes volúmenes de datos médicos para ofrecer diagnósticos precisos y recomendaciones de tratamiento personalizadas. Además, en el campo de la automoción, la IA es fundamental en los sistemas de conducción autónoma, gestionando la navegación, el control del vehículo, la optimización del tráfico y la seguridad en carretera.

Uno de los conflictos más significativos en la regulación de la inteligencia artificial (IA) es el equilibrio entre promover la innovación y proteger al público de posibles daños, especialmente en el contexto de fortalecer las ciudades inteligentes. Las regulaciones estrictas pueden frenar el desarrollo tecnológico y la competitividad en el mercado global, mientras que una regulación laxa puede resultar en el despliegue de tecnologías que no han sido adecuadamente evaluadas en términos de seguridad y ética.

Actualmente, el fundamento legal para la implementación de ciudades inteligentes varía según la jurisdicción y el país, pero la creación y operación de estas ciudades están respaldadas por una combinación de leyes, regulaciones y políticas gubernamentales que permiten la implementación de tecnologías y la gestión eficiente de servicios urbanos. Esto abarca la protección de datos y privacidad, la ciberseguridad, las normativas de construcción y desarrollo urbano, las licencias y regulaciones para tecnologías específicas, y la participación ciudadana. Es crucial que estas iniciativas se desarrollen dentro del marco legal existente y se adapten las leyes para abordar los desafíos

y oportunidades específicos que surgen con la implementación de tecnologías avanzadas en entornos urbanos.

La colaboración entre el sector público y privado, junto con la participación ciudadana, es esencial para lograr una implementación exitosa y sostenible de ciudades inteligentes. En pleno siglo XXI, varias ciudades en todo el mundo han adoptado tecnologías inteligentes para mejorar la eficiencia de los servicios urbanos y la calidad de vida de los ciudadanos. Estas iniciativas están alineadas con los Objetivos de Desarrollo Sostenible (ODS) aprobados por la ONU, especialmente el Objetivo 11, que busca lograr que las ciudades y los asentamientos humanos sean inclusivos, seguros, resilientes y sostenibles. Este objetivo representa el futuro del modo de vida global y es uno de los principales pilares de una ciudad inteligente.

¿Cuáles son las ciudades inteligentes en el mundo?

En el corazón de las ciudades inteligentes reside la ambición de crear experiencias excepcionales para sus ciudadanos. Desde sistemas que preservan recursos valiosos como la energía y el agua, hasta la optimización de la movilidad y otros servicios urbanos, la infraestructura del Internet de las Cosas (IoT), así como la IA, se convierten en el elemento central de esta transformación; se erigen como un modelo urbano innovador que aprovecha el poder de la tecnología para mejorar la calidad de vida de sus ciudadanos en múltiples aspectos.

Rozga, Ryszard y Hernández (2022) señalan que el Índice de Ciudades Inteligentes 2020 del Instituto Internacional para el Desarrollo de la Capacidad de Gestión (IMD) nos ofrece una valiosa radiografía de las urbes que están liderando la transformación hacia un futuro más sostenible, eficiente y conectado. En este análisis, destacamos los avances y desafíos de algunas ciudades ejemplares, como Shanghái, Seúl, Barcelona, Dubái, Ámsterdam,

Tokio, Zúrich, Singapur, Nueva York, Medellín, Buenos Aires, y la Ciudad de México.⁶

Shanghái, la metrópolis china, se ha convertido en un referente global de innovación urbana gracias a la implementación de la **Ciudad Nube**, una plataforma digital que ofrece a sus ciudadanos un **acceso integral a más de 1,200 servicios públicos**; este sistema pionero se ha convertido en el **punto de contacto central** con el gobierno municipal, eliminando la necesidad de buscar números telefónicos específicos para cada departamento o trámite.⁷

Seúl, la capital de Corea del Sur, ha implementado durante las últimas dos décadas activamente proyectos pioneros, como el uso de robots **patrulla autónomos**, **un programa piloto que circula en las calles de la ciudad**, y **las balizas inteligentes para la seguridad infantil** en guarderías y centros educativos que emiten señales constantes que permiten **rastrear la ubicación de los niños en tiempo real** en caso de que se extravíen.⁸

Barcelona, en 2015, comenzó a transformar su red y a desarrollar su infraestructura 5G, para que todos tengan acceso a internet a través de Wi-fi; la visión futurista de Barcelona permite planificar cosas como autobuses 5G autoconducidos y brindar transmisiones de video en directo mejoradas con IA para detectar delitos. Como zona turística, esta ciudad con perspectiva futurista sigue lanzando aplicaciones de fácil uso para los ciudadanos a través de IoT, como la gestión de residuos, las farolas inteligentes, el transporte público y los aparcamientos.⁹

⁶ *El concepto de Ciudad Inteligente en Europa y América Latina*, en <https://ru.iiec.unam.mx/5745/1/2.%20214-Rozga-Hern%C3%A1ndez.pdf>.

⁷ Smart Cities: la revolución tecnológica llega a las ciudades, en <https://www.iberdrola.com/innovacion/smart-cities>

⁸ *Seúl: la ciudad inteligente del futuro*, en <https://iccsi.com.ar/seul-ciudad-inteligente/>.

⁹ *Smarter Cities, Smarter Future*, en https://www.techradar.com/features/smarter-cities-smarter-future_

Dubái, Emiratos Árabes Unidos, se ha convertido en los últimos años en un importante centro de investigación e innovación en inteligencia artificial, que trabaja en el desarrollo de nuevas aplicaciones de la IA en campos como la salud, la educación y la seguridad, donde los ciudadanos residentes tienen una identidad digital (pase de los Emiratos Árabes Unidos) para acceder a los servicios gubernamentales. Es la primera ciudad totalmente impulsada por *blockchain*, con tres pilares estratégicos: eficiencia, creación de industria y liderazgo internacional; esto ayuda a optimizar la utilización de los recursos y promover la sostenibilidad ambiental; también se han implementado iniciativas en áreas como el acceso abierto a datos, el transporte inteligente, la optimización de los recursos energéticos y los parques y playas inteligentes para proporcionar servicios integrales y eficientes a los clientes y al turismo.¹⁰

Ámsterdam, Países Bajos, ganó en 2022 un premio a las ciudades inteligentes en el certamen *Smart City Awards*, gracias al proyecto *HackShield* que versa sobre seguridad y protección que ayuda a concientizar a los ciudadanos sobre las amenazas a la ciberseguridad en línea; la agencia gubernamental ofrece servicios de transporte público, planificación espacial y gestión del agua, y cuenta con un sistema energético inteligente que combina múltiples fuentes de energía renovables, tecnologías de almacenamiento, vehículos eléctricos y optimización del consumo energético en un único sistema inteligente de gestión de la energía.¹¹

Singapur intenta, por su parte, que todos los coches que circulen por las calles sean autónomos para 2025, que los es-

¹⁰ Las ciudades inteligentes en Emiratos Árabes: ejemplos de innovación y sostenibilidad, en <https://iccsi.com.ar/ciudad-inteligente-emiratos-arabes/?shared=false>.

¹¹ Ámsterdam gana el primer premio en los *Smart City Awards* 2022 por el proyecto *Hackshield*, en <https://siliconcanals.com/promoted-content/city-of-amsterdam-wins-smart-city-awards/>.

tudiantes de la Universidad Nacional de Singapur atraviesen el *campus* en un autobús autónomo, que los ciudadanos mayores y discapacitados puedan utilizar una flota autónoma de lanzaderas sin conductor para desplazarse por los complejos médicos, así que la ciudad ha incorporado un sistema de tarifas de peaje en tiempo real que utiliza las condiciones del tráfico para ajustar las tarifas y gestionar el flujo del tráfico. Derivado del impacto de covid-19, la población de trabajadores extranjeros en Singapur se redujo entre diciembre de 2019 y septiembre de 2021, lo que llevó a la ciudad-Estado a adoptar a los trabajadores robóticos como solución. De igual forma, se ha fomentado el método de pago sin efectivo para evitar que la gente tenga que llevar dinero en efectivo y hacer largas colas en los cajeros automáticos.¹²

Tokio es una de las ciudades más pobladas y tecnológicamente avanzadas del mundo. Busca convertirse en una ciudad inteligente y sostenible siguiendo los Objetivos de Desarrollo Sostenible de Naciones Unidas. La ciudad está implementando diversas acciones para mejorar la movilidad sostenible, como fomentar el uso del transporte público y la bicicleta, y reducir las emisiones de vehículos, así como promueve el uso de energías renovables, como la solar y la eólica, y trabaja en el reciclaje de residuos y la reducción de emisiones de gases de efecto invernadero. Además, Tokio está adoptando tecnologías de inteligencia artificial y análisis de datos para mejorar la seguridad y la resiliencia ante desastres naturales y emergencias. Se está enfocando en mejorar el acceso a servicios básicos, como la salud, la educación y el agua potable en áreas desfavorecidas, e impulsa la innovación en energía, transporte y gestión de residuos, colaborando con empresas y universidades para desarrollar tecnologías avanzadas.¹³

¹² *Technological Advancements That Make Singapore a Smart City*, 1 de febrero de 2023, en <https://www.iotforall.com/singapore-smart-city>.

¹³ *Tokio trabaja para convertirse en una ciudad inteligente y sostenible*, en <https://utopiaurbana.city/2023/05/12/tokio-trabaja-para-convertirse-en-una-ciudad-inteligente-y-sostenible/>.

Zúrich, Suiza, se ha convertido en un referente mundial en el desarrollo de ciudades inteligentes, gracias a la implementación de diversas iniciativas tecnológicas que buscan mejorar la calidad de vida de sus ciudadanos y la sostenibilidad del entorno urbano. Ejemplo de ello son las farolas inteligentes que son el punto de partida para una serie de innovaciones urbanas desde 2017. Estas farolas no sólo iluminan según la densidad del tráfico, reduciendo la energía en un 70 por ciento, sino que también ofrecen servicios adicionales, como carga para coches eléctricos, recopilación de datos ambientales y Wi-Fi público. El proyecto Ciudad Verde de Zúrich incluye edificios que funcionan con energías renovables, mientras que la ciudad ha implementado tecnologías IoT para monitorear la calidad del aire y los niveles de agua. Además, la policía y otros organismos colaboran en soluciones de movilidad y gestión de eventos, y se ha lanzado la aplicación móvil *Zürimobil* para ofrecer información de tráfico en tiempo real.

Nueva York, Estados Unidos, es una de las ciudades más densamente pobladas del planeta. Cuenta con un sistema automatizado de lectura de contadores a gran escala que ayuda a reducir el consumo de agua avisando a los clientes cuando detecta un consumo anormal y ya ha ahorrado millones de dólares. Asimismo, ha mejorado drásticamente su red de infraestructuras inalámbricas y habilitado sistemas inteligentes de gestión del tráfico. Los sensores inteligentes gestionan servicios, como la agricultura LED de interior, el control de la calidad del aire y el flujo del tráfico, y se reutilizan las cabinas telefónicas como estaciones de recarga Wi-Fi y en línea.

Medellín, Colombia, elaboró, a través de la Secretaría de Innovación Digital, un Plan Maestro para convertirla en una ciudad inteligente. Este plan incluye la implementación de herramientas tecnológicas para mejorar la calidad de vida, la gobernanza y la sostenibilidad ambiental. *MedeINN*, laboratorio de innovación *GovTech* del Municipio de Medellín, creado en 2021, desempeña un papel clave en este proceso al impulsar

la investigación, el desarrollo y la innovación en el gobierno local. Como resultado, se ha diseñado el Plan de Promoción y Difusión de los Derechos Digitales, que tiene tres objetivos claros: integrar la temática de los derechos digitales en la agenda pública y privada, diseñar herramientas para que los ciudadanos puedan defender sus derechos y capacitar a los funcionarios públicos para que actúen en esta área.¹⁴

Buenos Aires, Argentina —ubicada en el puesto 124 del *Smart City Index 2023*, destacado por el International Institute for Management Development (IMD) y la Organización Mundial de Ciudades Inteligentes y Sostenibles (WeGO)—, se distingue por su enfoque en soluciones sostenibles y tecnológicas; de tal modo, la instalación de paneles solares, cámaras de vigilancia para patentes, la gestión de residuos y los programas de movilidad sostenible, así como el servicio de bicicletas públicas, son ejemplos de sus iniciativas. Como ciudad inteligente, Buenos Aires cuenta con la Subsecretaría de Ciudad Inteligente y Tecnología Educativa, adscrita al Ministerio de Educación e Innovación, que lidera acciones para abordar desafíos urbanos con soluciones innovadoras, priorizando la mejora de la experiencia.¹⁵

En la Ciudad de México, en la Constitución Política de la Ciudad de México,¹⁶ se abordan principios más generales que respaldan la modernización administrativa y la incorporación de tecnologías de la información en la Administración Pública para transformarla en una “Ciudad Inteligente”. Podemos observar

¹⁴ *Medellín: una ciudad inteligente en busca de la transformación cultural*, 11 de noviembre de 2023, en <https://digitalhelpdeskforcities.org/es/medellin-una-ciudad-inteligente-en-busca-de-la-transformacion-cultural/>.

¹⁵ *Buenos Aires se consagra frente a un nuevo paradigma: ciudad inteligente*, en <https://ciudadaniametropolitana.org.ar/2019/09/buenos-aires-se-consagra-frente-a-un-nuevo-paradigma-ciudad-inteligente/>.

¹⁶ Constitución Política de la Ciudad de México, en https://data.consejeria.cdmx.gob.mx/images/leyes/estatutos/CONSTITUCION_POLITICA_DE_LA_CDMX_8.2.pdf.

que se ha avanzado en la ejecución de iniciativas de gobierno digital con el objetivo de mejorar la eficiencia de los servicios gubernamentales, aplicando las tecnologías de la información en el transporte, respetando el derecho a la información y transparencia y protección de datos personales, actualizando los derechos digitales, implementando las infraestructuras de datos abiertos, la modernización administrativa, así como la participación ciudadana y la tecnología para abordar desafíos urbanos y proyectos de gobierno digital que, a menudo, buscan optimizar recursos y reducir el impacto ambiental, los cuales se encuentran en diversos artículos de la Constitución.

Entre las acciones claves podemos mencionar que se han elaborado plataformas digitales¹⁷ que permiten a los ciudadanos realizar trámites y acceder a servicios gubernamentales en línea, como el pago de impuestos, la solicitud de documentos y otros servicios que anteriormente requerían visitas a oficinas gubernamentales; también se ha fomentado la transparencia gubernamental mediante la publicación de datos abiertos para que los ciudadanos accedan a información relevante sobre el funcionamiento del gobierno, presupuestos, proyectos de infraestructura y más; el uso de herramientas digitales para fomentar la participación ciudadana en la toma de decisiones, como las consultas ciudadanas virtuales y plataformas para recopilar comentarios sobre políticas y proyectos.

Igualmente, para mejorar la movilidad urbana, se han incorporado tecnologías inteligentes en el sistema de transporte a través de aplicaciones móviles para el seguimiento de autobuses y la planificación de rutas, así como sistemas de pago electrónico, como las tarjetas de Movilidad Integrada de la Ciudad de México que se utilizan en el Metro, el Metrobús, el Cablebús, el Trolebús y el Tren Ligero.

¹⁷ <https://gobierno.cdmx.gob.mx/acciones/gobierno-digital/>.

En cuanto a la seguridad ciudadana, se han instalado Sistemas Tecnológicos de Videovigilancia de seguridad conectadas a centros de monitoreo, y de análisis de datos para prevenir y abordar incidentes, monitoreados por los operadores del Centro de Control, Comando, Comunicación, Cómputo y Contacto Ciudadano (C5). Actualmente, hay más de 63 mil cámaras distribuidas en toda la Ciudad de México y se cuenta con el programa Mi C911e que se compone de postes de videovigilancias equipados con dos cámaras, un Botón de Auxilio, alerta visual, un altavoz para alertas auditivas y un monitor para la gestión de video y almacenamiento, enlazado directamente con operadores del C2 y C5 que envían una alerta en tiempo real; mediante la cual la persona recibe apoyo inmediato de una unidad policial en caso de emergencias o ser víctima de un delito.

En la capital mexicana se cuenta con Wifi en los lugares públicos. El 28 de febrero de 2023, se publicó en la *Gaceta Oficial de la Ciudad de México* un decreto que reforma el artículo 8, numeral 3 del apartado C de la Constitución Política de la Ciudad de México, que establece que “toda persona tiene derecho a acceder de forma libre y gratuita al servicio de internet de banda ancha en espacios públicos de la Ciudad”, por lo que el acceso a internet en espacios públicos ya es un derecho; así, en 2018 la ciudad contaba con 98 puntos de acceso a internet gratuito en espacios públicos; pero hoy tiene 34,001 puntos Wifi.¹⁸

Otros programas proporcionan dispositivos electrónicos a estudiantes y plataformas en línea para la educación a distancia y soluciones digitales en el sector de la salud, incluyendo la telemedicina y plataformas en línea para la programación de citas y acceso a información de salud.

En los últimos cinco años, la Ciudad de México ha impulsado una revolución tecnológica a través de la Agencia Digital de

¹⁸ Wifi gratuito en la Ciudad de México, <https://internetparatodas.cdmx.gob.mx/puntos-wifi>.

Innovación Pública (ADIP), encargada de diseñar, implementar y supervisar políticas de gestión de datos, gobierno abierto, gobierno digital y gobernanza tecnológica. Este proyecto ha puesto internet y servicios digitales al alcance de todos los sectores de la población, reduciendo la brecha de desigualdad digital. La ADIP ha simplificado y digitalizado trámites para la apertura de negocios, y ha creado “Plaza Pública” para consultas ciudadanas digitales. Además, ha desarrollado el Portal de Datos Abiertos con más de cuatrocientos conjuntos de datos y la app CDMX, que incluye un módulo de movilidad integrada para monitorear el transporte público en tiempo real. También ha establecido Escuelas de Código en los *Puntos de Innovación, Libertad, Arte, Educación y Saberes* (PILARES) y la Línea SOS Mujeres *765 en LOCATEL.

La ciudad cuenta con tres sitios *web* clave: cdmx.gob.mx, un portal de servicios con alrededor de 94 mil visitantes semanales; mexicocity.cdmx.gob.mx, en colaboración con la Secretaría de Turismo, que ofrece información sobre más de 1,600 lugares en la ciudad y ha registrado más de 6.6 millones de visitas; y Cartelera Cultural CDMX, con la Secretaría de Cultura, que recibe más de 53 mil visitas semanales. Además, la Llave CDMX proporciona una bandeja de entrada única para las interacciones digitales de los usuarios, permitiendo el almacenamiento y reutilización de documentos y la consulta en tiempo real de otras dependencias para la validación de trámites y documentos.¹⁹

Como hemos visto, uno de los objetivos de la Administración Pública es satisfacer las necesidades de las personas a través de los servicios públicos, mediante información accesible, comple-

¹⁹ *En los últimos cinco años la Ciudad de México ha vivido una verdadera Revolución Tecnológica a cargo de la ADIP*, 28 de noviembre de 2023, en <https://jefaturadegobierno.cdmx.gob.mx/comunicacion/nota/en-los-ultimos-cinco-anos-la-ciudad-de-mexico-ha-vivido-una-verdadera-revolucion-tecnologica-cargo-de-la-adip-marti-batres>.

ta, disponible y útil, la apertura de datos gubernamentales para que estén disponibles al público en general, fomentando la transparencia, permitiendo a los ciudadanos acceder y utilizar información relevante para garantizar la privacidad de los ciudadanos en el entorno digital. Especialmente en las iniciativas de gobierno digital que involucran el manejo de información personal, el bienestar común puede ser incrementado y, en consecuencia, se fortalece la confianza pública del Estado a través de la legitimidad que ello conlleva.

En la Ciudad de México y en el mundo, la aplicación de un gobierno electrónico y un gobierno digital, es de gran importancia, ya que el uso de la IA nos enseña diferentes usos y modalidades para la gestión, planificación y administración, por medio de portales en Internet con información referente a las dependencias de la Administración Pública, órganos de gobierno, poderes, legislación de los tres niveles de gobierno, así como servicios y trámites para permitir a la sociedad lograr un mayor contacto con la ciudadanía y quienes nos gobiernan, y se enfatizó aún más derivado de la pandemia generada por el covid-19 que sirvió como experiencia para trascender lo hecho hasta ahora y avanzar hacia nuevos paradigmas que expandan los horizontes y alcances del gobierno electrónico y gobierno digital en nuestro país.

México se encuentra en un proceso de avance hacia la adopción de modelos de ciudades inteligentes, la inversión en infraestructura y tecnología es fundamental para el desarrollo, existen avances significativos en ciudades específicas y a nivel nacional, pero persisten retos como la brecha digital, la falta de un marco regulatorio robusto y la necesidad de mayor inversión y capacitación. Por tanto, la colaboración entre diferentes niveles de gobierno, el sector privado, la academia y la sociedad civil es esencial para un desarrollo exitoso de las ciudades inteligentes.

CONCLUSIONES

Las ciudades inteligentes representan una transformación crucial en la gestión urbana mediante la integración de tecnologías avanzadas, como la Inteligencia Artificial, el Internet de las Cosas, el gobierno electrónico y el gobierno digital. Estas tecnologías mejoran la eficiencia de los servicios públicos, promueven la sostenibilidad ambiental y elevan la calidad de vida de los ciudadanos, la implementación de sensores, sistemas de gestión y plataformas digitales permite la optimización de recursos vitales, como el agua, la energía y el transporte- Esto contribuye significativamente a la reducción de emisiones contaminantes, mejora la movilidad urbana y proporciona servicios de salud más eficientes.

La adopción de tecnologías inteligentes en el ámbito urbano plantea importantes consideraciones éticas y de seguridad. Para que las ciudades inteligentes sean exitosas y aceptadas por la sociedad, es fundamental abordar cuestiones relacionadas con la privacidad, la protección de datos y la seguridad cibernética. La inclusión de innovaciones, como la iluminación LED, la monitorización ambiental y las plataformas de gobierno digital no sólo mejoran la eficiencia y la seguridad, sino que fomentan la participación ciudadana y aseguran la accesibilidad para personas con discapacidades.

REFERENCIAS BIBLIOGRÁFICAS

- Bocigas, A., *Smarter Cities, Smarter Future*, Techradar Pro, 24 de octubre de 2022, en <https://www.techradar.com/features/smarter-cities-smarter-future>.
- Business School University of Navarra, *¿Cuáles son las ciudades más “inteligentes” del mundo?*, 9 de abril de 2014, en <https://www.iese.edu/es/insight/articulos/ciudades-mas-inteligentes-mundo/>.
- Cities and Digital Human Rights, *Medellín: una ciudad inteligente en busca de la transformación cultural*, 11 de noviembre de 2023, en <https://digital-helpdeskforcities.org/es/medellin-una-ciudad-inteligente-en-busca-de-la-transformacion-cultural/>.

- Comisión Económica para América Latina y el Caribe, *Tecnologías digitales para un nuevo futuro*, Naciones Unidas. 2021, en <https://repositorio.cepal.org/server/api/core/bitstreams/879779be-c0a0-4e11-8e08-cf80b-41a4fd9/content>.
- Constitución Política de la Ciudad de México, 5 de febrero de 2017, en https://data.consejeria.cdmx.gob.mx/images/leyes/estatutos/CONSTITUCION_POLITICA_DE_LA_cdmx_8.2.pdf.
- Gobierno de la Ciudad de México, *¿Qué quieres hacer hoy?*, s/f, en <https://www.cdmx.gob.mx>.
- Gobierno de la Ciudad de México, *Wifi Gratuito en la Ciudad de México*; s/f, en <https://internetparatodas.cdmx.gob.mx/puntos-wifi>.
- Iberdrola, *"Smart Cities": la revolución tecnológica llega a las ciudades*, s/f, en <https://www.iberdrola.com/innovacion/smart-cities>.
- ICCSI, *Las ciudades inteligentes en emiratos árabes: ejemplos de innovación y sostenibilidad*, s/f, en <https://iccsi.com.ar/ciudad-inteligente-emiratos-arabes/?shared=false>.
- ICCSI, *Seúl: la ciudad inteligente del futuro*, s/f, en <https://iccsi.com.ar/seul-ciudad-inteligente/>.
- Jefatura de Gobierno, *En los últimos cinco años la Ciudad de México ha vivido una verdadera Revolución Tecnológica a cargo de la ADIP: Martí Batres*. 28 de noviembre de 2023, en <https://jefaturadegobierno.cdmx.gob.mx/comunicacion/nota/en-los-ultimos-cinco-anos-la-ciudad-de-mexico-ha-vivido-una-verdadera-revolucion-tecnologica-cargo-de-la-adip-marti-batres>.
- ONU-Habitat *explora el uso de la inteligencia artificial en las ciudades*, 13 de marzo de 2019, en <https://onuhabitat.org.mx/index.php/onu-habitat-explora-el-uso-de-la-inteligencia-artificial-en-las-ciudades>.
- Rozga, L., Ryszard, E., y Hernández, R., *El concepto de Ciudad Inteligente en Europa y América Latina*, en Martínez, S. E., Venegas, M. A. C., Amparo, D., y Ken, C. A. (coords.). *El orden mundial reconfigurando las teorías, las políticas públicas regionales y sus resultados migratorios*, UNAM-AMECIDER, 2022, pp. 115-138, en <http://ru.iiec.unam.mx/5745/>.
- Singh, V., *City of Amsterdam wins first prize at Smart City Awards 2022 for the Hackshield project: Know more here*, Silicon Canals, 18 de noviembre de 2022, en <https://siliconcanals.com/promoted-content/city-of-amsterdam-wins-smart-city-awards/>.
- Tecnologías para los negocios, *¿Blockchain qué es y para qué sirve?*, s.f, en <https://ticnegocios.camaravalencia.com/servicios/tendencias/blockchain-que-es-y-que-ventajas-tiene/>.

- Tkachuk, C., *Buenos Aires se consagra frente a un nuevo paradigma: ciudad inteligente*. Ciudadanía Metropolitana, s/f), en <https://ciudadaniametropolitana.org.ar/2019/09/buenos-aires-se-consagra-frente-a-un-nuevo-paradigma-ciudad-inteligente/>.
- Utopia Urbana City, *Tokio trabaja para convertirse en una ciudad inteligente y sostenible*, 12 de mayo de 2023, en <https://utopiaurbana.city/2023/05/12/tokio-trabaja-para-convertirse-en-una-ciudad-inteligente-y-sostenible/>.
- Zoria, S., *Technological Advancements that Make Singapore a Smart City*. Iotforall. 1 de febrero de 2023, en <https://www.iotforall.com/singapore-smart-city>.

Derechos digitales: asignatura pendiente en México

ONITSED URIEL BUSTAMANTE SILVA¹

INTRODUCCIÓN

La revolución digital ha generado nuevas maneras de participación social, económica y política que permiten la existencia de una red mundial en la que pueden intercambiarse información, ideas, opiniones, y todo aquello relacionado con la vida diaria de las personas.

En México las tecnologías de la información e internet han experimentado una transformación significativa en las últimas décadas, impulsados por el crecimiento de la infraestructura digital. Sin embargo, a pesar de los avances, el país aún enfrenta retos considerables, como la brecha digital, la privacidad, la ciberseguridad, la inteligencia artificial, entre otras.

Por esos motivos, se deben tomar las medidas necesarias para fomentar la independencia de esos nuevos medios y asegurar a las personas el acceso a éstos de una manera libre y segura, por lo que se considera necesario la elaboración de políticas públicas y la emisión de normativa acorde con todo el sistema jurídico mexicano.

Lo anterior nos lleva a plantearnos las siguientes preguntas: ¿se reconoce a las personas derechos digitales en el marco regulatorio mexicano?, ¿se han llevado a cabo acciones por parte del

¹ Licenciado en Derecho por la Facultad de Derecho de la UNAM.

Estado Mexicano dirigidos a proteger los derechos humanos de las personas en el ámbito digital?

Sólo si respondemos estos cuestionamientos podremos tener una luz que nos guíe en el camino para llegar a nuestro destino académico y contestar a la pregunta central de este trabajo: ¿los derechos digitales constituyen una asignatura pendiente en México?

Para abordar estas cuestiones es necesario proveernos de un marco conceptual que nos permita avanzar con alguna seguridad. Así, serán abordados diversos temas, como el derecho humano de acceso a internet y las tecnologías de la información, así como los diversos instrumentos en materia de derechos digitales y el estado regulatorio actual en México en ese tema.

Internet y el uso de las tecnologías de la información y la comunicación como derecho humano

La expansión acelerada de internet y las tecnologías asociadas han traído consigo un universo de oportunidades para el desarrollo económico, social y cultural del país, pues han puesto a nuestra disposición herramientas para acceder a una gran cantidad de información, así como para difundirla fácil y rápidamente, lo que ha permitido hacer frente a diversas problemáticas o llevado a la creación de políticas públicas para una mejor gobernanza.

Si bien en México el panorama de las telecomunicaciones y las tecnologías de la información han experimentado una transformación significativa en las últimas décadas, a pesar de esos avances, también ha supuesto retos importantes a los que el derecho y las instituciones deben hacer frente de manera constante.

Lo anterior, si partimos del hecho que, a nivel constitucional, el derecho humano de acceso a las tecnologías de la información y comunicación se encuentra previsto en el artículo 6º constitucional, el cual establece lo siguiente:

Artículo 6°. La manifestación de ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.

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.

*El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios. [...]*²

Por su parte, la Relatoría Especial para la Libertad de Expresión e Internet de la Comisión Interamericana de Derechos Humanos, señala cuatro criterios orientadores relacionados con el acceso a internet y a las tecnologías de la información, al respecto:

Acceso

[...]

16. *El principio de acceso universal se refiere a la necesidad de garantizar la conectividad y el acceso universal, ubicuo, equitativo, verdaderamente asequible y de calidad adecuada, a la infraestructura de Internet y a los servicios de las TIC, en todo el territorio del Estado*, tal como ha sido reconocido por los jefes de Estado en las Cumbres de las Américas. *Le corresponde al Estado decidir cuáles son los medios más adecuados, bajo las circunstancias, para asegurar la implementación de este principio*. Sin embargo, como se explica adelante, esta oficina otorga este principio. Sin embargo, como se explica adelante, esta oficina otorga particular importancia a aquellas medidas que buscan asegurar que las estructuras de precios sean inclusivas, para no dificultar el acceso; que la conectividad se extienda a todo el territorio, para promover de manera efectiva el acceso de los usuarios rurales y de comunidades marginales; que las comunidades tengan acceso a centros de tecnologías de la información y comunicación comunitarios y

² Constitución Política de los Estados Unidos Mexicanos, artículo 6°, p. 12, en Constitución Política de los Estados Unidos Mexicanos (diputados.gob.mx).

otras opciones de acceso; y que los esfuerzos de capacitación y educación sean reforzados, en especial en sectores pobres, rurales y entre la población mayor. *El acceso universal supone también, de manera prioritaria, asegurar el acceso equitativo en términos de género, así como el acceso incluyente de personas en situación de discapacidad y/o pertenecientes a comunidades marginadas.*

[...]

Pluralismo

[...]

19. *Le corresponde al Estado preservar las condiciones inmejorables que posee Internet para promover y mantener el pluralismo informativo. Esto implica asegurar que no se introduzcan en Internet cambios que tengan como consecuencia la reducción de voces y contenidos. Las políticas públicas sobre la materia deben proteger la naturaleza multidireccional de Internet y promover las plataformas que permitan la búsqueda y difusión de informaciones e ideas de toda índole, sin consideración de fronteras, en los términos del artículo 13 de la Convención Americana.*

[...]

No discriminación

20. [...] Esta obligación de no discriminación se traduce, entre otros, en el *deber del Estado de remover los obstáculos que impidan a los ciudadanos – o a un sector en particular – difundir sus opiniones e informaciones.*

21. *En el entorno digital, la obligación de no discriminación implica, además de los deberes de acceso y pluralismo ya referidos, la adopción de medidas, a través de todos los medios apropiados, para garantizar que todas las personas – especialmente aquellas que pertenecen a grupos vulnerables o que expresan visiones críticas sobre asuntos de interés público – puedan difundir contenidos y opiniones en igualdad de condiciones.* En estos términos, resulta necesario asegurar que no haya un trato discriminatorio a favor de ciertos contenidos en Internet, en detrimento de aquellos difundidos por determinados sectores. Un desarrollo de este principio es el principio de neutralidad de la red...

Privacidad

[...]

23. Tal y como fue observado por la Asamblea General de las Naciones Unidas en la resolución “El derecho a la privacidad en la era digital”, adoptada por consenso, *los Estados tienen la obligación de respetar y proteger el derecho a la privacidad de conformidad con el derecho internacional de los derechos humanos, incluyendo en el contexto de las comunicaciones digitales... las*

autoridades deben, de una parte, abstenerse de hacer intromisiones arbitrarias en la órbita del individuo, su información personal y sus comunicaciones y... deben garantizar que otros actores se abstengan de realizar tales conductas abusivas. Por ejemplo, se debe promover la existencia de espacios en línea libres de observación o documentación de la actividad e identidad de los ciudadanos. Esto incluye, por ejemplo, la preservación de plataformas anónimas para el intercambio de contenidos y el uso de servicios de autenticación proporcionales...

*24. Finalmente, la defensa de la privacidad de las personas debe hacerse atendiendo a criterios razonables y proporcionados que no terminen restringiendo de manera arbitraria el derecho a la libertad de expresión...*³

Como se puede observar, el primer principio consiste en garantizar el acceso a internet y las tecnologías de la información en igualdad de condiciones, es decir, que los Estados cuenten con la infraestructura para acceder a ellas mediante la implementación de acciones o políticas públicas que permitan el desarrollo de la ciberseguridad, hacer frente a la brecha y alfabetización digital, así como la eliminación de cualquier barrera arbitraria para su uso y acceso.

Respecto del pluralismo informativo, se refiere a la implementación de acciones que promuevan y mantengan el mayor número de voces y de contenidos posibles que permitan la búsqueda y difusión de informaciones e ideas de toda índole, como un medio multidireccional e interactivo.

El tercer principio, relacionado con nuestro artículo primero constitucional y el principio de neutralidad de la red, se refiere a la no discriminación, donde se garantice el acceso a las tecnologías de la información en igualdad de condiciones, aplicando

³ Comisión Interamericana de Derechos Humanos. Libertad de Expresión e Internet. Relatoría Especial para la Libertad de Expresión. Resolución OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13 del 31 diciembre de 2013, pp. 7-11, en https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf.

incluso acciones en favor de personas en situación de vulnerabilidad.

Al respecto, en la Declaración Conjunta Sobre Libertad de Expresión e Internet,⁴ se señaló que la neutralidad de la red es un principio según el cual el tratamiento de los datos y el tráfico de internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen y/o destino del material, servicio o aplicación.

Lo que persigue tal principio es que la libertad de acceso y elección de los usuarios de utilizar, enviar, recibir u ofrecer cualquier contenido, aplicación o servicio legal por medio de internet no esté condicionada, direccionada o restringida, por medio de bloqueo, filtración, o interferencia, pues, a través de este principio, se busca facilitar el acceso y la difusión de contenidos, aplicaciones y servicios de manera libre y sin distinción alguna y, al mismo tiempo, derribar barreras de entrada para ofrecer nuevos servicios y aplicaciones incentivando la creatividad, la innovación y la competencia.

Por lo que hace a la privacidad de las personas, contenido en el cuarto principio, contempla la obligación de los Estados de respetar y proteger este derecho, incluyendo el contexto de las comunicaciones digitales, absteniéndose de hacer intromisiones arbitrarias en su información personal y sus comunicaciones, promoviendo la existencia de espacios en línea libres de observación o la documentación de la actividad e identidad de las personas.

⁴ Del Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), OEA:: Relatoría Especial para la Libertad de Expresión (oas.org).

En el mismo sentido, la Constitución Política de la Ciudad de México, en su artículo 8º, apartado C, denominado “Derecho a la ciencia y a la innovación tecnológica” prevé lo siguiente:

Artículo 8

Ciudad educadora y del conocimiento

“[...]”

C. Derecho a la ciencia y a la innovación tecnológica

1. En la Ciudad de México *el acceso al desarrollo científico y tecnológico es un derecho universal y elemento fundamental para el bienestar individual y social*. El Gobierno de la Ciudad garantizará el libre acceso, uso y desarrollo de la tecnología y la innovación, la plena libertad de investigación científica y tecnológica, así como a disfrutar de sus beneficios.

2. *Toda persona tiene derecho al acceso, uso y desarrollo de la ciencia, la tecnología y la innovación, así como a disfrutar de sus beneficios* y desarrollar libremente los procesos científicos de conformidad con la ley.

3. *Las autoridades impulsarán el uso de las tecnologías de la información y la comunicación. Habrá acceso gratuito de manera progresiva a internet en todos los espacios públicos, escuelas públicas, edificios gubernamentales y recintos culturales.*

4. Las autoridades, en el ámbito de sus competencias, fortalecerán y apoyarán la generación, ejecución y difusión de proyectos de investigación científica y tecnológica, así como la vinculación de éstos con los sectores productivos, sociales y de servicios, a fin de resolver problemas y necesidades de la Ciudad, contribuir a su desarrollo económico y social, elevar el bienestar de la población y reducir la desigualdad; la formación de técnicos y profesionales que para el mismo se requieran; la enseñanza de la ciencia y la tecnología desde la enseñanza básica; y el apoyo a creadores e inventores.

Garantizan igualmente la preservación, el rescate y desarrollo de técnicas y prácticas tradicionales y originarias en la medicina y en la protección, restauración y buen uso de los recursos naturales y el cuidado del medio ambiente.

5. El Instituto de Planeación Democrática y Prospectiva elaborará un Programa de Desarrollo Científico, Tecnológico y de Innovación que será parte integral del Plan General de Desarrollo de la Ciudad de México, con una visión de veinte años, y que se actualizará cada tres.

6. *En el presupuesto de la Ciudad de México, se considerará una partida específica para el desarrollo de la ciencia y la tecnología,*

que no podrá ser inferior al dos por ciento del Presupuesto de la Ciudad.

7. Se estimulará el establecimiento de empresas tecnológicas, así como la inversión en ciencia, tecnología e innovación, en los sectores social y privado en la Ciudad de México.⁵

Se observa que, en la Ciudad de México, se contempla de manera expresa el acceso, uso y desarrollo científico y tecnológico como un derecho universal, previendo el acceso gratuito de manera progresiva a internet en todos los espacios públicos, escuelas públicas, edificios gubernamentales y recintos culturales, por lo que las autoridades deberán realizar todas las acciones necesarias para garantizar este derecho.

Sin duda, en el ámbito federal e internacional y local, se reconoce a toda persona el derecho a acceder a las tecnologías de la información y comunicación, incluido el internet, en un sentido de progresividad, pues tal como lo resolvió la Suprema Corte de Justicia de la Nación en el amparo en revisión 1242/2015,⁶ el debido ejercicio de este derecho requiere:

- Calidad del servicio, el cual evolucionará acorde con el avance de las posibilidades tecnológicas.
- Libertad del usuario de elegir el sistema utilizado así como el *software* respectivo.
- Inclusión digital, esto es, la disposición del internet para la ciudadanía en puntos públicos de acceso.
- Neutralidad e igualdad de la red, esto es, la protección y promoción del internet como herramienta para el intercambio libre, abierto, equitativo y no discriminatorio de la información, la comunicación y la cultura, sin privilegios

⁵ Constitución Política de la Ciudad de México, artículo 8º, p. 14, en [CONSTITUCION_POLITICA_DE_LA_CDMX_9.pdf](#)

⁶ Segunda Sala de la Suprema Corte de Justicia de la Nación, Amparo en revisión 1242/2015, 2_188609_3107.doc (live.com).

especiales u obstáculos por razones económicas, sociales, culturales o políticas.

Garantizar este derecho resulta trascendental, ya que su importancia radica en que las plataformas digitales, e incluso ya las inteligencias artificiales que habitan el espacio digital, conviven con nosotros y son partícipes de nuestras actividades diarias. Por lo que hacer accesible y posible este derecho permitirá una mejor interacción y comunicación humana, que elimine cualquier barrera física que nos imponían el tiempo y la distancia.

No obstante, México enfrenta retos considerables en su esfuerzo por acortar la brecha digital y aprovechar el potencial de las tecnologías de la información y la comunicación para el desarrollo del país, pues parecería ser sólo una cuestión de infraestructura; sin embargo, también incluyen diferencias en habilidades digitales y en la capacidad para utilizar efectivamente estas tecnologías, es decir, el problema es más complejo que abarca diferencias económicas, educativas, geográficas y culturales.

Pues, aunque el uso de internet y de dispositivos móviles ha crecido sustancialmente en áreas urbanas, las regiones menos accesibles carecen a menudo de conectividad básica, lo cual dificulta reducir esta disparidad que limita las oportunidades de desarrollo personal, y representa una barrera para la implementación efectiva de políticas públicas, con el fin de asegurar que la población pueda aprovechar plenamente las oportunidades que ofrece el mundo digital.

Otro tema del cual hay que preocuparse, y que se relaciona estrechamente con la protección de las personas, es el de la ciberseguridad, pues a medida que usamos más internet y las tecnologías de la información, la protección de datos personales y la seguridad en línea se convierten en asignaturas primordiales, además de que hay que considerar el alto costo económico a los Estados y empresas cada año.

Por lo que a través de la ciberseguridad podemos proteger equipos, redes, aplicaciones de *software*, sistemas críticos y datos

personales de posibles amenazas digitales. No obstante, debemos tener presente que los ciberataques evolucionan a la par que las tecnologías. Los ciberdelincuentes utilizan nuevas herramientas y elaboran nuevas estrategias para vulnerar la red.

Para combatirlo es indispensable el fortalecimiento de la legislación y las políticas públicas en este ámbito, como la adopción en nuestro sistema jurídico del Convenio sobre la Ciberdelincuencia, conocido como Convenio de Budapest, el cual fue elaborado en 2001 por el Consejo de Europa, con el fin de hacer frente a la comisión de delitos informáticos.

Este instrumento prevé para los Estados Parte la incorporación a su ordenamiento jurídico nacional de la legislación para investigar y perseguir penalmente los delitos en contra de sistemas o medios informáticos o mediante el uso de éstos y faciliten la cooperación internacional en la materia.

A pesar de haber sido invitado, a la fecha México se encuentra sólo como observador.

De igual modo, es responsabilidad de todas y todos. Un uso correcto de las plataformas digitales y las tecnologías de la información, así como navegar con éxito en internet, yace en nuestra capacidad para adoptar un enfoque equilibrado, donde reconocamos los riesgos y las recompensas de estas herramientas. De ahí que resulte importante entre el gobierno, el sector privado y la sociedad civil colaborar para desarrollar una estrategia nacional inclusiva y efectiva en el reconocimiento del derecho humano de acceso a las tecnologías y el internet, mediante la debida protección contra amenazas digitales.

Lo anterior, porque debemos ver al desarrollo tecnológico como un complemento de nuestras vidas; por ejemplo, por medio de la inteligencia artificial, podemos ampliar nuestro conocimiento, agilizando nuestras actividades cotidianas mediante la automatización de tareas y funciones, sin perder esa naturaleza humana y creativa.

Derechos digitales de las personas

La era en la que vivimos presenta grandes oportunidades. Ello es así porque el desarrollo de las tecnologías de la información, junto a la expansión de internet, y la creación de espacios y plataformas digitales ha permeado cada faceta de nuestra existencia, desde cómo interactuamos con otras personas, hasta cómo concebimos el entorno que nos rodea, lo cual, como fue abordado, constituye un derecho humano.

No obstante, herramientas, como la inteligencia artificial, el Internet de las Cosas, la realidad aumentada y otras tantas tecnologías, plantean desafíos adicionales en la protección de los derechos fundamentales de las personas. De esta manera, surge en el universo jurídico un concepto que intenta hacer frente a la falta de regulación del mundo digital: los derechos digitales.

En su afán de querer regular las actividades que se desarrollan en internet y las tecnologías de la información, algunos países y convenciones internacionales han planteado y definido a los derechos digitales, entendiéndolos como una extensión de los derechos humanos en el mundo digital, cuyo objetivo principal es garantizar el acceso a internet y reducir la brecha en este ámbito, promoviendo un uso correcto de la red como un bien común de toda la humanidad.

De esta manera, la Organización de las Naciones Unidas y la Comisión Interamericana de Derechos Humanos han establecido que los mismos derechos que tienen las personas en el mundo *offline* deben protegerse en el mundo en línea.

Pues la *Relatoría Especial para la Libertad de Expresión. Estándares para una Internet Libre, Abierta e Incluyente* y la resolución de la Asamblea General de las Naciones Unidas A/HRC/38/L.10, reconocieron y reafirmaron respectivamente la importancia de proteger y garantizar el ejercicio de los derechos humanos en línea, al exhortar a los Estados miembros a fomentar la seguridad y la confianza en internet, en particular derechos como la libertad de

opinión y de expresión, así como a la privacidad, con el objetivo de facilitar el desarrollo y la innovación en sus territorios.

Con base en lo anterior, si bien actualmente no existe un estándar de estos derechos —puesto que cada país o región ha creado su propio documento—, lo cierto es que constituyen importantes avances, lo cual permite que las personas naveguen con confianza y de forma segura en internet, por lo que a continuación se analizan algunos instrumentos sobre el tema.

*Carta de derechos digitales de España*⁷

Aprobada y publicada en 2021, fue elaborada por un Comité de expertos y sometida a dos procesos de consulta pública, la cual señala que no trata de crear nuevos derechos fundamentales sino de perfilar los más relevantes en el entorno y los espacios digitales, es decir, no trata de descubrir derechos digitales pretendiendo que sean distintos de los derechos fundamentales ya reconocidos o que las tecnologías y el ecosistema digital se erijan por definición en fuente de nuevos derechos.

Se resalta que este instrumento constituye una declaración, por lo que no es vinculante ni obligatoria, pues señala que no tiene carácter normativo, sino que su objetivo es reconocer los retos de aplicación e interpretación que la adaptación de los derechos al entorno digital plantea, así como sugerir principios y políticas referidas a ellos en ese contexto.

Se trata de un marco de referencia para que las personas sepan y conozcan cuáles son los derechos digitales y por tanto puedan respetarlos, defenderlos y como ejercerlos, al igual que busca impulsar el desarrollo de nuevas leyes en la materia.

Está estructurada en seis categorías principales, que agrupan los 28 derechos digitales de la siguiente manera:

⁷ Carta de Derechos digitales de España, en https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf.

Derechos de Libertad

Establece la identidad digital y el derecho a protegerla, la cual estará determinada por el nombre y por los demás elementos que la configuran, por lo que no podrá ser controlada, manipulada o suplantada por terceros contra la voluntad de la persona, con la finalidad de evitar manipulaciones, suplantaciones, o su control, lo cual es trascendente en nuestros días, pues con ello se pueden evitar las prácticas de *Deep fakes*. También reconoce el derecho a la protección de datos, lo anterior conforme al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, y la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

En esta categoría también se prevén los derechos digitales al pseudoanonimato, a la persona a no ser localizada y perfilada, a la ciberseguridad y a la herencia digital.

Derechos de igualdad

Este grupo de derechos digitales están dirigidos al reconocimiento de la igualdad y la no discriminación, en el entorno digital y en el acceso a internet, combatiendo la exclusión y las brechas digitales en todas sus manifestaciones, incluyendo las de género, económicas, de edad y de discapacidad. Asimismo, se prevé la protección de las personas menores de edad en el entorno digital.

El grupo de derechos digitales de esta categoría son a la igualdad y a la no discriminación en el entorno digital, acceso a internet, protección de las personas menores de edad en el entorno digital, accesibilidad universal en el entorno digital y brechas de acceso al entorno digital.

Derechos de participación y de conformación del espacio público

Aquí se reconoce el derecho de neutralidad e igualdad de la red, el cual ya fue mencionado; también esta categoría busca combatir la desinformación y las *fake news*, así como concientizar

sobre como internet y las redes sociales facilitan la difusión de estos contenidos. Se establecen los derechos digitales de libertad de expresión e información, a recibir información veraz, participación ciudadana, y necesidad de educar a las personas para un uso responsable de los medios digitales.

Derechos del entorno laboral y empresarial

Son derechos digitales relacionados con derechos laborales, dirigidos a reconocer el tiempo de descanso de las personas trabajadoras, su intimidad personal y familiar, limitar y regular el control del empresario, para que sus derechos y los de los trabajadores no choquen, etcétera.

Derechos digitales en entornos específicos

En este apartado se abordan los relacionados con la salud, el interés público, investigación científica o histórica, desarrollo tecnológico y la cultura. También reconoce dos derechos que en los últimos años han sido trascendentes en la vida cotidiana de las personas: el uso de la inteligencia artificial estableciendo la no discriminación, transparencia, auditabilidad, explicabilidad, trazabilidad, supervisión humana y gobernanza; así como el empleo de las neurotecnologías, específicamente en la confidencialidad, autodeterminación individual, seguridad de los datos obtenidos o relativos a sus procesos cerebrales y su pleno dominio y disposición.

Garantía y eficacia

En este apartado se prevé la creación de mecanismos de autorregulación y control propio en los entornos digitales, así como la creación de procedimientos para la resolución alternativa de los conflictos que puedan surgir en el espacio digital.

***Carta Iberoamericana de Principios y Derechos en Entornos Digitales*⁸**

Aprobada durante la XXVIII Cumbre Iberoamericana de Jefes de Estado y de Gobierno, celebrada el 25 de marzo de 2023, tiene carácter declarativo y no vinculante. Al momento, se han adherido 22 países, incluyendo España, México, Portugal, Andorra y Brasil.

Tiene por objeto promover principios comunes para que sean tomados en cuenta por los Estados al momento de adoptar o adecuar las legislaciones nacionales o poner en marcha políticas públicas relacionadas con la protección de los derechos y el cumplimiento de los deberes en entornos digitales.

La Carta también resalta la importancia de desarrollar sociedades en las que se respeten digitalmente los derechos humanos, tomando en consideración los diversos obstáculos, como infraestructura, educación, inversión o desigualdad entre países.

⁸ *Carta Iberoamericana de Principios y Derechos en los Entornos Digitales*, en

Especifica que será revisada y actualizada para adecuarla a las nuevas realidades.

Está conformado por diez apartados, resaltando la importancia de la privacidad y ciberseguridad, educación y formación tecnológica en los grupos más desfavorecidos.

Centralidad de la persona. Derechos y deberes en entornos digitales

Plantea que, ante la incidencia de la tecnología y herramientas digitales en todos los ámbitos de la sociedad y vida de las personas, sus derechos deben ser garantizados, respetados y protegidos en estos entornos; asimismo señala que la falta de medios, habilidades o competencias digitales no debe suponer una discriminación o exclusión para quienes no pueden o no están en disposición de integrarse en el proceso de transformación de la tecnología.

Inclusión digital y conectividad

Se reconocen derechos en favor de grupos vulnerables a fin de combatir la brecha digital, exclusiones o desigualdades, mediante políticas públicas que reconozcan y mitiguen estas conductas y ninguna persona quede fuera del proceso de transformación digital.

Establece que la transformación digital debe contribuir a crear entornos digitales inclusivos, abiertos y centrados en el ser humano, a que se reduzcan las brechas y no se creen nuevas, tomando especialmente en cuenta a las personas en situación de vulnerabilidad.

Privacidad, confianza, seguridad de datos y ciberseguridad

Resalta que se deben hacer esfuerzos relevantes para garantizar que la privacidad de las personas y el procesamiento de sus datos personales estén protegidos en entornos digitales seguros y confiables centrados en las personas, respetando las legislaciones nacionales en la materia. Por lo que los sistemas digitales de información utilizados con fines personales, profesionales o sociales deben poseer, desde su diseño y por defecto, las medidas de segu-

ridad adecuadas que permitan garantizar la integridad, confidencialidad, disponibilidad, resiliencia y autenticidad de la información procesada y la disponibilidad de los servicios prestados.

Igualmente establece la importancia de desarrollar un marco legal, políticas y acciones educativas que apunten a convertir la ciberseguridad y la lucha contra el cibercrimen y la violencia digital, orientado a garantizar los derechos de las personas y a fortalecer la seguridad de los países.

Acceso pleno a la educación, la cultura y la salud en entornos digitales inclusivos y seguros

Aduce que las tecnologías de la información constituyen herramientas con la capacidad de impulsar el desarrollo social y cultural, el acceso pleno a la educación, la cultura y la salud, por lo que se requiere el desarrollo de capacidades y la formación de nuevas competencias en las personas, así como garantías en la regulación para hacerlo efectivo.

Promueve la creación de planes e iniciativas de política en materia de educación y formación sobre el uso y apropiación de las tecnologías digitales, que prevean la adaptación curricular, la ciberseguridad, el uso de recursos digitales, la conectividad y la capacitación de educadores para la adaptación de los procesos de enseñanza-aprendizaje en la Era Digital.

Especial atención a niñas, niños y adolescentes

Al ser un sector de la población sujeto a una especial exposición y vulnerabilidad en los entornos digitales, la protección a la niñez y adolescencia requiere de políticas específicas que permitan un uso amplio y seguro de las tecnologías de la información.

Mediante políticas públicas que tengan por objeto resguardar el interés superior de la niñez, la integridad, la privacidad y la salud física y psíquica de niñas, niños y adolescentes en los entornos digitales, mediante medidas para identificar, denunciar y combatir el ciberacoso, así como las acciones nocivas, abusivas y delictivas a las que se encuentran expuestas y expuestos.

Participación social, económica y política en entornos digitales justos y sostenibles

Reconoce que los espacios digitales pueden convertirse en instrumento de desinformación y alteración del orden constitucional, que puede afectar la convivencia pacífica, la estabilidad política y seguridad de los países e incitar a la violencia, el odio y la discriminación.

Razón por la cual promueve el derecho a recibir libremente información veraz, buscando desarrollar acciones para combatir la desinformación y promover la libre elección de servicios y contenidos digitales, considerando que el acceso oportuno y la incorporación de la transparencia, como una dimensión transversal de las políticas públicas, posibilitan la participación pública efectiva y el ejercicio de todos los derechos humanos por todas las personas.

Resalta la importancia de consolidar la libertad de expresión y el derecho a informar y ser informado en los nuevos medios en el marco de las leyes nacionales vigentes, a fin de consolidar la protección de los derechos humanos y los valores democráticos. Por lo que el ejercicio de este derecho entraña deberes especiales y las restricciones deben estar expresamente fijadas por la ley o las constituciones de los Estados.

Administración pública digital

Señala la importancia de la simplificación y digitalización de los procesos y trámites administrativos, tanto en relación con las personas usuarias de los servicios públicos —pues eficientiza las administraciones públicas y facilita el ejercicio de derechos y cumplimiento de deberes—, además de que fortalece a la ciudadanía y refuerza su confianza en las instituciones, como en la reducción de los procesos burocráticos.

Economía digital justa, inclusiva, y segura

Menciona que la transformación digital trae aparejada una reconfiguración de la economía, por lo que deben adecuarse los instrumentos, políticas y acciones para asegurar la protección

social, el acceso al trabajo, la salud y la participación de los trabajadores sin discriminación de tipo alguno, teniendo en cuenta a los grupos vulnerables y las particularidades de los entornos digitales, sin reproducir o aumentar brechas existentes como las de género, socioeconómica, etaria y territorial, entre otras, ni crear nuevas.

Un abordaje de tecnologías emergentes que no renuncie a la centralidad de las personas

Reconoce que se deben garantizar los derechos de las personas ante la innovación tecnológica y los nuevos desarrollos tecnológicos y científicos, como la Inteligencia Artificial, neurotecnologías o computación cuántica, tomando en consideración sus ventajas y riesgos.

Asistencia y cooperación iberoamericana para la transformación digital

Resalta la consolidación de la cooperación iberoamericana como mecanismo para contribuir al desarrollo sostenible de la región desde el diálogo político y la articulación intergubernamental y multiactoral, según los roles y responsabilidades que correspondan, con la participación voluntaria de los países en correspondencia con sus prioridades nacionales, así como la realización conjunta de acciones de solidaridad para el desarrollo socioeconómico y sostenible.

***Carta de derechos de la persona en el entorno digital. Código de buenas prácticas del Sistema Nacional de Transparencia (SNT)*⁹**

Para su elaboración se llevaron a cabo diversas mesas de trabajo, en las que participaron integrantes del Sistema Nacional de Transparencia (SNT), asociaciones civiles, académicos, empresas y especialistas en los temas que contiene. Tiene por objetivo robustecer el reconocimiento de los derechos en el mundo digital

⁹ *Carta de derechos de la persona en el entorno digital. Código de buenas prácticas del SNT*, <https://snt.org.mx/wp-content/uploads/CONAIP-SNT-ACUERDO-ORD02-09-10-2023-04-ACLARATORIA.pdf>.

y ser un impulso para la creación de políticas públicas y leyes cuya finalidad sea lograr su plena protección.

Al ser un código de buenas prácticas, no crea u otorga derechos subjetivos, ni establece obligaciones para los entes públicos o privados, es decir, no es vinculante u obligatoria, y sólo orienta o describe los derechos que se consideran óptimos para que la persona usuaria desarrolle de manera integral su personalidad y ejerza, plenamente, los derechos que le reconoce el orden jurídico mexicano, y las obligaciones y deberes que tendrían que asumir el Estado y las instituciones privadas para garantizar estos derechos.

En este documento se aborda con un lenguaje claro y cercano a la ciudadanía, los derechos que puede exigir como usuaria de las tecnologías de la información y las comunicaciones, ante qué instancias acudir si consideran violentados estos derechos, y de qué manera mantener la titularidad y entera disponibilidad de sus datos personales.

Capítulo I. Igualdad digital

Se desarrollan diversas temáticas como Acceso universal a internet, No discriminación, Educación digital y Derecho a la neutralidad de internet.

Capítulo II. Libertades en el entorno digital

Las temáticas que aquí se abordan son: Derecho a la identidad, derecho a la presudonimidad, derecho de la persona a no ser localizada y perfilada, libertad de expresión y acceso a la información, derecho a la propiedad intelectual en el entorno digital, derecho a la herencia digital, derecho al ocio en el ciberespacio y derecho al uso de redes sociales.

Capítulo III. Derecho a la seguridad y protección de datos personales

Los temas aquí señalados son: Derecho a la privacidad y a la protección de datos personales, Derecho a la Transmisión, recepción y tratamiento seguro de la información, derecho a la portabilidad, derecho a la ciberseguridad, derecho a la imagen digital y derecho a la identidad.

Capítulo IV. Derechos a la participación, a la democracia y al buen gobierno digital

Entre los temas que se desarrollan están: Derecho a la participación ciudadana por medios digitales, Derechos digitales frente a la Administración Pública, Derecho de reunión, asociación y participación.

Capítulo V. Derechos laborales

Se tocan temáticas como: Teletrabajo, Derecho a la desconexión digital, Derecho a la privacidad en el uso de cámaras de videovigilancia al interior de los lugares de trabajo y al desechamiento de datos digitales almacenados.

Capítulo VI. Derechos de las personas en situación de vulnerabilidad

Los temas que se abordan son: Personas con discapacidad, Niñas, niños y adolescentes, Personas adultas mayores, Personas pertenecientes a pueblos originarios y Mujeres.

Capítulo VII. Neuroderechos

Se manejan las siguientes temáticas: Derecho a la preservación de la identidad personal, Derecho a la privacidad de datos neuronales, Derecho al libre albedrío, Derecho a la equidad en el mejoramiento de la capacidad cerebral, Derecho de protección contra el sesgo y de discriminación.

Capítulo VIII. Ética en el uso de la inteligencia artificial (IA)

Contempla el derecho al uso de la inteligencia artificial centrada en la persona, a la privacidad y la protección de datos personales en el uso de la IA, así como Transparencia y acceso a la información en el uso de la IA, y el derecho a la seguridad en el uso de la IA.

Capítulo IX. Medios de defensa y derechos de las víctimas en el entorno digital

Los temas abordados en este capítulo son: Recurso efectivo, el derecho a la asistencia, protección, atención, verdad, justicia, reparación integral y debida diligencia.

Regulación en México

Una nueva realidad se impone en nuestras relaciones sociales, donde internet y las tecnologías de la información se han convertido en herramientas importantes que ayudan al desarrollo de las personas y Estados, así como a la evolución de los derechos humanos, porque proporcionan nuevos medios e instrumentos para ejercerlos y amplían su contenido. Sin embargo, también representan una amenaza, pues las desigualdades, delitos y esquemas de discriminación imperan de manera cotidiana en el espacio digital con sus propias particularidades.

Por lo anterior, resulta importante regular y emitir acuerdos nacionales e internacionales que permitan, por un lado, acceder y navegar de manera segura al internet y demás herramientas tecnológicas, pero que, al mismo tiempo, implique proteger los derechos humanos de las personas de manera progresista y sin discriminación alguna.

Esta nueva realidad demanda anticiparnos y actuar de manera rápida, como se mencionó, los derechos humanos deben respetarse tanto en línea como fuera de internet, ya que, ante las diversas amenazas se debe buscar tutelar derechos que garanticen la vida y dignidad de las personas. Como ejemplo de ello tenemos la protección de los datos personales y la privacidad, la identidad digital, la libertad de expresión, el uso de tecnologías de vigilancia, la ciberseguridad para hacer frente a la violencia y el acoso en línea, entre otros.

Si bien algunos instrumentos intentan reconocer los derechos digitales de las personas, como los analizados, ninguno tiene el carácter de vinculante, pues no crea u otorga derechos subjetivos, ni establece obligaciones para los entes públicos o privados, ya que sólo tienen naturaleza orientadora y descriptiva.

Por otro lado, resulta necesario resaltar que el 4 de agosto de 2021 en la *Gaceta Oficial de la Ciudad de México*, se publicó la reforma de diversas disposiciones del Código Civil para el Distrito Federal y de la Ley de Notariado para la Ciudad de

México, donde de manera expresa reconoce bienes y derechos digitales.

Al respecto, el artículo 1392 bis del Código Civil para el Distrito Federal establece lo siguiente:

ARTÍCULO 1392 Bis. *El legado también puede consistir en la titularidad sobre bienes o derechos digitales almacenados en algún equipo de cómputo, servidor, plataforma de resguardo digital, dispositivo electrónico, redes sociales o dispositivos físicos utilizados para acceder a un recurso restringido electrónicamente, los cuales pueden consistir en:*

I. Cuentas de correo electrónico, sitios, dominios y direcciones electrónicas de internet, archivos electrónicos tales como imágenes, fotografías, videos, textos; y

II. Claves y contraseñas de cuentas bancarias o de valores, aplicaciones de empresas de tecnología financiera de los que el testador sea titular o usuario y para cuyo acceso se requiera de un nombre o clave de usuario, clave y contraseña.

Los bienes o derechos digitales serán independientes de su valor económico y contenido determinable.

Los datos necesarios para el acceso a los bienes o derechos digitales podrán ser resguardados por el mismo notario en el apéndice del instrumento correspondiente al testamento o en el caso de la actuación digital notarial a que se refiere la Ley del Notariado para la Ciudad de México, en un sistema de almacenamiento permanente.

El testador podrá nombrar a un ejecutor especial que, constatado que se trató del último testamento otorgado y su validez fue reconocida, estará facultado para que se le proporcione la información correspondiente a los accesos de los bienes o derechos digitales y proceda según las indicaciones del testador.

La gestión de la información a que se refiere el primer párrafo de este artículo no implicará que el ejecutor especial sea titular de dichos bienes o derechos digitales o que pueda disponer de ellos, salvo disposición del testador.

Si el testador no dispuso sobre el tratamiento de su información personal almacenada en registros electrónicos públicos y privados, incluyendo imágenes, audio, video, redes sociales y cualquier método de búsqueda de internet o, en su caso, ordenó su eliminación, una vez que se tenga certeza de que se trata del último testamento y se haya declarado la validez del mismo, el

albacea o el ejecutor especial procederá de inmediato a solicitar su eliminación a las instituciones públicas y/o privadas que conserven dicha información a fin de salvaguardar el derecho al olvido a favor del autor de la sucesión, salvo disposición expresa de éste.¹⁰

Como se puede observar, la normativa civil de la capital del país reconoce la herencia digital para disponer de los bienes y derechos que se hayan adquirido en vida en el espacio digital, lo cual representa un avance sobre el tema, ya que significan normas de carácter vinculante y, por tanto, obligatorias, para las personas y autoridades.

Lo anterior representa un ejemplo de progresividad en los derechos humanos frente a las nuevas tecnologías, pues se adaptó el sistema jurídico para proteger los valores constitucionales y la seguridad jurídica de las personas para hacer frente a las nuevas realidades, lo cual no es menor, pues sirve de antecedente para inspirar la incorporación de otros derechos digitales en la legislación nacional para responder a los retos del ecosistema digital.

Ello dentro del marco constitucional y legal de nuestro país, ya que, como advertimos, el último párrafo de la disposición señalada, que también regula el derecho al olvido de las personas fallecidas, fue declarada inconstitucional por la Suprema Corte de Justicia de la Nación en el amparo en revisión 341/2022¹¹ con los siguientes argumentos:

- La porción normativa respecto de la cancelación de datos personales de personas fallecidas es contraria a la libertad de expresión y al derecho al libre acceso a la información.

¹⁰ Código Civil para el Distrito Federal, artículo 1392 bis, pp. 168-169, en CODIGO_CIVIL_PARA_EL_DF_11.pdf (cdmx.gob.mx).

¹¹ Pleno de la Suprema Corte de Justicia de la Nación, amparo en revisión 341/2022, en Microsoft Word-AR-341-2022-Engrose (scjn.gob.mx).

- Resaltó que, debido a la amplitud del concepto constitucional de datos personales, el cual no está limitado a la información de alguna naturaleza (información u opiniones), ni al formato o medio en el que se contenga, ni a su carácter privado o íntimo, tampoco si es generada por el titular o tercero, pueden llegar suscitarse conflictos entre la libertad de expresión y este derecho.
- Por lo anterior, determinó que las relaciones entre este derecho y libertad fundamentales deben partir de que la Constitución prohíbe cualquier acto de censura previa respecto de dicha libertad; únicamente es posible la asignación de responsabilidades posteriores a partir de la valoración de varios factores como el interés público, la notoriedad o proyección pública de la persona y conducta previa, contenido y forma de la publicación y la intención de la publicación y diseminación.
- Por lo que resolvió que la porción normativa reclamada resulta contraria a la libertad de expresión y al derecho a la información. Esto, tras advertir que su redacción es ambigua y general, pues no se distingue entre información que no ha sido objeto de una publicación respecto de aquella que sí lo ha sido.
- Además, no se prevé condición alguna para determinar la procedencia de la cancelación de los datos cuando se encuentren involucrados derechos de terceros.
- Finalmente, en relación con el supuesto “derecho al olvido” destacó que no existe definición legal en nuestro país sobre lo que implica esta expresión, aunado a que no es posible deducir un contenido específico de la interpretación literal de sus términos, límites y alcances.
- Asimismo, no puede ser aplicado sin calificaciones en México debido a que la Constitución Federal establece la presunción de que toda información pública debe permanecer con dicho carácter, sin que el mero paso del tiempo pueda

ser determinante en la pérdida del interés público de la información.

Por otro lado, cabe resaltar que, a partir del 9 de noviembre de 2023, quedó instalada la Comisión de Derechos Digitales en el Senado de la República, la cual estará encargada de analizar asuntos sobre la regulación del uso, aprovechamiento e implementación de las herramientas y plataformas tecnológicas, además de que abordará cuestiones relacionadas con la privacidad, ciberseguridad, la libertad de expresión y el acceso a la información.

Hasta el momento, a la Comisión se han remitido trece iniciativas relacionadas al acceso a internet libre de violencia contra niñas, niños y adolescentes; para prevenir el ciberacoso; facultar al Congreso de la Unión para dictar leyes sobre inteligencia artificial y sus aplicaciones, ciberseguridad y neuroderechos.

Si bien México enfrenta desafíos significativos en su camino hacia la inclusión digital y el aprovechamiento de las tecnologías de la información, a través de esfuerzos concertados y políticas innovadoras, el país puede superar los obstáculos y abrir nuevas oportunidades que aseguren a las personas el pleno goce de sus derechos humanos en la realidad virtual y física, las cuales están interconectadas, pues no se tratan de dos mundos distintos sino de uno solo donde coexisten las personas.

México puede y debe avanzar hacia este futuro digital inclusivo y próspero, pues si bien, la asignatura aún no está completa, ya se dieron pasos significativos para reconocer los derechos de las personas en el espacio digital, que permita a cada persona acceder y utilizar las tecnologías de la información de una forma segura.

REFERENCIAS

Normativa y criterios nacionales

Constitución Política de los Estados Unidos Mexicanos, Constitución Política de los Estados Unidos Mexicanos (diputados.gob.mx).

Constitución Política de la Ciudad de México, CONSTITUCION_POLITICA_DE_LA_cdmx_9.pdf.

Código Civil para el Distrito Federal, artículo 1392 Bis, CODIGO_CIVIL_PARA_EL_DF_11.pdf (cdmx.gob.mx).

4. Segunda Sala de la Suprema Corte de Justicia de la Nación, Amparo en revisión 1242/2015, 2_188609_3107.doc (live.com).

Criterios Internacionales

Comisión Interamericana de Derechos Humanos. Libertad de Expresión e Internet. Relatoría Especial para la Libertad de Expresión. Resolución OEA/Ser.L/V/II. CIDH/RELE/INF. 11/13 del 31 diciembre 2013, en https://www.oas.org/es/cidh/expresion/docs/informes/2014_04_08_internet_web.pdf.

Declaración conjunta sobre libertad de expresión e Internet del Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión, la Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), la Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión y la Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP), en https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2_

Relatoría Especial para la Libertad de Expresión. Estándares para una Internet Libre, Abierta e Incluyente, Resolución OEA/Ser.L/V/II CIDH/RELE/INF.17/17 del 15 de marzo de 2017, en https://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf.

Resolución de la Asamblea General de las Naciones Unidas “A/HRC/38/L.10”, en https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf.

Cartas de derechos digitales

Carta de Derechos digitales de España, en https://www.lamoncloa.gob.es/presidente/actividades/Documents/2021/140721-Carta_Derechos_Digitales_RedEs.pdf.

Carta de derechos de la persona en el entorno digital. Código de buenas prácticas del Sistema Nacional de Transparencia (SNT), en <https://>

snt.org.mx/wp-content/uploads/CONAIP-snt-ACUERDO-ORD02-09-10-2023-04-ACLARATORIA.pdf.

Carta Iberoamericana de Principios y Derechos en los Entornos Digitales, en [### *Informes*](https://oei.int/downloads/disk/eyJfcmlFpbHMiOnsibWVzc2FnZSI6IkJBaDdDRG9JYTJWNVNTSWWhOV0kwYUc5eGJtZGxhelEzWWpKM2Jta-3pZWE0yY0hRNE1tWnlOQVk2QmtWVU9oQmthWE53YjNOcGR-HbHZia2tpQWNKcGJteHBibVU3SUdacGJHVnVZVzFsUFNKR-FlYSjBZUzFKWW1WeWIyRnRaWEpwWTJGdVlTMWtaUzFRY21sd-VkybHdhVzl6TFhrdFJHVnlaV05vYjNNdFpXNHRIrZl6TFVWdWR-HOXlibTl6TFVScFoybDBZV3hsYzE5RmN5NXdaR1lpT3lCbWFXe-GxibUZ0WlNvOVZWUkdMVGduSjBOaGNuUmhMVWxpWlhKd-llXMWxjbWxqWVclalExXUmxMVkj5YVclamFYQnBiM010ZVMxRVpYS-mxZMmh2Y3kxbGJpMXNiM010Ulc1MGIzSnViM010UkdsbmFYUmhiR-1Z6WDBWekxuQmtaZ1k3QmxRNkVXTnZibJlsYm5SZmRlbHdaVWtpRkd-Gd2NHeHBZMkYwYVc5dUwzQmtaZ1k3QmxRPSIsImV4cCI6IjIwMjQtMDUtMTZUMTg6NDA6MzQuMTgwWiIsInB1ciI6ImJsb2Jfa2V5In19-b0144702ca403965d5115de20832d0d5d82b075f/Carta-Iberoamericana-de-Principios-y-Derechos-en-los-Entornos-Digitales_Es.pdf?content_type=application%2Fpdf&disposition=inline%3B+filename%3D%22Car-ta-Iberoamericana-de-Principios-y-Derechos-en-los-Entornos-Digitales_Es.pdf%22%3B+filename%2A%3DUTF-8%27%27Carta-Iberoamericana-de-Principios-y-Derechos-en-los-Entornos-Digitales_Es.pdf.</p>
</div>
<div data-bbox=)

Informe de Actividades de la LXV Legislatura del Senado. Noviembre 2023-abril 2024, en http://sil.gobernacion.gob.mx/Archivos/Documentos/2024/05/asun_4756563_20240508_1715204205.pdf.

Inteligencia artificial y responsabilidad algorítmica. Apuntes para entender el nuevo sentido del Derecho

JOSÉ LUIS HERNÁNDEZ SÁNCHEZ¹

INTRODUCCIÓN

Hace casi 25 años, Manuel Atienza escribió su libro *El sentido del Derecho*.² La idea de fondo —dice el autor— era entender que el Derecho tiene un sentido y éste no puede ser otra cosa más que la aspiración a la justicia. Para lograrlo, dice Atienza, debemos contestar algunas preguntas clave que dan vida a la filosofía del Derecho, entre ellas:

...por qué, y desde cuándo, existe el Derecho, en qué medida consiste en normas, qué relación guarda con la moral y con el poder, para qué sirve, qué funciones sociales cumple, cómo debería ser, qué objetivos y valores deben -y pueden- alcanzarse con él, cómo puede conocerse y de qué manera ha de construirse una ciencia jurídica, hasta qué punto consiste en una actividad argumentativa, cómo ha de entenderse su aplicación e interpretación... si el sentido del Derecho (o cierto tipo de Derecho) integra una práctica social valiosa, constituye un tipo de realidad que quizás sólo puede llegar a entenderse plenamente si se asume un determinado punto de vista, y una realidad que no está ahí simplemente para ser conocida, criticada o utilizada estratégicamente, sino para ser

¹ Doctor en Derecho por la Universidad Panamericana. Fundador de The White Box Project Institute, primer centro de formación especializado en supervisores de inteligencia artificial para América Latina (*Chief Artificial Intelligence Officer*, LATAM).

² Manuel Atienza, *El sentido del Derecho*, Ariel, Madrid, 2001.

mejorada por los sujetos que forman parte de la misma... éstas son las grandes preguntas de la filosofía del Derecho.³

Estas preguntas y el contenido del libro fueron pensados sin tener contacto con la nueva inteligencia artificial avanzada y los sistemas inteligentes, los cuales, a partir de 2024, cobran realce por sus nuevas habilidades multimodales que les permiten hacer prácticamente cualquier cosa relacionada con la creación de contenidos, dejando atrás a la inteligencia artificial tradicional que sólo “comprendía contenidos”. Si bien aún no hemos llegado al nivel de una IA General, no se descarta que la IA generativa sea el camino para alcanzarla. Hoy estos modelos pueden

- Conversar con lenguaje natural vía texto y vía voz.
- Interpretar, analizar y generar soluciones a problemas complejos.
- Generar códigos.
- Crear imágenes, logotipos, videos, historietas, fotografías, entre otros.

Atienza también tiene una aportación interesante respecto del uso de la inteligencia artificial y la “dignidad humana”. Este término, fruto principalmente de las aportaciones kantianas, es estudiado por el filósofo de la Universidad de Alicante con el fin de redescubrir su evolución histórica y usos presentes. Atienza lo ubica tanto en la filosofía como en los sistemas constitucionales y, principalmente, como el soporte de la teoría de los derechos fundamentales. El análisis del concepto “dignidad humana” lo hace en 2022,⁴ aportando dos conceptos nuevos que son reconocidos en muchas democracias contemporáneas: los derechos de los animales y los derechos de las máquinas.

³ Idem, p. 10.

⁴ Manuel Atienza, *Sobre la dignidad humana*, Trotta, Madrid, 2022, pp. 142-ss.

De ambos se pregunta si poseen o se les debe reconocer cierto grado de “dignidad” y, en consecuencia, una titularidad de derechos o de algún concepto parecido cuyo origen lo encontramos en la moral.

Respecto de los derechos de las máquinas, reflexiona sobre si pueden ser considerados como “agentes morales”, partiendo de que existe determinado tipo de inteligencia artificial que tiene la capacidad de operar en el entorno del mundo real sin ninguna forma de control humano y por periodos de tiempo prolongado.⁵ En ese año, aún no se había comercializado la inteligencia artificial generativa multimodal ni todos los ejemplos de uso que hoy existen. Sin embargo, su estudio es semillero de reflexiones que se pueden construir hoy y que vale la pena realizar para preguntarse si la Teoría del Derecho se mantiene vigente o si requiere de una reformulación (o por lo menos, de una actualización). También esto nos lleva a la teoría de la responsabilidad y al derecho probatorio. En cualquiera de estos campos académicos, vale la pena preguntarnos el tipo de regulación que se requiere para proteger la innovación y evitar un impacto adverso a la persona, el medio ambiente, la sociedad o el gobierno corporativo de una empresa.

La inteligencia artificial avanzada es un nuevo fenómeno que nos lleva a ubicar, en primer término, los beneficios que traerá en los próximos años. La IA avanzada ya no puede ser considerada sólo como una herramienta, ya que sus impactos pueden llegar a al Estado de Derecho, la democracia o los derechos fundamentales. Pero ¿cómo regular algo sin entender primero su naturaleza y sus impactos?

Existen dos errores comunes que se cometen al estudiar los avances de la IA: 1) considerar que es como un ser humano; y, 2)

⁵ Atienza toma esta definición de Lucas Misseri, profesor de la Universidad de Alicante.

mirar a la IA con el lente de las definiciones actuales del mundo (esto evita entender lo que realmente hace la IA).

Lo valioso de las aportaciones de Atienza y de otros publicistas del Derecho es que son una guía clave para entender al Derecho como una construcción social, fruto de diversas posturas teóricas (positivismo jurídico, realismo jurídico, normativismo o iusnaturalismo) que nos lleva ahora hacia una vinculación con la inteligencia artificial.

Este ensayo busca acercar estos temas a la comunidad jurídica con el fin de que se conozcan y se valore el estudio, la enseñanza y la aplicación de la inteligencia artificial y su regulación. Hay algo que el lector debe tener claro: los avances de los científicos y las empresas que están creando modelos de inteligencia artificial para el funcionamiento de sistemas inteligentes van dirigidos hacia la creación de una inteligencia artificial general, basada en las habilidades cognitivas y motivacionales de los propios humanos. El jurista aquí tiene un deber, por lo menos hoy, moral, de estudiar, informarse y entender los tipos y usos para construir el nuevo sentido del Derecho.

Por dar un ejemplo, la autoría o participación en algún hecho ilícito, la toma de decisiones sin intervención humana y su vinculación con responsabilidad jurídica, surgen de una manera distinta a la que los grandes teóricos, como Kant y Hegel, pudieron conocer y los nuevos agentes están transformando el mundo tal como el ser humano lo venía haciendo (de forma exclusiva).

Para concluir esta introducción, debemos decir que en América Latina tenemos una gran influencia del positivismo jurídico y del iusnaturalismo, este último con las aportaciones de Ronald Dworkin⁶ o John Finnis.⁷ Ambos autores fijaron las bases para ana-

⁶ Ronald Dworkin, *Taking Rights Seriously*, General Duckworth & Co. Ltd, Londres, 1977.

⁷ John Finnis, *Natural Law and Natural Rights*, Clarendon Press, Londres, 1980.

lizar los cambios que la inteligencia artificial está generando. El reto lo tenemos, no en cuestionar dichas teorías, sino en el uso que les debemos dar para entender estos avances tecnológicos y en cómo la inteligencia artificial está cambiando el sentido del Derecho. Y aunque Atienza comenta que muchas preguntas de la Filosofía del Derecho se deben responder tomando en cuenta el sistema de valores y las condiciones de desarrollo de cada cultura, lo complicado surge cuando el ser humano enfrenta fenómenos nunca antes vistos.⁸

Evolución tecnológica y conceptos clave para entender la inteligencia artificial

Fue Alan Turing (1912-1954), matemático inglés, el que publicó en 1950 el artículo “Computing Machinery and Intelligence”, con el que pretendía diferenciar entre entidades inteligentes y seres humanos. Turing sometió a la comunidad científica la pregunta: ¿pueden pensar las máquinas? y abrió el debate con el llamado “juego de la imitación”,⁹ al crear una prueba para determinar si

⁸ Atienza, *El sentido del Derecho*, p. 19.

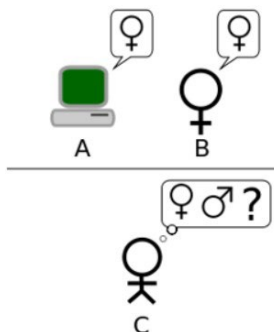
⁹ Turing inicia su texto diciendo: 1. The Imitation Game. I PROPOSE to consider the question, ‘Can machines think?’ This should begin with definitions of the meaning of the terms ‘machine’ and ‘think’. The definitions might be framed so as to reflect so far as possible the normal use of the words, but this attitude is dangerous. If the meaning of the words ‘machine’ and ‘think’ are to be found by examining how they are commonly used it is difficult to escape the conclusion that the meaning and the answer to the question, ‘Can machines think?’ is to be sought in a statistical survey such as a Gallup poll. But this is absurd. Instead of attempting such a definition I shall replace the question by another, which is closely related to it and is expressed in relatively unambiguous words. The new form of the problem can be described in terms of a game which we call the ‘imitation game’. It is played with three people, a man (A), a woman (B), and an interrogator (C) who may be of either sex. The interrogator stays in a room apart from the other two. The object of the game for the interrogator is to determine which of the other

una máquina podía pensar. La máquina superaba la prueba de Turing si el evaluador (humano) no lograba distinguir entre las respuestas dadas por una persona y las respuestas dadas por una máquina. El evaluador se encontraba en una habitación distinta a la de la máquina y a la de la otra persona y sus respuestas le llegarían mediante otra máquina. Turing pensaba que una máquina se podía considerar inteligente si superaba la prueba, es decir, si el humano no podía distinguir el origen de las respuestas (humano o máquina).¹⁰

two is the man and which is the woman. He knows them by labels X and Y, and at the end of the game he says either 'X is A and Y is B' or 'X is B and Y is A'. The interrogator is allowed to put questions to A and B thus: C: Will X please tell me the length of his or her hair? Now suppose X is A, then A must answer. It is A's object in the game to try and cause C to make the wrong identification. His answer might therefore be 'My hair is shingled, and the longest strands are about nine inches long.' In order that tones of voice may not help the interrogator, the answers should be written, or better still, typewritten. The ideal arrangement is to have a teleprinter communicating between the two rooms. Alternatively, the question and answers can be repeated by an intermediary. The object of the game for the third player (B) is to help the interrogator. The best strategy for her is probably to give truthful answers. She can add such things as 'I am the woman, don't listen to him!' to her answers, but it will avail nothing as the man can make similar remarks. We now ask the question, 'What will happen when a machine takes the part of A in this game?' Will the interrogator decide wrongly as often when the game is played like this as he does when the game is played between a man and a woman? These questions replace our original, 'Can machines think?' Cfr. Alan Turing, *Computing machinery and intelligence*, *Mind*, 59 (236), Londres, 1950, pp. 433-460 en <https://doi.org/10.1093/mind/LIX.236.433>.

¹⁰ El cerebro, para algunos pensadores de esa época, podía ser visto como una máquina (ordenador o computadora) que a su vez controla a un cuerpo (robot). En palabras de John Searle, el fenómeno mental y su relación con el cuerpo tiene 4 rasgos característicos: Conciencia, Intencionalidad, Subjetividad y Causación. John Searle debate la prueba de Turing en John Searle, *¿Pueden los computadores pensar?* en *Mentes, cerebros y ciencia*, Ediciones Cátedra, Madrid, 1985, pp. 33-48. Consúltese

Prueba de Turing



Fuente: https://en.wikipedia.org/wiki/File:Turing_Test_Version_1.svg.

El lenguaje de programación de una computadora, conjuntamente con los programas o *software*¹¹ (cada vez más potentes y fáciles de utilizar), han permitido el desarrollo de sistemas, como *ChatGPT* y los *Large Language Models* (LLMs). Un tipo de inteligencia artificial que no existía en el siglo XX y que cobró gran auge a partir de noviembre de 2022, fecha en la que OpenAI lanza su primera versión

también a J. Copeland, *Inteligencia artificial*, Alianza Universidad, Madrid, 1996.

¹¹ Luis Joyanes Aguilar explica lo siguiente “Un programa de *software* es un conjunto de sentencias o instrucciones a la computadora. El proceso de escritura o codificación de un programa se denomina programación y las personas que se especializan en esta actividad se denominan programadores. Existen dos tipos importantes de *software*: *software* del sistema y *software* de aplicaciones. Cada tipo realiza una función diferente. El *software* del sistema es un conjunto generalizado de programas que gestiona los recursos de la computadora, tales como el procesador central, los enlaces de comunicaciones y dispositivos periféricos. Los programadores que escriben *software* del sistema se llaman programadores de sistemas. El *software* de aplicaciones es el conjunto de programas escritos por empresas o usuarios individuales o en equipo y que instruyen a la computadora para que ejecute una tarea específica. Los programadores que escriben *software* de aplicaciones se llaman programadores de aplicaciones”. Cfr. Luis Joyanes Aguilar, *Programación de computadores*, McGraw-Hill Interamericana, Madrid, 2008.

del *ChatGPT*. Sin entrar a una descripción más detallada, podemos decir que la creación de este tipo de inteligencia artificial tuvo que pasar por varias etapas y varias aportaciones de diversas disciplinas.

El debate entre el funcionamiento del cerebro humano, la inteligencia artificial y el lenguaje fueron incorporando a diversas disciplinas, como, por ejemplo, de la Filosofía (dualismo, materialismo, empirismo, inducción, positivismo, lógica, teoría de la confirmación); las matemáticas (algoritmos, teorema de incompletitud, probabilidad); la economía (teoría de la decisión, teoría de juegos, satisfacción y utilidad); neurociencia (cómo procesa el cerebro la información; las neuronas; inteligencia, conciencia); la psicología (conductismo, psicología cognitiva); la Ingeniería computacional; la cibernética (teoría de control); lingüística (lenguaje y pensamiento; representación del pensamiento), y, con ellas, la creación de seis actividades científicas que se relacionan con las funciones que una máquina puede realizar:

- Procesar el lenguaje natural (sistemas expertos).
- Representar conocimiento (sistemas expertos).
- Generar razonamiento automático (sistemas expertos).
- Aprender automáticamente para adaptarse a nuevas circunstancias y patrones (ML/DL).
- Desarrollar visión computacional (ML/DL).
- Manipular objetos (robótica).

A estas funciones, tradicionales de la inteligencia artificial desarrollada en el siglo xx, se le añade la de “crear conocimiento” a partir del uso de los *Large Language Models* (LLMs). Los modelos de lenguaje de gran tamaño (LLM) utilizan algoritmos basados en *Deep Learning* y un concepto denominado “transformador”,¹² que consta de un codificador y un decodi-

¹² D. Jurafsky y J. H. Martin, *Speech and Language Processing*, 2021, consúltese en <https://web.stanford.edu/~jurafsky/slp3/10.pdf>.

ficador con capacidades de autoatención con las que pueden detectar palabras que faltan y que son complementadas gracias al entrenamiento con grandes cantidades de datos. Un LLM puede responder preguntas, resumir documentos, traducir idiomas y completar oraciones. Los LLM pueden generar código a partir de indicaciones en lenguaje natural. Estos modelos también se están entrenando con video y audio.

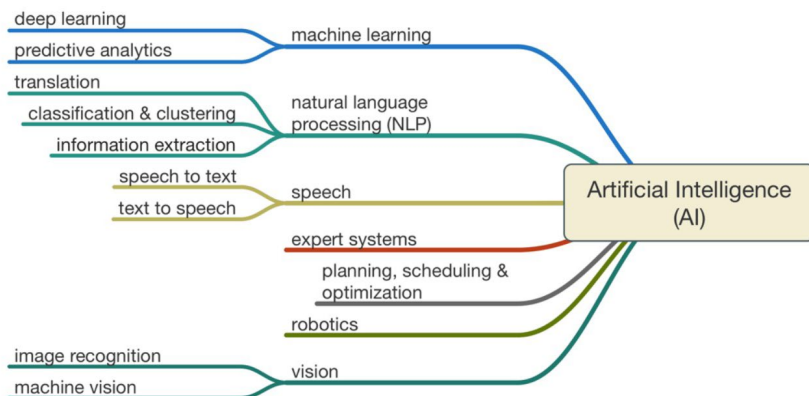
Antes de la existencia de esta tecnología, lo que se utilizó para el procesamiento de textos se basó en los llamados “Sistemas Expertos Decisionales” (SED), su construcción, funcionamiento, tipos y su relación con el procesamiento del lenguaje natural, la representación de conocimiento y la generación el razonamiento automático por un experto humano.¹³

Un SED es capaz de “decidir/recomendar” con base en reglas, conocimiento, casos y/o la experiencia de un humano determinada solución.¹⁴ El objeto de los SED está en el aprovechamiento del conocimiento y experiencia de un humano para transferirlo a la computadora. La computadora almacena el conocimiento, el usuario humano le pide consejos específicos y la computadora hace inferencias hasta llegar a una conclusión específica.

¹³ Cfr. Andrew Myers, Stanford’s Jeffrey Ullman Receives ACM Turing Award. *Stanford News*, marzo 31, 2021. Consúltase en <https://news.stanford.edu/2021/03/31/jeffrey-ullman-receives-acm-turing-award/>. Para conocer más sobre la opinión de expertos en lenguajes de programación y su evolución consúltase: A. Herranz, 20 años después quiero volver a programar: qué grandes cambios ha habido y por dónde empezar, *Xataka*, 2020, June 22, en <https://www.xataka.com/otros/20-anos-despues-quiero-volver-a-programar-que-grandes-cambios-ha-habido-donde-empezar>.

¹⁴ Edward A. Feigenbaum, y Patrick Klahr, Expert Systems, en Anthony Ralston, Edwin D. Reilly, y David Hemmendinger, *Encyclopedia of Computer Science*, Wiley, Hoboken, 2013, pp. 684-689, en <https://doi.org/10.5555/1074100.1074389>.

Ubicación de los Sistemas Expertos Decisionales dentro del campo de la Inteligencia Artificial



Fuente: Hill, 2015.

Otro tipo de inteligencia artificial está basada en lo que se conoce como *Machine Learning*, un subconjunto de la inteligencia artificial que tiene “la capacidad de aprender y mejorar de forma automática a partir de las experiencias, sin necesidad de programación explícita”.¹⁵

¹⁵ Cfr. The Toronto Declaration, *Protecting the Rights to Equality and Non-Discrimination in Machine Learning Systems*, 2018. Consúltase en <https://www.accessnow.org/the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/>.

La siguiente tabla contiene ejemplos de las definiciones más utilizadas de esta tecnología:

Definiciones sobre *Machine Learning* o “Aprendizaje Automático”

Autor	Definición
Artur Samuel	...el campo de estudio que da a las computadoras la capacidad de aprender sin enseñarles explícitamente...
Tom Mitchell	...un programa de computadora aprende de la experiencia (<i>experience</i> = “E”), con respecto a alguna tarea (<i>Task</i> = “T”) y alguna medida del desempeño (<i>performance</i> = “P”), si su desempeño en T, medido por P, mejora con la experiencia E.
Declaración de Toronto	...la capacidad de aprender y mejorar de forma automática a partir de las experiencias, sin necesidad de programación explícita...
Libro blanco	En lo que se refiere a las técnicas de aprendizaje automático, que constituyen un subapartado de la IA, los algoritmos son entrenados para inferir determinados modelos a partir de un conjunto de datos, a fin de determinar las acciones que se requieren para alcanzar un objetivo determinado. Los algoritmos pueden seguir aprendiendo mientras se utilizan.

Fuente: Elaboración propia.

Visto este modelo de inteligencia artificial como un generador de sesgos, podemos advertir que los riesgos que genera tienen que ver con el peligro de amplificar la discriminación de determinadas personas o grupos vulnerables de la población humana. Cuando se utilizan datos históricos para entrenar a los sistemas de aprendizaje automático, estos sistemas pueden reafirmar o incluso aumentar el sesgo estructural. También se pueden causar daños discriminatorios cuando las decisiones tomadas al diseñar los sistemas de IA producen resultados sesgados, ya sea de forma deliberada o no.¹⁶

¹⁶ Thomas G. Dietterich, "Machine Learning." en Anthony Ralston, Edwin D. Reilly, y David Hemmendinger (eds.), *Encyclopedia of Computer Science*, Wiley, Hoboken, 2013, pp. 1114-1118. Hay varios tipos de algoritmos de ML, los principales son los que la doctrina ha clasificado en

El otro tipo de inteligencia artificial que debemos mencionar está dentro de los algoritmos clasificados “por refuerzo” o algoritmos basados en Redes Neuronales Profundas (*Deep Learning*, DL). El DL es “un subcampo del aprendizaje automático que diseña y evalúa algoritmos de entrenamiento y arquitecturas para modelos de redes neuronales *profundas modernas*”.¹⁷ Resaltamos aquí dos conceptos “profundas” y “modernas”, ya que al momento de su creación la red neuronal artificial funcionaba con capas simples (no con múltiples capas). En cambio, una Red Neuronal Profunda (RNP) “es una red de neuronas que tiene *múltiples capas*”.¹⁸

Un dato clave de su evolución lo encontramos en 1969, cuando Marvin Minsky y Seymour Papert publicaron el libro *Perceptrons* con el cual pretendían cuestionar y desaparecer el uso de las redes neuronales del mapa de la IA. Este libro influyó mucho en la comunidad que se dedicaba a realizar investigaciones de inteligencia artificial (por el prestigio que tenían sus autores) al grado que fue disminuyendo de manera considerable la investigación sobre redes neuronales en las universidades de todo el mundo desapareciendo casi por completo por varias décadas.¹⁹

En medio de este primer intento de sepultar las redes neuronales, aparece Geoffrey Hinton, quien en 1978 obtiene su doctorado

tres categorías: 1) aprendizaje supervisado, 2) aprendizaje no supervisado y 3) aprendizaje por refuerzo.

¹⁷ John D. Kelleher, “Deep Learning”, en *The MIT Press*, Cambridge, 2019.

¹⁸ *Idem*.

¹⁹ Cfr. F. Ramírez, Historia de la IA: Frank Rosenblatt y el Mark I Perceptrón, el primer ordenador fabricado específicamente para crear redes neuronales en 1957, *LUCA*, 2018, julio 20. Consúltase en https://web.archive.org/web/20180722124753/https://data-speaks.luca-d3.com/2018/07/historia-de-la-ia-frank-roosenblatt-y-el.html#_

en Inteligencia Artificial en la Universidad de Edimburgo con el tema *Relaxation and its Role in Vision*.²⁰

Hinton estudió a Kant, a Piaget y a Bartlett para explicar que la idea que entendemos el mundo asimilando a nuestros propios esquemas no es nueva. Utiliza a Minsky en sus disertaciones para contraargumentar sus propuestas e inventa el llamado “sistema SETTLE” para demostrar cómo la relajación puede usarse para controlar un sistema basado en datos que hace crecer una red relacional al notar cuando las condiciones complejas se vuelven verdaderas y usar el encadenamiento hacia adelante. Una forma de organizar una búsqueda dentro de un sistema.

Hinton²¹ también es considerado el creador del algoritmo *de Backpropagation* que permite detectar aciertos y errores partiendo de un resultado final y volviendo sobre los pasos que se siguieron previamente. Asimismo desarrolló el algoritmo que creó las Redes Neuronales Profundas (RNP), el cual ha permitido una revolución total de la IA en sectores relacionados con el reconocimiento de imágenes y el procesamiento del lenguaje natural, vehículos sin conductor e interpretación de imágenes médicas para predecir el cáncer.

²⁰ Geoffrey E. Hinton, *Relaxation and Its Role in Vision*, tesis doctoral, Universidad de Edimburgo, 1978. Consúltese en <https://era.ed.ac.uk/handle/1842/8121>.

²¹ Nació en Reino Unido. Su tatarabuelo paterno fue el matemático George Boole. Hinton estaba obsesionado con comprender la mente y sintió que, para hacerlo, uno debía comprender el cerebro. Estudió Psicología Experimental en Cambridge (1970). Obtuvo un doctorado en Inteligencia Artificial en la Universidad de Edimburgo (1978). Actualmente es profesor emérito en el Departamento de Ciencias de la Computación de la Universidad de Toronto (Canadá). Fue vicepresidente en el área de Ingeniería de Google. Para más datos consúltese <https://www.cs.toronto.edu/~hinton/fullcv.pdf>.

El 27 de mayo de 2015, Yann LeCun, Yoshua Bengio y Geoffrey Hinton²² dieron a conocer parte de sus avances científicos con el artículo “*Deep Learning*”. El aprendizaje profundo —comentaron los autores— permite que los modelos computacionales que están compuestos por múltiples capas de procesamiento aprendan representaciones de datos con múltiples niveles de abstracción. Estos métodos han mejorado drásticamente el estado de la técnica en reconocimiento de voz, reconocimiento de objetos visuales, detección de objetos y muchos otros dominios, como el descubrimiento de fármacos y la genómica.

El aprendizaje profundo descubre una estructura intrincada en grandes conjuntos de datos mediante el uso del algoritmo de retropropagación para indicar cómo una máquina debe cambiar sus parámetros internos que se utilizan para calcular la representación en cada capa a partir de la representación en la capa anterior. Las redes convolucionales profundas han producido avances en el procesamiento de imágenes, video, voz y audio, mientras que las redes recurrentes han arrojado luz sobre datos secuenciales como texto y voz.²³

En 2019, Yoshua Bengio, Geoffrey Hinton y Yann LeCun obtuvieron el Premio Turing por sus aportaciones al campo del *Deep Learning*. LeCun comenta que desde mediados de la década de los años de 1990 hasta mediados de la década del 2000 la comunidad científica había perdido interés en este tema, pero lograron organizar reuniones y talleres regulares de verano, creándose una pequeña comunidad que protagonizó un cambio fundamental a partir de 2012-2013.

El punto de quiebre de esa mala imagen que se tenía sobre el uso del *Deep Learning* llegó cuando Hinton ganó el concurso *ImageNet* (2012) gracias a una red neuronal convolucional llama-

²² Yann LeCun, Yoshua Bengio, y Geoffrey Hinton, *Deep Learning*, *Nature*, N° 521, 2015, pp. 436-444. Consúltase en <https://doi.org/10.1038/nature14539>.

²³ Idem, p. 440.

da *AlexNet*, que logró superar a todos sus competidores por una amplia diferencia.²⁴ A partir de ahí, el mundo de la inteligencia artificial retoma el camino de la percepción biológica, dejando a un lado la precisión lógica.

En todo este viaje debemos preguntarnos dónde queda la responsabilidad si ya el ser humano no interviene en la toma de decisiones. Por ejemplo, en el ámbito laboral, se han detectado disparidades en la contratación y en la forma de interpretar datos para la toma de decisiones. Margaret Hu²⁵ explica el caso *Cambridge Analytica-Facebook* (que involucró a millones de usuarios que fueron liberados y explotados sin la debida autorización) analizando una variedad de soluciones legales y políticas que se han propuesto para mejorar la privacidad de la información (una reforma a la Comisión Federal de Comercio e imponer requisitos procesales

²⁴ M. Merino, El Premio Turing, para tres de los principales responsables del actual auge de la inteligencia artificial, *Xataka*, 2019, marzo 29. Consúltase en <https://www.xataka.com/inteligencia-artificial/premio-turing-para-tres-principales-responsables-actual-auge-inteligencia-artificial#:~:text=Geoffrey%20Hinton,-Geoffrey%20Hinton%2C%20brit%C3%A1nico&text=En%201986%20invent%C3%B3%20junto%20a,supervisado%20de%20transformaciones%20de%20imagen%22>.

²⁵ Margaret Hu, Cambridge Analytica's Black Box en *Big Data & Society*, 2020. Consúltase en <https://doi.org/10.1177/2053951720938091>. La autora comenta que el escándalo *Cambridge Analytica-Facebook* generó una preocupación generalizada sobre los métodos implementados para apuntar a los votantes a través de algoritmos de perfiles basados en datos de usuarios de Facebook. El escándalo finalmente condujo a una multa de 5 mil millones de dólares impuesta a Facebook por la Comisión Federal de Comercio (FTC) en julio de 2019. Sin embargo, la acción de la FTC ha sido criticada por no abordar adecuadamente la privacidad y otros daños que emanan de la liberación de Facebook de aproximadamente 87 millones de datos de usuarios de Facebook, que fueron explotados sin la autorización. El ensayo resume la respuesta de la FTC y concluye que en la necesidad de explorar "protecciones del tipo de debido proceso dentro de las acciones de aplicación de las agencias reguladoras como la FTC".

para respetar el debido proceso a actores privados). Prácticamente no hay un sector de la producción o los servicios en los que la inteligencia artificial no se haya usado o no se pueda utilizar; es una herramienta que ha demostrado incrementar la eficacia y eficiencia; pero también se ha convertido en foco de filósofos y expertos en ética, quienes cuestionan permanentemente los impactos negativos, entre ellos, conceptos que están siendo repensados, como, por ejemplo:

- Persona y su dignidad.
- Libre albedrío y autonomía.
- Agencia-agente moral.
- Responsabilidades, *compliance* y programas de integridad.
- Gestión de riesgos por el uso de IA.

Para los fines de este ensayo, atenderemos en particular las reflexiones correspondientes a la responsabilidad y el uso de la ética empresarial en sistemas inteligentes.

Categorías de la responsabilidad y el uso de la ética empresarial en sistemas inteligentes

Una vez hecha la delimitación histórica y conceptual de la inteligencia artificial, así como la descripción de sus tipos, debemos llevar su discusión al ámbito de las categorías de la responsabilidad jurídica y el uso de la ética empresarial con el fin de dar a las personas (físicas y jurídicas) un conjunto de ideas para la creación de indicadores para la gestión de riesgos generados por el uso de la IA.

Esto se debe hacer desde tres distintas dimensiones con el fin de ubicar los riesgos legales, tecnológicos y éticos presentes en cualquier empresa que utilice inteligencia artificial, pero que muchas veces no se mitigan por un desconocimiento de estos temas. Las dos primeras dimensiones son ontológicamente idénticas,

pero epistémicamente distintas; y la tercera tiene que ver con las aportaciones de la ética empresarial.

Las dos primeras dimensiones tienen la misma ontología, ya que surgen de un mismo objeto de estudio que es la realidad denominada “Inteligencia Artificial” (que representa personas, objetos y conceptos de un área de interés y sus relaciones) y la búsqueda de su regulación basada en valores, normas y hechos que están ocurriendo en la sociedad, pero epistémicamente son distintas, puesto que la primera la encontramos en el sistema jurídico (norma jurídica) y en la doctrina que le da soporte; y la segunda la ubicamos en el ámbito de la Ingeniería y la ciencia de datos (norma no vigente, pero sí aplicable, en ocasiones, por las organizaciones que las han creado). Ambas, se relacionan con la medición de riesgos legales y tecnológicos y su mitigación. Todo riesgo tecnológico a su vez puede ser un riesgo legal y ético, pero no a la inversa.

En cambio, la tercera dimensión se relaciona con las virtudes que debe tener el empresario, el lograr un ambiente laboral bueno, el buscar cumplir principios, valores y reglas de comportamiento (integridad empresarial) y sus fines van más allá de las dos dimensiones previas tanto en el tiempo como en la amplitud de los beneficios.

En la primera dimensión, encontramos la norma vigente y la dogmática que le da vida y que le permite enjuiciar por un hecho ilícito o por la comisión de un delito a cualquier persona que esté en los supuestos contenidos en la propia ley. Aquí nos preguntamos si las categorías vigentes de la responsabilidad jurídica y su dogmática sirven para solucionar los problemas que pueden surgir por el uso de sistemas inteligentes, analizando qué salidas ofrece la legislación.

La segunda dimensión, tiene relación con conceptos que aún no se encuentran vigentes ni el Derecho mexicano ni en muchos otros sistemas jurídicos. Esta dimensión se está construyendo en los laboratorios y actividades académicas de las facultades de Ingeniería, de Ciencia de Datos y de Filosofía de la

IA,²⁶ a través de propuestas de diversas organizaciones (IEEE, ACM, OCDE, UNESCO, entre otras), expertos independientes y académicos (como el de interpretabilidad y explicabilidad), y es la base para crear una nueva categoría de responsabilidad por el uso de sistemas inteligentes. Aquí nos preguntamos si es necesario ampliar las categorías de responsabilidad con el concepto: responsabilidad algorítmica.

La responsabilidad algorítmica surge conjuntamente con otro concepto denominado “Agente Artificial Moral Autónomo”, “Persona Electrónica” o “Persona Algorítmica”. El uso de estos conceptos, a su vez permitirá dividir la responsabilidad que le corresponde a la máquina de la responsabilidad que les corresponde a los seres humanos, como la de: 1) los que producen los datos, 2) los que procesan los datos, 3) los que desarrollan los sistemas; 4) los que utilizan el sistema; 5) los que adquieren el sistema; 6) los que certifican un sistema; y 7) los que auditan el sistema. En un futuro, la búsqueda de la responsabilidad del ser humano y la búsqueda de la responsabilidad de las máquinas será parte de la valoración que hagan jueces, peritos, fiscales, árbitros, etcétera.

Y, finalmente, la tercera dimensión tiene que ver con la ética empresarial y busca regular conductas que pueden generar afectaciones a las personas (dentro y fuera de la organización).

²⁶ Un ejemplo de nuevos conceptos es la llamada “Ética algorítmica” que se pregunta cómo la IA, aprendizaje máquina y robots interpretan los datos y de una “Ética de la IA”, que prioriza consideraciones para la creación de sistemas de IA, promoviendo estándares o difundiendo políticas globales, regionales o nacionales para su uso; también hay una “Ética de las máquinas”, que busca construir sistemas inteligentes que tomen decisiones autónomas y se pregunta cómo codificar la moral en las máquinas; y, hay una “IA moral”, dedicada a conseguir la cooperación máquina-ser humano para resolver problemas complejos con el uso de la moral; la IA es vista como un mecanismo para la mejora de los seres humanos. *Cfr.* Aníbal Monasterio Astobiza, *Ética Algorítmica: Implicaciones Éticas de una sociedad cada vez más gobernada por algoritmos*, *Dilemata*, N° 24, 2017, pp.185-217.

Aquí nos preguntamos si a la par de una respuesta jurídica debería haber una respuesta ética; creemos que sí y que las actuales aportaciones de la ética en la IA, así como de la ética empresarial proporciona el soporte adecuado para ello.

Un pensador que lleva la Filosofía al mundo empresarial es Carlos Llano Cifuentes. Sus reflexiones pueden ser útiles para construir lo que podemos llamar la “Teoría de las responsabilidades”²⁷ con sus cuatro campos de actuación: 1) la responsabilidad del consecuente (o responsabilidad de las consecuencias de la acción); 2) la responsabilidad del antecedente (o responsabilidad de los principios); 3) la responsabilidad congruente (o responsabilidad de los proyectos anteriores de mi vida); y 4) la responsabilidad del trascendente (o de la misión a la que, con mi vida, he sido destinado). La importancia de utilizar esta teoría como ingrediente adicional a los controles de autorregulación o de integridad corporativa que las empresas tienen y como un complemento a sus programas de *compliance*, les permitirá demostrar a la autoridad que la empresa ha hecho todo lo que está en sus manos para evitar una afectación derivada de sistemas de IA y evitará así una posible sanción jurídica o reputacional.

Llano conocía perfectamente las distintas posturas de los abogados en el tema de la responsabilidad (Kant, Rawls, Dworkin, entre otros) y con su pensamiento las analizó y decidió construir categorías de responsabilidades específicas para la empresa. Para Llano, la empresa debe ser entendida no como un lugar de comercio de productos o servicios, sino como una comunidad de seres humanos con dignidad, inteligencia, fines en común y responsabilidades. No en vano se conoce a Carlos Llano Cifuentes como el filósofo-empresario y el empresario-filósofo.

Las tres dimensiones, en conjunto, constituyen la metodológica para la medición de riesgos legales, tecnológicos y éticos que

²⁷ Carlos Llano Cifuentes, *Dilemas éticos de la empresa contemporánea*, IPADE-Ediciones ECA, México, 2019.

utiliza un catálogo de indicadores básicos como instrumento para que las empresas y los gobiernos mitiguen sus riesgos, incorporando estos indicadores a su programa de integridad corporativa y a su programa de *compliance*, así como a los sistemas automatizados que utilizan para medir los riesgos. Lo anterior, se puede esquematizar en la siguiente tabla:

Catálogo de indicadores básicos para la gestión de riesgos legales, tecnológicos y éticos

Riesgos legales (1era dimensión)	Riesgos tecnológicos (2da dimensión)	Riesgos éticos (3ra dimensión)
1. Responsabilidad civil (DDHH)	1. Tipo de inteligencia artificial	1. Responsabilidad del antecedente
2. Responsabilidad penal (DDHH)	2. Datos	2. Responsabilidad del congruente
3. Privacidad (DDHH)	3. Sesgos algorítmicos	3. Responsabilidad del trascendente
4. Transparencia (DDHH)	4. Opacidad	
	5. <u>Interpretabilidad</u>	
	6. <u>Explicabilidad</u>	
	7. Responsabilidad algorítmica	

Compliance (Responsabilidad del consecuente)

Integridad corporativa

Gobierno corporativo basado en la responsabilidad moral (según Carlos Llano Cifuentes)

Fuente: Elaboración propia.

Este tipo de metodología permite a las organizaciones gestionar sus riesgos por el uso de inteligencia artificial y vincularlo esta actividad con sus políticas, procesos y procedimientos y contando en su estructura a un supervisor de inteligencia artificial. Sin embargo, ese supervisor difícilmente podría gestionar los riesgos que se derivan de esa tecnología.

A continuación, explicaremos el perfil de ese nuevo puesto que está surgiendo en diversas organizaciones.

El *Chief Artificial Intelligence Officer* (CAIO)

La IA se traduce en una valiosa herramienta de trabajo que optimiza los resultados de cualquier organización. Ahora bien, así como se generan beneficios, hay obligaciones que tienen las organizaciones y una de las más importantes se refiere a una actividad de supervisión humana que se sustenta en dos fases: la primera, es la contratación de cursos de actualización, y en su caso, de especialización en IA para quienes ejercen acciones en puestos directivos o gerenciales y, una vez satisfecha esta necesidad, existe el deber de compartir estos conocimientos en toda la organización.

La segunda fase se refiere a la creación de una posición específica que supervise la IA, esto es, un *Chief Artificial Intelligence Officer* (CAIO) o responsable del despliegue de la IA. Este puesto no es un simple ajuste a la estructura de la organización, sino que forma parte de los cambios que están permitiendo un incremento exponencial de la productividad, procurando en todo momento, que la empresa también responda a exigencias éticas que derivan del uso de la IA.

De 2016 a 2022, a nivel mundial, se presentaron más de mil iniciativas legislativas para regular o estandarizar con principios éticos la utilización de IA. Todas tienen un elemento en común: la necesidad de que las organizaciones, cuenten con una persona responsable de la supervisión de la IA. Esto generó que desde 2019 ya existieran empresas que comenzaron a experimentar con figuras de supervisión de la IA; pero a partir del inicio de la Inteligencia Artificial Generativa (Inteligencia Artificial Avanzada), en noviembre de 2022, las prácticas que se derivan de una y otra, han cobrado más fuerza generando una demanda de talento, principalmente, en Estados Unidos y Europa.

Empresas, gobiernos, líderes de opinión, académicos e investigadores, coinciden en que la IA coadyuva a mejorar la toma de decisiones, disminuye costos y tiempos y a respaldar soluciones que puedan transformar sus negocios para beneficio de la comunidad

a la que sirven. Para lograrlo, quienes tengan la responsabilidad de decidir e incidir en las estructuras internas de la organización, deben tener en cuenta que el CAIO es un actor clave para aprovechar este enorme potencial, protegiendo a las empresas de posibles impactos adversos a los derechos humanos.

El puesto de CAIO es estratégico en cualquier organización. Es el responsable de supervisar el despliegue de la IA y prever la gestión de los riesgos, con el fin de que la empresa o la institución de gobierno no impacte de forma negativa en los derechos de las personas, el entorno social, ambiental, la democracia y el Estado de Derecho. Pero a la vez debe garantizar que el modelo de IA mantenga e incremente los beneficios que recibe la organización, sin afectar los estándares éticos y regulatorios. El CAIO será quien implemente las normas ISO, normas IEEE o cualquier otra especializada que se encuentren en los diversos sectores de la producción o de los servicios que existen en un país.

En este orden de ideas, su función va más allá del respeto a la privacidad y seguridad de los datos personales; tampoco se debe ver como el responsable de la ciberseguridad o el director de tecnologías de la información. El diseño del perfil de puesto debe partir de entender estas características y de añadir una más que no está en las mencionadas, es decir, la evaluación de impactos adversos a derechos humanos por el uso de IA (auditorías algorítmicas).

En resumen, actúa como un puente entre la tecnología, el negocio, los marcos éticos y regulatorios vigentes para la empresa, y, por otra parte, asegura que el modelo de negocio y el modelo de IA sean compatibles, evitando en consecuencia la imposición de sanciones o de multas cuyos montos pudieran ser extremadamente onerosos.

El puesto de CAIO requiere también la formación de un profesional que tenga las bases fundamentales de la Ingeniería, el Derecho y la Filosofía. Por ello, se requiere que el candidato a CAIO tenga una profunda comprensión de los diversos tipos de IA, sus usos y riesgos y una sólida base de la ética y de conocimientos de

las diferentes normas jurídicas que regulan el sector en el que se desarrolla la organización.

En este sentido, el responsable de CAIO debe comprender que la gestión de riesgos está presente como en cualquier otra posición de *compliance* dentro de la organización, pero los riesgos derivan de toda la estructura que conforman las normas internacionales que protegen derechos humanos, y en su caso, de la forma como el régimen constitucional en el que se ve inmerso entiende estos temas y su protección. Además, debe contar con habilidades blandas (pensamiento estratégico, comunicación efectiva, gestión del cambio, persuasión y negociación, entre otros) para liderar equipos multidisciplinarios de personas y fomentar los valores éticos que dan vigencia a una IA responsable.

Sin entrar a detalles que impacten presupuestalmente a las empresas, es válido afirmar que este puesto es necesario para la organización que pretende utilizar o ya esté utilizando IA. Según datos de *Foundry*, en 2023, el 11 por ciento de las organizaciones medianas y grandes ya tienen un CAIO designado o equivalente en esta responsabilidad, y el 21 por ciento de las organizaciones están buscando activamente contratar uno.

La entrada en vigor de la AI Act (Reglamento de Inteligencia Artificial de la Unión Europea) y el enorme cúmulo de reformas legislativas que están por entrar en vigor en todo el mundo (México tiene por lo menos más de cuarenta iniciativas de ley), hacen más que evidente la inaplazable creación de esta posición en las organizaciones de los sectores público, privado y social.

Como en todo cambio de esta importancia, siempre surgirán personas que tengan sus reservas o sean escépticos, y, por otra parte, se encuentran aquellos que sean optimistas y promotores del cambio. Al final del día, en esto se debe pensar: los empresarios, el gobierno y la sociedad en general deben construir un ecosistema de protección social para la utilización de una IA responsable.

La creación del puesto de CAIO refleja un reconocimiento de la importancia estratégica de la IA para el futuro mediano de las empresas. A medida que se avanza hacia un mundo cada vez más impulsado por esta tecnología, la figura del CAIO será esencial para liderar con éxito la transformación digital de las empresas, gobiernos y sociedad en general, asegurando que las organizaciones no sólo se mantengan a la vanguardia de la innovación, sino que también transiten por el complejo panorama ético y regulatorio que ya se encuentra presente el uso de la IA.

Este rol emergente es un testimonio de cómo la IA está impactando al mundo, y, por tanto, se hace necesaria la participación de filósofos y juristas, como actores clave para la protección de la persona en la Era Digital. Las organizaciones que reconozcan y se adapten a esta evolución estarán mejor posicionadas para aprovechar las oportunidades que la IA ofrece. El mercado laboral exige que las universidades y centros de formación directiva deban planear una trayectoria académica que permita atender la necesidad de un perfil de egresado que pueda hacerse responsable de las funciones del CAIO.

La integración de la IA en el modelo de negocio trae consigo desafíos significativos. De tal manera, el informe de Baker McKenzie, *Risky Business: Identifying Blind Spots in Corporate Oversight of Artificial Intelligence* (2022),²⁸ destaca la necesidad de una supervisión corporativa en el uso de IA identificando los riesgos actuales y subrayando la importancia de un enfoque proactivo hacia la gestión de estas tecnologías. Hay que enfatizar que IA permite potencializar la toma de decisiones, optimizar procesos y abrir nuevos mercados. Sin embargo, las organizaciones deben estar conscientes de las responsabilidades legales que implican el consecuente impacto que puede tener esta tecnología en la persona, su dignidad, sus capacidades decisorias y, por supuesto, en los riesgos de su utilización sin un debido fundamento ético dentro de la

²⁸ Consúltase en <https://www.bakermckenzie.com/-/media/files/aisurveypptfinalmarch2022.pdf>.

organización. Es aquí donde el CAIO desempeña un rol crucial y relevante en la atención a dos aspectos notoriamente relevantes: la responsabilidad moral (normas UNESCO) y la responsabilidad jurídica (normas de cada país o comunidad).

Auditorías algorítmicas y la implementación de la norma ISO 42001

Una auditoría algorítmica es un análisis que se hace para detectar y mitigar los riesgos que genera el uso de determinados tipos de inteligencia. Se analiza todo el ciclo de vida del modelo de IA; lo aprendido y los resultados, con el fin de mitigar los impactos adversos a derechos humanos. En este tema es muy importante tener presente la clasificación de riesgos que se está proponiendo en la Unión Europea en su AI Act para vincularla con metodologías para la gestión de riesgos de algunas organizaciones como la IEEE o las normas ISO.

Las organizaciones, públicas o privadas que están utilizando inteligencia artificial deben intentar implementar algún sistema de gestión de riesgos. Así surge la supervisión y así tendríamos en un futuro mediano mecanismos de gestión de riesgos para detectar impactos adversos a derechos fundamentales en el uso de IA. Coincidimos con los autores que están proponiendo la aplicación de auditorías algorítmicas de IA basada en *Machine Learning-Deep Learning*, es decir, que la inteligencia artificial sea supervisada por la propia IA. Sin lugar a dudas, este tipo de acciones ha traído grandes resultados a muchos sectores de la producción y los servicios, sobre todo, en el ámbito financiero y de los servicios de salud. Partamos de una pregunta: ¿cómo determinar en una auditoría algorítmica qué impacta y qué no impacta al ser humano? Hay dos caminos para ello. El camino de los datos y la privacidad y el camino de la ética de la IA. También podemos crear un tercer camino basado en los derechos fundamentales y sus principios.

Por ello, las auditorías algorítmicas se basan en un enfoque de gestión riesgos y en lo que se conoce como una “Evaluación

de Impacto en Derechos Humanos” (EIDH). Dos conceptos claves que se interrelacionan y que buscan, entre otras cosas analizar la opacidad y la explicabilidad, aclarando que dependiendo la metodología y el modelo de negocio, serán los indicadores de medición.

Veamos algunas ideas, pensando en que sirvan de ejemplos para la construcción de una metodología para la gestión de riesgos basada en normas ISO y en el uso de una inteligencia artificial generativa.

Respecto de la opacidad, las empresas deben medir los riesgos que tendrán por la opacidad de sus algoritmos. Los llamados “algoritmos de caja negra” han sido cuestionados porque se desconoce su trazabilidad. Este indicador tiene que ver con el uso de datos y de los sesgos algorítmicos. Las empresas que utilizan algoritmos de caja negra deben estar conscientes que su uso genera riesgos que deben ser medidos para que no se genere un daño legal o reputacional. La empresa debe detectar si la opacidad es el resultado de los propios algoritmos, o es una decisión humana que busca ocultar secretos corporativos, o es una decisión humana derivada de la falta de conocimiento técnico de su equipo de trabajo. La principal bandera roja de la opacidad es el uso de patrones oscuros que genera cierto tipo de algoritmos. La mitigación de este tipo de riesgo se hace a través de los principios interpretabilidad y explicabilidad, así como de las auditorías algorítmicas para entender su utilización y los resultados de éstas. La detección de una opacidad derivada del propio algoritmo tiene que ser atendida con algún otro sistema de IA que pueda dar al ser humano la interpretabilidad y explicabilidad necesarias para no afectar los derechos de las personas. La opacidad algorítmica puede limitar las categorías de responsabilidad y acarrea consecuencias como la discriminación por motivos de raza, sexo, entorno social, entre otros.

Respecto de la explicabilidad, las empresas deben medir los riesgos por el uso de la IA que genera la imposibilidad de explicar las decisiones de los algoritmos IA basada en *Machine Learning*.

Deep Learning. Si bien la explicabilidad algorítmica está en algunos métodos de inteligencia artificial (*explanatory artificial intelligence*, XAI), dicha explicabilidad no sirve para explicar a la sociedad o a los usuarios lo que ocurre en el procesamiento de datos con un lenguaje cotidiano. Estamos nuevamente con el concepto de opacidad y los “algoritmos de caja negra”. Las empresas se deben preguntar si el sistema de IA o su equipo especializado en estos temas tienen la posibilidad de generar explicaciones “comprensibles para los seres humanos”. Y, en caso contrario, qué mitigantes tiene para evitar una carga de responsabilidad por el uso de IA no explicable. En este sentido, sirve mucho ubicar si los algoritmos tienen explicaciones internas (para expertos de IA) o externas (las exigidas por la sociedad y los usuarios).

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea crea obligaciones para los procesos de toma de decisiones automáticos y el derecho a una explicación. La empresa medirá sus riesgos tomando como base el tratamiento de la información o los datos que regulan las normas jurídicas, que, para el caso, encontramos en el artículo 71 del reglamento mencionado: es el derecho a obtener intervención humana, a expresar su punto de vista, a recibir una explicación de la decisión tomada después de tal evaluación y a impugnar la decisión. Se medirá: 1) las circunstancias y contexto específicos en los que se tratan los datos personales, 2) si el responsable del tratamiento de los datos utilizó procedimientos matemáticos y estadísticos adecuados para la elaboración de perfiles, 3) aplicación de medidas técnicas y organizativas apropiadas para garantizar, y 4) si se buscó reducir al máximo el riesgo de error para asegurar los datos personales de forma que se tengan en cuenta los posibles riesgos para los derechos del interesado y se impidan, entre otras cosas, efectos discriminatorios en las personas físicas por motivos de raza u origen étnico, opiniones políticas, religión o creencias, afiliación sindical, condición genética o estado de salud u orientación sexual, o que den lugar a medidas que produzcan tal efecto.

Las decisiones automatizadas y la elaboración de perfiles sobre la base de categorías particulares de datos personales únicamente deben permitirse en condiciones específicas. Este indicador busca generar confianza en los usuarios de los sistemas de IA, mostrando sus fortalezas, beneficios y desafíos, y, a la vez, sirve para que cualquier parte inconforme del resultado pueda impugnar ante la autoridad el mismo (la vía legal con base en evidencias) y generar una “IA fiable”. Una buena explicación lleva varios ingredientes que se deben incluir en las reflexiones del grupo de expertos que la empresa constituya para medir los riesgos de este indicador.

La norma ISO/IEC 42001 es una herramienta básica para la realización de una auditoría algorítmica, ya que se adapta a cualquier empresa, independiente de su tamaño o de su naturaleza (pública o privada). La norma tiene la intención de ayudar a las organizaciones a desempeñar de manera responsable su papel con respecto a los sistemas de IA (por ejemplo, usar, desarrollar, monitorear o proporcionar productos o servicios que utilicen IA). La IA, dicen sus creadores, puede plantear consideraciones tales como:

- El uso de la IA para la toma de decisiones automáticas, a veces de forma poco transparente e inexplicable, puede requerir una gestión específica más allá de la gestión de los sistemas informáticos clásicos.
- El uso del análisis de datos, la información y el aprendizaje automático, en lugar de la lógica codificada por humanos para diseñar sistemas, aumenta las oportunidades de aplicación de los sistemas de IA y cambia la forma en que se desarrollan, justifican e implementan dichos sistemas.
- Los sistemas de IA que realizan un aprendizaje continuo cambian su comportamiento durante el uso. Requieren una consideración especial para garantizar que su uso responsable continúe con el cambio de comportamiento.

Para ello, la norma proporciona a las organizaciones los requisitos básicos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de IA en el contexto de una organización. Se espera que las organizaciones centren su aplicación de requisitos en características que son exclusivas de la IA. Ciertas características de la IA, como la capacidad de aprender y mejorar continuamente o la falta de transparencia o explicabilidad, pueden justificar diferentes salvaguardas si plantean preocupaciones adicionales en comparación con la forma en que se realizaría tradicionalmente la tarea. La adopción de un sistema de gestión de IA para ampliar las estructuras de gestión es una decisión estratégica para una organización.

El sistema de gestión que implemente la organización para proteger su modelo de negocio y el uso de la IA debe integrarse a los procesos de la organización y a la estructura de gestión. En unos años tendremos oficiales de cumplimiento especializados en IA que estén vigilando el uso de ésta con base en este estándar de operación, siendo un requisito tener un supervisor y la regulación básica para gestionar riesgos de IA.

Hacia un ecosistema de protección social para el uso responsable de la inteligencia artificial (conclusiones)

Consideramos importante hacer una serie de conclusiones que complementan las argumentaciones previas con el fin de entender cómo se está construyendo el nuevo sentido del Derecho. La justicia como fin de ese nuevo sentido del Derecho debe surgir de la construcción de un “Ecosistema de protección social para el uso de IA” (o quizás varios ecosistemas regionales); aclarando aquí que los filósofos del Derecho deben vincularse más con los eticistas y con los ingenieros para entrar al debate de conceptos que estarán ampliándose (dignidad, persona, agencia moral, responsabilidad, sesgos, entre otros). La doctrina hará su parte y los operadores jurídicos deberán

trabajar para lograr la materialización de los siguientes elementos:

- Normas jurídicas (dentro y fuera de la empresa y los gobiernos).
- Agencias de gobierno supervisoras de la IA, responsables de verificar que las organizaciones se capaciten, creen políticas, procedimientos y procesos para el uso responsable de la IA.
- Empresas certificadoras y auditoras de IA.
- Programas y responsables de implementar el *Compliance* en IA,
- Creación de metodologías para la medición y evaluación del impacto adversos de la IA en los derechos humanos (por ejemplo, Norma ISO/IEC 42001).
- Autoridades especializadas en dirimir conflictos por el uso de IA y en llevar un registro público de algoritmos, así como en supervisar el impacto social y ambiental de esta tecnología.
- Tribunales especializados en dirimir controversias por temas de responsabilidad algorítmica y afectación a derechos humanos por el uso de este tipo de tecnología.
- Fortalecer el comité de IA que tiene la Organización de las Naciones Unidas (ONU) y replicarlo en sus homólogos regionales.
- Actualización de planes de estudio en escuelas, universidades y centros de investigación para incluir los nuevos conceptos y usos de la IA y hacer labores de prevención y de divulgación.
- Participación de los organismos empresariales y cámaras de comercio en la capacitación y divulgación de estos temas.

- Utilizar los beneficios de la ética empresarial y de la participación de eticistas expertos en IA.
- Desarrollar políticas, procesos, procedimientos, sistemas, certificaciones y mecanismos de auditoría o vigilancia al interior y exterior de las empresas que generan IA o de los gobiernos que la estén utilizando para alguna actividad en la que se vea involucrada la población.

La inteligencia artificial avanzada va a transformar el mundo. Generará oportunidades de negocio para todo aquel que decida descubrir sus aportaciones. Es un descubrimiento científico nunca antes visto. Hay industrias maduras y otras que requieren de ayuda. Por ello, diferentes tipos de IA requieren diferentes tipos de regulación. La IA eliminará muchos empleos y creará otros completamente nuevos. Por todo ello, los juristas deben crear el nuevo sentido del Derecho.

BIBLIOGRAFÍA

- Atienza, Manuel, *El sentido del Derecho*, Ariel, Madrid, 2001.
- Atienza, Manuel, *Sobre la dignidad humana*, Trotta, Madrid, 2022.
- Copeland, Jack, *Inteligencia artificial*, Alianza Universidad, Madrid, 1996.
- Dietterich, Thomas G., Machine Learning, en Ralston, Anthony: Reilly, Edwin D., y Hemmendinger, David. *Encyclopedia of Computer Science*, Wiley, Hoboken, 2013.
- Dworkin, Ronald, *Taking Rights Seriously*, General Duckworth & Co. Ltd, Londres, 1977. Hay una versión en castellano, traducida por Marcial Guastavino, Ariel, Barcelona, 2002.
- Feigenbaum, Edward A., y Klahr, Patrick, Expert Systems, en Ralston, Anthony: Reilly, Edwin D., y Hemmendinger, David. *Encyclopedia of Computer Science*, Wiley, Hoboken, 2013. <https://doi.org/10.5555/1074100.1074389>.
- Finnis, John. *Natural Law and Natural Rights*, Clarendon Press, Oxford, 1980. Existe una versión en castellano traducida por Carlos Orrego, Abeledo-Perrot, Buenos Aires, 2000.

- Hill, Caroline. Artificial Intelligence in Law –The State of Play in 2015?, *Legal Technology*, noviembre 3, 2015, <https://legaltechnology.com/artificial-intelligence-in-law-the-state-of-play-in-2015/>.
- Hinton, Geoffrey E., *Relaxation and Its Role in Vision*, tesis doctoral, Universidad de Edimburgo, 1978, <https://era.ed.ac.uk/handle/1842/8121>.
- Hu, Margaret, Cambridge Analytica's Black Box, *Big Data & Society*, 2020. <https://doi.org/10.1177/2053951720938091>.
- International Organization for Standardization, ISO/IEC 42001:2023 Information Technology —Artificial Intelligence— Management of AI Systems, ISO, Ginebra, 2023.
- Jurafsky, Daniel, y Martin, James H., *Speech and Language Processing, Draft* de febrero 3 de 2024, <https://web.stanford.edu/~jurafsky/slp3/10.pdf>.
- Kelleher, John D., *Deep Learning*, Cambridge, Massachusetts, The MIT Press, 2019.
- Llano Cifuentes, Carlos, *Dilemas éticos de la empresa contemporánea*, IPADE-Ediciones ECA, México, 2019.
- Merino, Marcos, El Premio Turing, para tres de los principales responsables del actual auge de la Inteligencia Artificial, *Xataka*, marzo 29, 2019, en <https://www.xataka.com/inteligencia-artificial/premio-turing-para-tres-principales-responsables-actual-auge-inteligencia-artificial#:~:text=Geoffrey%20Hinton,-Geoffrey%20Hinton%2C%20brit%C3%A1nico&text=En%201986%20invent%C3%B3%20junto%20a,supervisado%20de%20transformaciones%20de%20imagen%22>.
- Monasterio Astobiza, Aníbal, Ética Algorítmica: Implicaciones éticas de una sociedad cada vez más gobernada por Algoritmos, *Dilemata*, N° 24, 2017.
- Myers, Andrew, Stanford's Jeffrey Ullman Receives ACM Turing Award, *Stanford News*, marzo 31, 2021, en <https://news.stanford.edu/2021/03/31/jeffrey-ullman-receives-acm-turing-award/>.
- Samuel, Arthur, "Some Studies in Machine Learning Using the Game of Checkers", *IBM Journal of Research and Development*, 3, N° 3, 1959.
- Searle, John, ¿Pueden los computadores pensar?, en *Mentes, cerebros y ciencia*, Ediciones Cátedra, Madrid, 1985.
- The Toronto Declaration, *Protecting the Rights to Equality and Non-Discrimination in Machine Learning Systems*, 2018, <https://www.accessnow.org/>

the-toronto-declaration-protecting-the-rights-to-equality-and-non-discrimination-in-machine-learning-systems/.

Turing, Alan M., Computing Machinery and Intelligence, *Mind*, 59, N° 236, 1950, <https://doi.org/10.1093/mind/LIX.236.433>.

Wikipedia, Turing Test Version 1, https://en.wikipedia.org/wiki/File:Turing_Test_Version_1.svg.



Inteligencia jurídica en expansión

Trabajamos para
mejorar el día a día
del **operador jurídico**

Adéntrese en el universo
de **soluciones jurídicas**

 +52 1 55 65502317

 atencion.tolmex@tirantonline.com.mx

prime.tirant.com/mx/