Memorias de la

# RUTA de la PRIVACIDAD

## Inteligencia Artificial: perspectivas y prospectivas desde el derecho a la protección de datos personales y la privacidad


Josefina Román Vergara

Francisco Javier Acuña Llamas

COORDINADORES



DIPDP 2022

inai

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Sistema Nacional de Transparencia

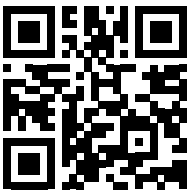
Acceso a la Información Pública y Protección de Datos Personales

# Memorias de la Ruta de la Privacidad

*Inteligencia Artificial: Perspectivas y prospectivas desde el derecho a la protección de datos personales y la privacidad*


Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Josefina Román Vergara
Francisco Javier Acuña Llamas
(Coordinadores)



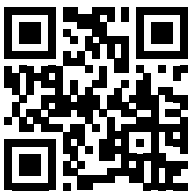
**inai.org.mx**

# Memorias de la Ruta de la Privacidad

*Inteligencia Artificial: Perspectivas y prospectivas desde el derecho a la protección de datos personales y la privacidad*

**Sistema Nacional de Transparencia**
Acceso a la Información Pública y Protección de Datos Personales

Josefina Román Vergara
Francisco Javier Acuña Llamas
(Coordinadores)



**snt.org.mx**

*Memorias de la Ruta de la Privacidad.*
*Inteligencia artificial: perspectivas y prospectivas*
*desde el derecho a la protección de datos personales y la privacidad*

D.R. Instituto Nacional de Transparencia, Acceso a la Información
y Protección de Datos Personales
D.R. Sistema Nacional de Transparencia, Acceso a la Información Pública
y Protección de Datos Personales
D.R. Editorial Didáctica M.R.
México, 2022. 256 páginas. Medida: 16 cm × 23 cm

ISBN 978-607-99443-9-1 Primera edición: noviembre de 2022

**Instituto Nacional de Transparencia, Acceso a la Información**
**y Protección de Datos Personales**
Avenida Insurgentes Sur 3211, Colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, Código Postal 04530, Ciudad de México.

**Coordinadores**

**Comisionada del INAI**
Josefina Román Vergara
**Comisionado del INAI**
Francisco Javier Acuña Llamas

**Compiladores**

**Jefe de Ponencia de la Oficina de la Comisionada del INAI, Josefina Román Vergara**
Felipe de Jesús Gutiérrez Rincón
**Directora de Facilitación del Sector Público**
Elizabeth Vicenté González

**Coordinación editorial**
Alfredo Díaz Barriga de los Cobos
**Correctores de estilo**
Simitrio Quezada Martínez
María Elizabeth Vázquez Flores
Jesús Roberto González de Ávila
Luis Felipe Pérez Magaña
Dan Gamaliel López Alegría
**Control de Calidad Editorial**
Carlos Iván Díaz Barriga de los Cobos

2022, Sello Editorial Didáctica (978-607-99443) M.R. | México
www.editorialdidactica.mx; produccion@editorialdidactica.mx

**Directorio**

# ÍNDICE

**Eje temático III**
Fortalecimiento Institucional
a través de la Ruta de la Privacidad
146

**Comentarios adicionales**
180

Galería de la Ruta de la Privacidad

225 - 256

# PRESENTACIÓN

BLANCA LILIA IBARRA CADENA

*Comisionada Presidenta*
*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*

En el marco de la conmemoración del Día Internacional de la Protección de Datos Personales de enero de 2022 inició la Ruta de la Privacidad, resultado del esfuerzo del INAI —con el respaldo de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia (SNT) y los organismos garantes de las entidades federativas—, que no sólo busca apuntalar la socialización y promoción del derecho a la protección de datos personales en todo el país, sino también impulsar el desarrollo y uso ético, justo y seguro de la inteligencia artificial a partir de la conformación de un espacio de diálogo y retroalimentación que facilite el intercambio de avances, desafíos y mejores prácticas en la materia.

Así, desde el Pleno del INAI, nos congratulamos al presentar las *Memorias de la Ruta de la Privacidad*, un producto editorial que busca exponer las voces expertas que nos acompañaron durante las actividades de esta iniciativa.

En el desarrollo de sus tres ejes temáticos, el lector encontrará valiosas reflexiones relacionadas con: los avances normativos en materia de datos personales en América Latina; la relación de esta prerrogativa con la ciberseguridad y la integración de la inteligencia artificial en sectores como el turismo, la seguridad pública y el gobierno electrónico; así como un análisis del avance institucional en la materia, incluyendo el diseño e implementación de las políticas de privacidad y protección de datos personales formuladas desde el SNT.

En esa tesitura, es necesario reconocer a los organismos garantes que impulsaron e hicieron suya dicha *Ruta* —Ciudad de México, Estado de México, Yucatán, Hidalgo, Chihuahua, Nuevo León, Veracruz, Michoacán, Guerrero, Quintana Roo, Tlaxcala, Querétaro, Oaxaca y Zacatecas—, pues

gracias a su esfuerzo y dedicación ha sido posible conformar el presente volumen.

Indudablemente, con su valiosa participación han demostrado su compromiso para fomentar una mayor concientización de la importancia de la protección de los datos personales y la privacidad en esta era digital. Sin importar el lugar y el contexto social y cultural, el imperativo de garantizar la eficaz protección de estos derechos humanos es la misma en toda la nación. Enhorabuena.

# PRÓLOGO

FRANCISCO JAVIER ACUÑA LLAMAS

*Comisionado del INAI*

Siempre resulta un privilegio redactar unas líneas para prologar un libro. Especialmente, cuando la obra se dedica a una temática que reclama toda nuestra atención como sociedad democrática; hablamos de dar contexto al derecho del Siglo XXI: el derecho a la privacidad.

La obra de mérito contiene una relatoría. En ella se recoge de modo selecto la esencia de las intervenciones de expertos más representativos de Iberoamérica, las voces más autorizadas en la protección de la vida privada a partir de los Datos Personales.

Hablamos de aquellos datos personales: tanto aquéllos en posesión de las instituciones y las dependencias públicas, como de aquellos bancos de datos que por cualquier razón tienen particulares respecto de otros particulares.

«Ruta de la Privacidad» es el título de un proyecto institucional que imaginaron y pusieron en marcha mi compañera comisionada del INAI, Josefina Román, y nuestro colega Rodrigo Arístides Guerrero, comisionado Presidente del INFO CDMX, coordinador de la comisión de Datos Personales del Sistema Nacional de Transparencia.

La idea de la Ruta de la Privacidad obedece a una necesidad pragmática: abrir un camino en la espesa indiferencia social sobre la conciencia crítica del valor de la información confidencial que descuidamos y que sin control se dispersa y se derrama por la cada vez más amplia vida digital que en paralelo a la existencia física vamos desarrollando minuto a minuto al transpirar y respirar en la era digital. Situación a la que fuimos arrojados sin advertencias. Simplemente fuimos empujados por la corriente tecnológica de la que somos contribuyentes pasivos y a la vez usuarios cautivos. El programa «Ruta de la Privacidad» es un ejercicio que, si bien ha tenido éxito, debemos ver como un proyecto de largo aliento, un semillero de

actualización y guía que ilumine a quienes en él participamos, de cualquier forma, como expertos o aprendices. Eso se convertirá en un laboratorio de reflexiones y debates permanentes, como los que se han creado los observatorios científicos para muy diversas temáticas.

Ahora bien, para efectos de alumbrar la arquitectura de un libro como el que estamos explicando de modo sintético —repito a manera de prólogo—, discurrimos por el estrecho camino que nos conduce a profundizar en esta asignatura todavía muy reciente entre nosotros.

Esta obra, sin con ello demeritar el acierto del título que lleva, podría también haberse denominado: *La senda de la vida privada en la era digital*. Lo que más importa es que, llamémosle como le llamemos, nos conduzca al mismo destino: el urgente sendero hacia la autodeterminación informativa, la cima de la autonomía y la suficiencia individual para decidir el cuándo, el cómo y el hasta dónde colocamos nuestros signos de vida, en tanto sabemos que casi todo lo que hacemos, decimos, sentimos y pensamos se traduce en una referencia digitalizada susceptible de ser aglutinada y descifrada. Tenemos cada vez menos vida real libre de interferencias tecnológicas que invariablemente, como las aguas de un río, se reúnen en el océano: en lo que antes era la vida propia de cada uno se ha edificado un monitor que nos persigue como sombra durante el día y como pesadilla por la noche. Experimentamos la sujeción digital, somos tributarios de una cobertura que nos vigila y marca nuestras palpitaciones en la pantalla digital. Hemos abandonado el mundo aquel que nos vio nacer a los que somos del siglo pasado; en aquella época todo lo que ahora vemos era una simple sospecha de ciencia ficción. A diferencia de nuestros jóvenes, «los nativos digitales», el impacto de las tecnologías intrusivas en la vida diaria nos causó perplejidad y hasta frustración; los altibajos de las habilidades digitales recién adquiridas nos juegan constantes bromas pesadas. Un día sabemos navegar en algunas aplicaciones y nos sumergimos en las redes sociales con cierto aire de triunfo, y otro día comprendemos la inestabilidad de las mareas tecnológicas y la falta de un criterio instintivo para descubrir alternativas a cada problema con los dispositivos y su uso adecuado.

El libro que estamos prologando anuncia el despertar de este movimiento de corte interinstitucional con un claro comportamiento académico para tratar de simplificar las complejidades de los conceptos y la trama de la teoría de la tutela de los datos personales en términos jurídicos y administrativos. La iniciativa del libro es parte del proyecto a largo plazo porque urge construir doctrina que sugiera acciones concretas; lo mismo nuevas y mejores normativas y más amplias decisiones jurisprudenciales para asistir realmente la defensa de la privacidad como un bien jurídico

objetivo de una tutela. El INAI y sus similares locales deben garantizar la protección de la vida privada a partir de los datos personales y sólo de manera omnicomprensiva y complementaria podrán conseguirlo.

Además se coloca en el punto de partida de una metodología para que todos y todas comprendamos mejor el significado de la ingente tarea que debe haber en torno a los registros de nuestra vida. Además, de la proporción de aquélla que consideramos exclusiva de nosotros aunque inconscientes de los peligros que rodean y acosan esa zona aparentemente reservada a nuestro arbitrio: es porosa a las invasiones inimaginables que, especialmente, amenazan las tecnologías de la información con su poderosa intervención en cada uno de nuestros movimientos corporales, emocionales, fisiológicos y espirituales.

La vorágine de las tecnologías de la información absorbe cada instante y de manera aislada, aunque los tratará de reagrupar, los rasgos y señas del libre desarrollo de la personalidad y la gama de aspectos que colindan con nuestra esfera de intimidad y aquellas extensiones de aquella atmósfera de nuestras relaciones humanas y sociales. La privacidad es una palabra polisémica: abarca campos diversos de la vida de cada persona. La privacidad no es un ambiente o un paisaje humano: se circunscribe a la individualidad. Que existan condiciones precisas y apropiadas para su garantía no la convierte en una suerte de cobertizo o burbuja para cobijar o incluir a las personas en general. Al final, las batallas por defender nuestra privacidad contra todo y contra todas las formas de interferencia es y será una experiencia individual a la que no podremos llegar sin conocimiento previo y hasta con una estrategia por sencilla o simple que parezca.

Acaso la mayor y mejor de las razones para aprender a defender nuestra privacidad sea el pretexto que nos lleve a seguir sufriendo los trances de cada experiencia digital para intentar ordenar lo que ya es —aun sin nuestro conocimiento y, menos aun, nuestro pleno consentimiento— la era de la supervivencia digital; porque, repito, fuimos aventados a sus misterios e incógnitas. Me emociona que el INAI sea el medio para esta empresa editorial que se convertirá en una vía para animar los deberes institucionales en aras de la tarea incesante de difundir el valor de los datos personales y la fragilidad de nuestra privacidad.

# BIENVENIDA

JOSEFINA ROMÁN VERGARA

*Comisionada del INAI*

Tradicionalmente, se había hablado muy poco en lo que se refiere al rol y participación de los organismos garantes en la protección y tutela del derecho a la protección de datos personales cuando, desde 2009, se le reconoció como derecho humano constitucional con la reforma al artículo 16 de la Carta Magna. No obstante, desde años anteriores a la mencionada reforma constitucional, los organismos garantes vislumbramos como objetivo que todas y todos los mexicanos pudieran ejercer plena y libremente el derecho a la protección de datos personales; esto ante el abrumante crecimiento de las tecnologías de la información.

La Ruta de la Privacidad ha continuado esa misión. Desde la conmemoración del Día Internacional de Protección de Datos Personales, en enero de 2022, los organismos garantes del país emprendieron un proceso de institucionalización de este derecho humano. Así, a la fecha, 14 órganos del país se han sumado a este esfuerzo de socialización de la cultura de la protección de datos personales. En seguimiento a ese impulso, esta obra pretende socializar y difundir entre el público, expertos, autoridades y cualquier persona las experiencias compartidas por los Ponentes nacionales e internacionales, tendientes a alcanzar el uso ético y armónico entre el derecho a la protección de datos y la inteligencia artificial, en el cual creemos conciencia sobre la corresponsabilidad, los responsables y titulares que la implementan. Esto, a su vez, para que, desde la voz de los organizadores, reflexionemos sobre el impacto de esta cruzada en el fortalecimiento del Sistema Nacional de Transparencia y la política nacional en la materia.

Estoy segura de que la inclusión de todas las voces en la presente obra es fundamental para continuar con la consolidación de la autodeterminación informativa, posicionándolo como un instrumento que permita alcanzar un México más justo y democrático.

# MENSAJE

LUZ MARÍA MARISCAL CÁRDENAS

*Comisionada Presidenta del IDAIP y Coordinadora de Organismos Garantes de las Entidades Federativas del SNT*

El hecho de que el manejo de nuestra privacidad se enfrente a la adaptación del nuevo orden digital que está regulando nuestras vidas, impactando en muchos ámbitos como los institucionales y los comerciales, nos debe replantear la importancia de proteger nuestros datos personales como un asunto de vital prioridad. En ese sentido, esta cruzada nacional que se realizó a través de la Ruta de la Privacidad impulsada por el INAI, en coordinación con los órganos garantes que conformamos el Sistema Nacional de Transparencia, cumplió con el objetivo de socializar y concientizar sobre este derecho humano a la protección de los datos personales, ante la presencia de la inteligencia artificial y el uso de las redes sociales, el internet, las operaciones *online* y todas las plataformas digitales.

Estas Memorias son, sin duda, un producto editorial que nos permitirá compartir las experiencias y el conocimiento que generó esta cruzada que llegó a todo el país, por medio de las Regiones Norte, Centro-Occidente, Centro y Sureste del SNT. Además, tendrá la recopilación de discursos, posicionamientos, experiencias y un gran acervo de contenidos que nos han compartido voces expertas en el tema.

La reflexión es clara: Hoy nuestros nombres, domicilios, claves de cuentas bancarias, información sensible de nuestras vidas y prácticamente toda nuestra privacidad están más vulnerables que nunca ante la nueva normalidad, el acelerado crecimiento del mundo digital y la presencia de la inteligencia artificial.

Esta ruta debe continuar su marcha, en virtud de que la protección de los datos personales es un asunto prioritario en México, porque no sólo está en juego la identidad de los individuos, sino también el patrimonio, la seguridad y la tranquilidad de las personas y sus familias.

# SURGIMIENTO

ARÍSTIDES RODRIGO GUERRERO GARCÍA

*Coordinador de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia*

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

La Ruta de la Privacidad es un proyecto que surge ante la necesidad de visibilizar el derecho a la protección de los datos personales en las diversas entidades federativas del país, a través de la colaboración institucional entre los diversos órganos garantes, locales y nacional.

En el ámbito internacional, el 28 de enero de cada año se conmemora el Día Internacional de Protección de Datos Personales. Sin embargo, y a pesar de la importancia de dicha fecha, resultaba fundamental tener una actividad de carácter permanente que permitiera llevar a todos los rincones del país la importancia de la tutela del derecho a la protección de los datos personales: a partir de ello surge el proyecto denominado la Ruta de la Privacidad.

La Ruta de la Privacidad se ideó como un mecanismo para dar a conocer los derechos que los protegen, poner sobre la mesa la necesidad de leyes actualizadas y dar a conocer a la población temas de actualidad que convergen con el derecho a la protección de datos personales; máxime que, a raíz de la pandemia por COVID-19, nuestra vida física ha ido transitando al mundo digital. Posteriormente, la *Ruta* cobró fuerza como un ejercicio de federalismo cooperativo, concepto que cobra sentido cuando se acude a su raíz alemana: *Politikverflechtung*: es decir, entrelazamiento político.

A través de este entrelazamiento institucional entre el INAI y los órganos garantes locales, se ha logrado la materialización de la Ruta de la Privacidad en diversas entidades federativas como Yucatán, Estado de

México, Ciudad de México, Hidalgo, Chihuahua, Nuevo León, Veracruz, Michoacán, Guerrero, Quintana Roo, Tlaxcala, Querétaro, Oaxaca, Zacatecas y Guanajuato, así como actividades confirmadas en Durango, Sonora y Chiapas para finales del presente año.

De esta manera, y al igual que como sucede con la Semana de la Transparencia, con actividades de manera anual, se tiene el objetivo de consolidar a la Ruta de la Privacidad como una actividad permanente del Sistema Nacional de Transparencia y Protección de Datos Personales, mediante la realización de diversos eventos en todo el país.

La presente obra tiene como objetivo coadyuvar en la consolidación de la cultura de protección de datos personales, extender el conocimiento en la materia, y visibilizar la importancia de garantizar uno de los bienes más preciados de toda persona: su intimidad. Para ello, fueron recopilados cada uno de los temas presentados en las diferentes *Rutas* celebradas hasta la fecha, a partir de tres ejes temáticos: «Inteligencia artificial y la protección de datos personales», «La inteligencia artificial y sus implicaciones prácticas» y «Fortalecimiento Institucional».

En este sentido, y a manera de preámbulo, cabe señalar que en las diferentes mesas y foros de reflexión se ha hecho patente, entre otros aspectos, que las leyes respectivas, y en especial la *Ley Federal de Protección de Datos Personales en Posesión de Particulares*, requieren de manera urgente diversas reformas o actualizaciones; que resulta necesario contar con mecanismos que atiendan, de manera eficaz, los retos que se nos presentan como personas usuarias de las redes digitales y de los cuales ha dado cuenta la Ruta de la Privacidad; y que cada vez surgen temáticas cuya comprensión y socialización se vuelven indispensables: inteligencia artificial, ciberseguridad, gobierno electrónico, ciudades inteligentes y derechos de personas en situación de vulnerabilidad, sólo por mencionar algunos ejemplos.

De esta manera, la Ruta de la Privacidad tiene el reto de mantenerse año con año, con la finalidad de seguir poniendo en el centro del debate la importancia de la protección de los datos personales y la cultura de la privacidad, siempre con la mira en la colaboración institucional entre los órganos garantes de todo el país.

# RUTA de la PRIVACIDAD

# EJE TEMÁTICO I

## *INTELIGENCIA ARTIFICIAL Y PROTECCIÓN DE DATOS PERSONALES*

# PROTECCIÓN DE LOS DATOS PERSONALES E INTELIGENCIA ARTIFICIAL

OSCAR R. PUCCINELLI

*Vicepresidente de la Red Académica Internacional de Protección de Datos y Acceso a la Información Pública*

Doctor en Derecho Constitucional por la Facultad de Derecho de la Universidad de Buenos Aires. Doctor y profesor honorario en diversas universidades latinoamericanas.

Profesor de grado y de posgrado de Derecho Constitucional, Derechos Humanos y Derecho Procesal constitucional y transnacional en diversas universidades de su país y del exterior.

Autor de numerosas obras como autor, coautor y colaborador, destacándose entre sus libros de autoría exclusiva *Derechos Humanos y Sida* (Depalma, 1993); *Habeas Data en Indoiberoamérica* (Temis, 1999); *Protección de datos de carácter personal* (Astrea, 2003) y *Juicio de Hábeas Data* (Hammurabi, 2016).

Miembro de la Red Global de Derechos Humanos Digitales (GDHRNet) y vicepresidente de la Red Académica Internacional de Protección de Datos y Acceso a la Información Pública, entre otras organizaciones académicas y no gubernamentales. Juez de la Sala Segunda de la Cámara de Apelación en lo Civil y Comercial de Rosario, Argentina.

## *La inteligencia artificial: un producto cultural humano*

Los humanos están definidos no sólo por los aspectos biológicos, sino también por los culturales. La cultura es forjada a través del pensamiento, que es un producto de la inteligencia, y ésta se nutre y progresa a través de la cultura, en una suerte de retroalimentación permanente (*v.gr.*, el lenguaje y la escritura como productos de la inteligencia inciden a la vez en su desarrollo).

Como lo predijera Descartes en 1637, al sostener que en el futuro existirían máquinas que pensarían por sí mismas, los avances tecnológicos han permitido emular algunas de las habilidades cognitivas humanas —que entre las básicas y las superiores cuentan las de razonamiento, memorización, percepción, atención, comprensión, lenguaje, aprendizaje, abstracción, pensamiento lateral, metacognición, motivación, planificación, autorregulación, evaluación, anticipación, reorganización, creación, emoción e inteligencia emocional —dando paso a lo que McCarthy denominó «Inteligencia artificial» (IA), definiéndola como «la ciencia e ingenio de hacer máquinas inteligentes, especialmente programas de cómputo inteligentes» (1956).

Actualmente, la IA puede ser entendida como «la capacidad de un sistema para interpretar correctamente datos externos, para aprender de dichos datos y emplear esos conocimientos para lograr tareas y metas concretas a través de la adaptación flexible» (Kaplan y Haenlein), e incluye una variedad de técnicas computacionales y de procesos enfocados a mejorar la capacidad de las máquinas para realizar ciertas actividades; especialmente a partir del uso de algoritmos (el conjunto de reglas o secuencias de operaciones lógicas que les proporcionan instrucciones para que tomen decisiones o actúen de determinada manera).

Partiendo del silogismo de Aristóteles —entendido como medio del conocimiento científico a través de premisas que permiten llegar a conclusiones racionales— y el muy posterior vaticinio de Descartes, los antecedentes históricos de la inteligencia artificial moderna son bien conocidos. Entre ellos, las ideas de Boole sobre la sistematización del pensamiento lógico (1847), el desarrollo de Frege de la lógica del primer orden (1877), la conceptualización del algoritmo y el test de Turing (1936 y 1950), las leyes de la robótica de Asimov (1941), el modelo de neuronas artificiales de McCulloch y Pitts (1946), el «Perceptrón» de Rosenbaltt, primer algoritmo aplicado a un *software* (1957), el *chatbot* «Eliza» de Weizenbaum (1966), el primer lenguaje de programación para robots (Wave) del Stanford Research Institute (1973); los 12 requisitos de Fischles y Firschein para establecer si un agente es inteligente (1987), la Deep blue de IBM aplicada al ajedrez (1997), el *bot* conversacional «Eugene Goostman» (2001), la aplicación de Google de reconocimiento de voz (2008), la «Watson» de IBM (2010), el AlphaGo de Google Deepmind (la Deep Blue del Go) (2015), y una familia de modelos de lenguaje neuronal conversacional desarrollada por Google, LaMDA (Language Model for Dialogue Applications), que habría alcanzado a adquirir —según un ingeniero de la compañía— conciencia de sí misma (2022).

En este contexto evolutivo, y a partir de su infinita posibilidad de aplicaciones, la IA se ha convertido en una herramienta esencial para el desarrollo humano. Pero, como toda herramienta compleja, puede producir efectos negativos sobre los derechos de las personas.

## *IA y protección de datos*

Desde que la escritura permitió representar gráficamente el lenguaje, se comprendió rápidamente que el despliegue de la inteligencia humana sería mucho más eficiente si se apoyaba en repositorios de información, como puede observarse de la creación de los antiquísimos archivos del Palacio de Ebla (Siria, 2.500 a.C.) y de la temprana afirmación de Aristóteles acerca de que los archivos resultaban indispensables en el Estado Modelo.

Esta correlación entre información e inteligencia también aplica a los sistemas de IA, que requieren cantidades ingentes de información para funcionar, que pueden incluir datos personales (v.gr., no son necesarios en la robótica aplicada a procesos industriales, pero sí para un *chatbot* de una empresa de servicios), en cuyo caso los fabricantes del *software*, dispositivo o producto de la IA deben respetar las normas dictadas a este respecto, en especial las de factura reciente dictadas precisamente porque el notable incremento del uso de la IA y sus nuevas aplicaciones se verificaron a partir de los avances tecnológicos que posibilitaron el desarrollo de la web 2.0, las redes sociales, el internet de las cosas, la computación en la nube y los datos masivos.

Los escenarios donde el uso de la IA genera los mayores riesgos para las personas se presentan cuando los sistemas dotados de IA pueden generar perfiles y tomar decisiones automatizadas a partir del *machine learning*, donde los sistemas, al procesar los datos disponibles aprenden por sí mismos, ajustando los *per se* los algoritmos, y del *deep learning*, donde se emula el enfoque de aprendizaje de las personas humanas para obtener ciertos tipos de conocimiento más complejos y abstractos.

El *machine learning* —vigorizado por el *big data* y el *IoT*— acarrea problemas no menores, puesto que no sólo pocas veces se conoce cómo la IA correlaciona y pondera la información para obtener el resultado —lo que genera una suerte de caja negra o *black box*, afectando el principio de transparencia—, sino que además ese aprendizaje puede estar contaminado por sesgos humanos que conllevan el «sesgo algorítmico» o *machine bias* (que puede ser de tipo estadístico, cultural, cognitivo o multifactorial), y puede traer consecuencias discriminatorias (*v.gr.*, cuando en 2015 una

afroamericana vio etiquetada su fotografía en Google Photos como «gorila» y cuando en 2016 el *chatbot* «Tay» de Microsoft, al responder a preguntas de los usuarios, publicó tuits empatizando con Hitler, el holocausto y posiciones antifeministas). Otros riesgos relevantes —ya no proveniente de los sistemas, sino del obrar humano— se relacionan con la elaboración inconsentida de perfiles y su uso con finalidades ilegítimas, como ocurrió con el escándalo Facebook-Cambridge Analytica, con el uso de análisis predictivos sobre 87 millones de usuarios de la red social con fines de manipulación comunicacional en el contexto de la elección presidencial estadounidense de 2016.

Desde luego, estos y otros riesgos sobre los derechos de las personas han sido objeto de múltiples regulaciones generales y específicas que intentan potenciar la utilización de la IA pero dentro del marco de los principios de la protección de datos, entre los cuales se encuentran especialmente involucrados los tradicionales de legalidad, consentimiento, finalidad, proporcionalidad, calidad, seguridad y nivel de protección adecuado en las transferencias internacionales de datos, como también los más recientes de transparencia, privacidad desde el diseño y, por defecto, prevención a través de estudios de impacto y *accountability*.

Actualmente existen innumerables regulaciones, recomendaciones, informes, comunicaciones y resoluciones tanto globales como regionales y locales de todo tipo y fuente, de modo que por razones de espacio nos limitaremos a mencionar las más relevantes en el sistema europeo e interamericano.

Son regulaciones señeras al respecto en el ámbito europeo, entre otras: *a*) el *Reglamento General de Protección de Datos* de la UE 2016/679 (RGPD); *b*) las Directrices del WP29 sobre decisiones individuales automatizadas y elaboración de perfiles a los efectos del RGPD; *c*) diversos documentos adoptados por la Comisión Europea desde 2018 (comunicaciones, COM(2018)0237; COM (2018)0795 y COM(2019)0168, estudio del 20/11/20 e informes, COM(2020)0064); *d*) la propuesta de Reglamento del Parlamento Europeo y del Consejo, del 21/04/21, sobre normas armonizadas en materia de inteligencia artificial (COM(2021)0206); *e*) diez Resoluciones del Parlamento Europeo de 16/02/17, 12/09/18, 12/02/19, 12/02/20, 20/10/20, 20/01/21, 20/05/21, 25/03/21, 19/05/21, 06/10/21 y 03/05/22); *f*) once estudios de la Dirección General de Políticas Interiores de la Unión (DG IPOL), desde 2021; *g*) 15 estudios de los Servicios de Estudios Parlamentarios (EPRS), desde 2020; *h*) seis documentos de trabajo de la Comisión Especial sobre Inteligencia Artificial en la Era Digital (AIDA), desde 2021; *i*) un informe de la Comisión Especial sobre Inteligencia Artificial en la Era

Digital (A9-0088/2022); *j*) varios informes del Grupo de expertos de alto nivel sobre inteligencia artificial (08/04/19, 26/06/19); del Grupo de expertos sobre responsabilidad y nuevas tecnologías (21/11/19) y de la Agencia de los Derechos Fundamentales de la Unión Europea (14/12/20), y *k*) una recomendación de la OCDE (22/05/19), entre muchos otros documentos y publicaciones que están revistadas en la Resolución del Parlamento Europeo, del 03/05/22, sobre la inteligencia artificial en la era digital —2020/2266(INI)—.

En el ámbito iberoamericano, además de los múltiples documentos emanados de las agencias de protección de datos, merecen mención tres documentos de la RIPD: los *Estándares de Protección de Datos Personales para los países iberoamericanos*, las *Recomendaciones generales para el tratamiento de datos en la inteligencia artificial* y las *Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de Inteligencia Artificial*. Precisamente, en las recomendaciones, además de aconsejarse el cumplimiento de las normas sobre tratamiento de datos personales, se insta a efectuar estudios previos de impacto en la privacidad, incorporar la privacidad, la ética y la seguridad desde el diseño y, por defecto, materializar el principio de responsabilidad demostrada, diseñar esquemas apropiados de gobernanza sobre el tratamiento de datos personales en las organizaciones que desarrollan esos productos de IA, adoptar medidas para garantizar los principios sobre tratamiento de datos personales en los proyectos de IA, respetar los derechos de los titulares de los datos e implementar mecanismos efectivos para su ejercicio, asegurar la calidad de los datos personales, utilizar herramientas de anonimización e incrementar la confianza y la transparencia.

Queda mucho todavía por recorrer y regular, pero estos recientísimos documentos constituyen las bases más sólidas y autorizadas a la hora de enmarcar estos avances tecnológicos dentro del debido respeto a los derechos humanos.

# PROTECCIÓN DE DATOS PERSONALES Y USO DE TECNOLOGÍAS

PABLO CORONA FRAGA

*Vicepresidente para Ciberseguridad de la Asociación de Internet MX*

Director de desarrollo de negocios en NYCE. Maestro en Administración de TI, Ingeniero en Sistemas Computacionales. Editor de la norma ISO/IEC 27001:2022. Vicepresidente para ciberseguridad en la Asociación de Internet MX y para Gobierno, riesgo y cumplimiento en el Consejo Mexicano de Seguridad de Información y Ciberseguridad. Profesor en la Universidad Iberoamericana, Maestría de Gobierno de las Tecnologías de Información y en INFOTEC, Maestría en Derecho las Tecnologías de Información. Autor del libro *Guía práctica para la gestión de riesgos en la era de la ciberseguridad* y el compendio *Practicum Ciberseguridad 2022*. Miembro del Comité Técnico Asesor del PREP para el proceso electoral 2018, extraordinario 2019 y 2021 en el Instituto Nacional Electoral (INE). Editor y redactor de iniciativas de cumplimiento para la LFDPPP.

Auditor líder certificado en Sistemas de Gestión de Seguridad de la Información, Gobernabilidad de TI, Gestión de Riesgos y Continuidad de Negocio.

La protección de datos personales es un derecho que ha tomado relevancia recientemente, en particular con el advenimiento de las redes sociales y el avance de tecnología que permiten dar trazabilidad a los hábitos de los usuarios, almacenar y procesar grandes cantidades de información en equipos de costo bajo, el procesamiento de esos datos con aplicaciones de inteligencia artificial, aprendizaje automatizado y *Big Data*, así como la facilidad con que los usuarios hemos adoptado estas tecnologías. De esta forma, los nuevos modelos de negocios ya no siempre se basan en pago por Servicios en una moneda corriente: ahora muchas aplicaciones y servicios brindan su acceso y uso

a cambio de que el usuario permita que se recaben sus datos personales y, en ocasiones, los de sus contactos o conocidos.

Debemos ver a la protección de datos personales como un asunto más allá de proteger datos, pues se trata de proteger también los derechos y garantías individuales de la persona, que debe ser el centro del tratamiento y quien decida sobre a quién se le proporcionan sus datos y qué se hace con ellos. Si bien en México existen dos regulaciones, una aplicable a la iniciativa privada y otra a la administración pública, esta última no está exenta de la obligación de proteger esos datos y, con ellos, los derechos de sus titulares. Si bien su reclamación y tratamiento en muchos casos no es opcional, pues se basa en un mandato legal para la prestación de un servicio a la ciudadanía, es de suma relevancia que esos datos personales sean adecuadamente protegidos a través de medias de seguridad físicas, administrativas y técnicas que eviten vulneraciones en su tratamiento, como el acceso, uso, modificación y eliminación no autorizados.

En este sentido, México fue uno de los países pioneros en la implementación de modelos de autorregulación vinculante en materia de protección de datos personales, contando con el primer Sistema de certificación reconocido por las autoridades competente en la materia; en este caso, la Secretaría de Economía como Autoridad Reguladora y el INAI como Autoridad Garante. Dentro de estos esquemas de autorregulación se encuentra la certificación de sistemas de gestión de datos personales, que es llevada a cabo por entes de tercera parte, que hacen el proceso más robusto y brindan seguridad y confianza de que la evaluación se ha llevado de forma imparcial y se han evaluado no sólo el diseño documental del Sistema de gestión, sino también la implementación, mantenimiento y mejora continua de los procesos que dan soporte al tratamiento de datos personales, así como a los controles de seguridad que refuerzan el tratamiento legítimo, controlado e informado de los datos personales, y la atención a los ejercicios de derechos ARCO.

Este caso —donde México tuvo una regulación de datos personales de acuerdo con los nuevos modelos, aún antes de otras regulaciones como GDPR— permitió la generación de lecciones aprendidas, así como la adopción y establecimiento de buenas prácticas que posicionaron a México como un referente importante a nivel internacional. De hecho, la norma ISO/IEC 27701, que está enfocada en establecer controles que extiendan los alcances de un Sistema de Gestión de Seguridad de la Información para considerar la protección de los datos personales y la privacidad de los titulares, tuvo referentes en el modelo mexicano y se ha convertido en un caso de éxito tanto a nivel regional como internacional. De este

modo hoy, a través de la certificación en esta norma, se puede demostrar cumplimiento con los esquemas de autorregulación y a su vez con los principios, deberes y obligaciones contenidos en la Ley, su reglamento y demás regulación secundaria en la materia, pero además permite dar cumplimiento a las obligaciones establecidas en otras regulaciones: por ejemplo las aplicables en la Unión Europea a través de GDPR.

Las prácticas contenidas en estos modelos de gestión para la protección de datos personales incluyen prácticas como:

- Realizar un inventario de datos personales que permita dar trazabilidad al tratamiento de los datos a través de los datos sistemas de tratamiento y las personas que lo realizan a lo largo de todo su ciclo de vida;
- Establecer roles, funciones y responsabilidades del personales y organizaciones subcontratadas con respecto del tratamiento de los datos personales;
- La asignación de recursos económicos, materiales, humanos, así como organizacionales, para llevar a cabo las acciones definidas por el sistema de gestión;
- Realizar un análisis de riesgos sobre los eventos y consecuencias que puedan llevar a comprometer los datos personales;
- Llevar a cabo un análisis de impacto a la privacidad que identifique la finalidad y proporcionalidad del tratamiento de los datos personales, justificando su tratamiento y minimizando su obtención así como su período de retención;
- Determinar medidas de seguridad administrativas, físicas y técnicas para atender los riesgos identificados en el análisis de impacto a la privacidad y el análisis de riesgos;
- Llevar a cabo revisiones y auditoria para identificar posibles desviaciones en la implementación de las acciones definidas;
- Mantener y mejorar continuamente el sistema de gestión, implementado acciones correctivas y de mejora según sea conveniente.

Todas estas acciones deben considerarse en constante revisión y actualización, ya que los avances en la relación, la tecnología, así como en las amenazas y los agentes que pueden llevar a cabo una vulneración están en constante cambio y evolución.

Actualmente, el uso de herramientas de reconocimiento de rostro y otros datos biométricos permiten identificar a una persona con muy alto nivel de certidumbre. Esto tiene usos loables para el control de accesos a edificios, identificación de criminales, prestación de servicios de salud, etc. Pero también pueden ser utilizados como medidas represivas, de

segmentación, discriminación y de coerción de los derechos humanos. De esta forma debe mantenerse un balance entre los beneficios del uso de las tecnologías, con las posibles consecuencias que puede tener una vulneración en el impacto a la privacidad y los derechos de los titulares. Para esto, la implementación de controles como la disociación, segmentación y cifrado de los datos, así como la autenticación de las personas y dispositivos, la autorización de las acciones a ejecutar de acuerdo con los roles permisos y privilegios que deben tener de acuerdo con sus funciones, y el monitoreo contante del tratamiento de los datos para identificar, proteger, contener, responder y recuperarse ante incidentes son acciones básicas que toda organización debe implementar.

# ÉTICA Y MARCO REGULATORIO

CARLA VÁZQUEZ WALLACH

*Directora General Legal + Innovation Consulting*

Cuenta con más de 25 años de experiencia en el entorno corporativo. Se ha desarrollado como emprendedora, abogada, servidora pública, consultora de política pública y socia.

Lideró proyectos de innovación de empresas con presencia internacional y equipos de emprendedores en el diseño de herramientas LegalTech, obteniendo el reconocimiento de la Barra Mexicana de Abogados, Capítulo Baja California, y en el Foro Asia Pacífico (APEC).

Como servidora pública participó en la modernización del Tratado de Libre Comercio con la Unión Europea y la Agenda Digital de Alianza Pacífico para incluir mejores prácticas sobre el uso y reconocimiento transfronterizo de la firma electrónica e identidad digital.

Su búsqueda por la innovación responsable le ha permitido participar en iniciativas del Consejo de la Judicatura Federal, Banco Interamericano de Desarrollo, gobiernos estatales, así como en el desarrollo de guías y estudios sobre el uso ético de la inteligencia artificial y protección de datos.

En este momento histórico donde la realidad nos exige reflexionar sobre el aspecto ético del uso de la tecnología en relación con la protección de los datos, recordé a Ronald Dworkin quien desde su perspectiva obliga a preguntarnos sobre el Derecho como herramienta social y política, el autor nos lleva a reflexionar cómo desde la ética (algo abstracto y general) surge la moralidad personal, de la cual surge la moralidad pública y, de ella, el Derecho[1].

Recuerdo que, en 2000, Dworkin presentó a la comunidad jurídica de la Ciudad de Nueva York el artículo *¿Deben nuestros jueces ser filósofos?*

[1] Moreso, José Juan y Queralt, Jahel, «Bosquejo de Dworkin: la imbricación entre el Derecho y la moralidad», *ISONOMÍA* N.° 41, octubre 2014, pp. 143-174.

*¿Pueden ser filósofos?*[2]. En ese entonces, el autor planteó una serie de dilemas controversiales (aborto, estado de interdicción, eutanasia, entre otros), los cuales podían ser resueltos de diversas maneras y considerando enfoques de diferentes disciplinas del conocimiento. Sin embargo, este autor concluye que en realidad estos dilemas descansan en la reflexión de valores y no de hechos, y es justo ahí donde se encuentra la necesidad de incluir en el debate la filosofía moral y política.

Al analizar la convergencia del uso de la inteligencia artificial y la protección de datos a casos concretos, los retos éticos y morales se multiplican para los entes reguladores, así como para los jueces y los usuarios. Es común encontrarnos la constante tensión entre los derechos y principios[3], y ello nos obliga a cuestionarnos sobre las asimetrías naturales de las relaciones jurídicas.

De acuerdo con la UNESCO[4], la inteligencia artificial es uno de los temas centrales de la era de las tecnologías convergentes con un doble matiz. Mientras se identifica el potencial de esta tecnología como precursor social, también se le relaciona con riesgos para los humanos, las culturas, las sociedades y el medio ambiente, entre otros. Esta dualidad ofrece una serie de aristas que plantean la necesidad de crear mecanismos que regulen los alcances de la inteligencia artificial desde una perspectiva ética, así como requisitos o elementos mínimos que permitan mitigar sus efectos en perjuicio de los humanos basados en valores y principios generalmente aceptados.

La inteligencia artificial invariablemente requiere el procesamiento de grandes cantidades de datos cuyo tratamiento debe protegerse bajo la dimensión íntima de las personas. Particularmente por los impactos que podrían provocar, tanto en la toma de decisiones como por el entrenamiento que se haga respecto de los datos y que con ello se magnifiquen desigualdades y brechas existentes.

[2] Dworkin, Ronald, *¿Deben nuestros jueces ser filósofos? ¿Pueden ser filósofos?*, traducción del texto *Must our judges be philosophers? Can they be philosophers?*, presentado en la Conferencia en Nueva York el 11 de octubre de 2000, honrando el nombramiento como Scholar of the Year del Cionseho Neoyorkino para las Humanidades.

[3] Por ejemplo, tensión entre el derecho a la intimidad y la libertad de expresión, el que difunde cierta información debe estar consciente si esto le representará un daño en la esfera más íntima de una persona.

[4] UNESCO, Consejo Ejecutivo, 206a reunión, 206 EX/42, 28 de marzo de 2019, publicado en https://unesdoc.unesco.org/ark:/48223/pf0000367422_spa

Esto se traduce en la supervisión de soluciones tecnológicas tanto del sector público como del sector privado, en función del potencial riesgo que puedan llegar a provocar para con los usuarios[5].

Cabe recordar que en 2021 se adoptó la primera *Recomendación global sobre el uso de la inteligencia artificial en el marco de la* UNESCO, la cual reconoció la necesidad de integrar los valores y principios que deben seguir los Estados para desarrollar un marco normativo dirigido al desarrollo fiable de la inteligencia artificial, lo cual sin duda nos deja la tarea de profundizar internamente para construir un marco equilibrado para favorecer la innovación y proteger a los usuarios en su interacción con la tecnología (cualquiera que sea su aplicación).

Sin embargo, para construir un marco regulatorio y/o autorregulatorio efectivo resulta indispensable promover la participación de los sectores privado, público y social. La realidad nos exige debatir, reflexionar, pensar en nuestra sociedad y analizar qué sucede en otras latitudes y cómo han enfrentado los retos desde diversos enfoques.

Celebro la organización del Foro del Sistema Nacional de Transparencia organizado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, que a pesar de las dificultades y limitaciones provocadas por la pandemia mantuvo el desarrollo de sus actividades para cumplir con la tutela en la protección de datos y orquestar espacios para comulgar distintas visiones sobre la creciente evolución. Un buen regulador se mantiene al tanto de las tendencias, novedades, retos y provoca el debate para alimentarse de los diversos enfoques que enriquecen su actuar para diseñar mecanismos que garanticen el respeto a los valores y principios circunscritos a su actividad regulatoria, lo cual se destaca en el INAI.

Los eventos de esta naturaleza acercan para la población en general las preocupaciones, reflexiones, debates que se están dando sobre el entorno digital, lo cual invariablemente se traduce en usuarios más informados y conscientes de los riesgos y oportunidades en el uso de la tecnología. No se busca inhibir el uso de la tecnología, sino de promover una cultura responsable en todos los involucrados (empresarios, consumidores, reguladores, investigadores). En un entorno de respeto y comunicación asertiva, se buscó compartir preocupaciones y reflexiones que ayudarán

[5] Se recomienda considerar los esfuerzos de comunidad europea para regular las soluciones de inteligencia artificial desde la perspectiva de la evaluación de riesgo. [Web oficial de la Unión Europea. «Excelencia y confianza en la inteligencia artificial», *Comisión Europea*, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/excellence-trust-artificial-intelligence_es

en el análisis de temáticas tan sensibles como la protección de los datos personales, evitando puntos ciegos que se darían si abordamos la problemática desde una sola disciplina o perspectiva.

El Foro reconoció la necesidad de conversar, genera el diálogo desde distintas perspectivas que permiten construir soluciones y dibujar una posible ruta para ofrecer a los usuarios esquemas efectivos de protección a sus datos. Esfuerzos de esta naturaleza contribuyen a construir una sociedad informada cuyo debate se lleva con orden, método y propósito, aleja las malas prácticas de la improvisación y retórica favoreciendo el análisis crítico, constructivo y apolítico.

# TRANSPARENCIA, EXPLICABILIDAD E INTERVENCIÓN HUMANA

JOSÉ LUIS PIÑAR MAÑAS

*Vicerrector de Relaciones Internacionales de la Universidad CEU de San Pablo Madrid*

Doctor en Derecho por la Universidad Complutense. Catedrático de Derecho Administrativo de las Universidades de Castilla-La Mancha y CEU-San Pablo de Madrid. Ha sido Director de la Agencia Española de Protección de Datos, Vicepresidente del Grupo Europeo de Autoridades de Protección de Datos y primer Presidente y fundador de la Red Iberoamericana de Protección de Datos.

Abogado. Of Counsel en CMS Albiñana & Suárez de Lezo, Madrid. Director del Máster Universitario en Protección de Datos y Transparencia. Universidad CEU-San Pablo. Vocal Permanente y Presidente de la Sección de Derecho Público de la Comisión General de Codificación de España. Presidió la Ponencia que elaboró el proyecto de la vigente ley española de Protección de Datos. Vicepresidente de la Sección de Derecho y TIC de la Real Academia Española de Jurisprudencia y Legislación.

Reconocido ponente en numerosos congresos internacionales y autor de numerosas publicaciones nacionales e internacionales sobre derecho público y privacidad.

«La transparencia y la explicabilidad de los sistemas de IA suelen ser condiciones previas fundamentales para garantizar el respeto, la protección y la promoción de los derechos humanos, las libertades fundamentales y los principios éticos», según la *Recomendación sobre la ética de la inteligencia artificial* de la UNESCO[6],

[6] Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura, *Recomendación sobre la ética de la inteligencia artificial*, (Francia: UNESCO, 2021). https://unesdoc.

adoptada el 23 de noviembre de 2021. Asimismo, señala que «el grado de transparencia y explicabilidad debería ser siempre adecuado al contexto y al efecto, ya que puede ser necesario encontrar un equilibrio entre la transparencia y la explicabilidad y otros principios como la privacidad, la seguridad y la protección. Las personas deberían estar plenamente informadas cuando una decisión se basa en algoritmos de IA o se toma a partir de ellos, en particular cuando afecta a su seguridad o a sus derechos humanos. En esas circunstancias, deberían tener la oportunidad de solicitar explicaciones e información al actor de la IA o las instituciones del sector público correspondientes. Además, las personas deberían poder conocer los motivos por los que se ha tomado una decisión que afecta a sus derechos y libertades». Por otra parte, la OCDE hizo públicos en 2019 unos principios de la inteligencia artificial[7], entre los que se encuentra el de transparencia y divulgación responsable.

En numerosas ocasiones he señalado que uno de los grandes peligros del derecho a la protección de datos es que su violación puede pasar desapercibida, y de hecho así es en la mayoría de las ocasiones. Podemos caer en la cuenta de inmediato de que nos han robado un bolígrafo, pero podemos no ser conscientes de que están robándonos nuestros datos, o que están manipulando nuestra identidad mediante un uso ilícito de nuestros datos o incluso lícito pero desleal[8]. Esta situación puede darse con especial virulencia en los casos en que se utilicen sistemas de inteligencia artificial que permiten, entre otras muchas cosas, perfilar a las personas y tomar decisiones que pueden afectar a sus derechos o intereses.

Precisamente la propuesta de *Ley Europea de Inteligencia Artificial* (*Artificial Intelligence Act*)[9] parte de que la inteligencia artificial puede reportar grandes beneficios para la sociedad. Por ello la propuesta «tiene por objeto inspirar confianza en los ciudadanos y otros usuarios para que adopten soluciones basadas en la IA, al tiempo que trata de animar a las empresas

unesco.org/ark:/48223/pf0000381137_spa

7 OECD Legal Instruments, *Recommendation of the Council on Enhancing Access to and Sharing of Data*, 05/10/2021. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

8 No olvidemos que el principio de lealtad en el uso de los datos es uno de los principios nucleares, configuradores del derecho a la protección de datos. A él se refiere el artículo 5 del *Reglamento General de Protección de Datos de la Unión Europea* (RGPD), como también se cita en el artículo 6 de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* o en el artículo 16 de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados.*

9 Bruselas, 21.4.2021 COM(2021) 206 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0206

a que desarrollen este tipo de soluciones». Pero tiene también en cuenta que la IA puede «generar riesgos y menoscabar los intereses públicos y los derechos», especialmente el derecho a la privacidad o a la protección de datos, por lo que prohíbe el uso de prácticas de inteligencia artificial que violen derechos fundamentales.

Para evitar o mitigar el impacto negativo en los derechos fundamentales, uno de los principios esenciales que ha de aplicarse es el ya citado de transparencia. Lo que puede plantear no pocos problemas. Entre otros, y no menor, el del alcance de la transparencia y la complejidad que puede suponer conocer aspectos técnicos del funcionamiento de los sistemas de inteligencia artificial y en particular de los algoritmos. Recientemente, la Agencia Española de Protección de Datos y el Supervisor Europeo de Protección de Datos, en un breve pero muy lúcido y esclarecedor documento conjunto, se han referido, entre otros asuntos, a ello. Señalan que «las personas deben recibir suficiente información sobre cómo se tratan sus datos personales, y los tratamientos basados en sistemas de *Machine Learning* no son una excepción». Pero advierten que «este tipo de transparencia no implica necesariamente la divulgación de información técnica detallada que, en la mayoría de los casos, no sería significativa para los usuarios». Lo que procede es ofrecer «información significativa que los haga conscientes de la lógica aplicada, así como la importancia y las consecuencias esperadas del procesamiento»[10].

Además de la transparencia, y para preservar la dignidad misma de la persona, es necesario asimismo reivindicar el principio de intervención humana. Que la sola máquina no pueda adoptar decisiones que puedan afectar a los derechos de las personas. Y que el funcionamiento de los sistemas de inteligencia artificial esté sometido a la vigilancia humana.

Transparencia e intervención humana son imprescindibles para limitar el impacto de la inteligencia artificial en los derechos fundamentales. Y de ello es consciente la normativa sobre protección de datos personales. El Reglamento General de Protección de Datos de la Unión Europea reconoce en su artículo 22 el derecho de todo interesado «a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida

[10] Agencia Española de Protección de Datos, «Malentendidos sobre el *machine learning* (aprendizaje automático)». El documento puede consultarse en https://edps.europa.eu/system/files/2022-09/22-09-20_10-misunderstandings-on-machine-learning_es.pdf y en https://www.aepd.es/es/documento/10-malentendidos-machinelearning-es.pdf. Un breve comentario del documento, por J.L. Piñar y M. Recio, en https://cms.law/es/esp/publication/documento-conjunto-de-la-aepd-y-del-sepd-sobre-10-malentendidos-y-realidades-sobre-machine-learning

la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar». Los artículos 13, 14 y 15 reconocen el derecho de los interesados a recibir «información significativa sobre la lógica aplicada [en el tratamiento], así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado». Y el citado artículo 22 reconoce asimismo a los interesados el «derecho a obtener intervención humana» por parte de quien trate sus datos personales.

Pero no sólo el RGPD reconoce tales derechos: la citada *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* permite que los interesados se opongan a que «sus datos personales sean objeto de un tratamiento automatizado, el cual le produzca efectos jurídicos no deseados o afecte de manera significativa sus intereses, derechos o libertades, y estén destinados a evaluar, sin intervención humana, determinados aspectos personales del mismo o analizar o predecir, en particular, su rendimiento profesional, situación económica, estado de salud, preferencias sexuales, fiabilidad o comportamiento».

En definitiva, la inteligencia artificial trae consigo grandes beneficios para la sociedad, al tiempo que no pocos retos. Por ello es imprescindible plantear su entero desarrollo con la perspectiva de los derechos fundamentales, y en particular el derecho a la protección de datos, cuya regulación contiene ya, al menos en la Unión Europea y en México, instrumentos que permiten controlar el desarrollo y aplicación de los sistemas de inteligencia artificial.

# INTELIGENCIA ARTIFICIAL Y TRATAMIENTO DE DATOS PERSONALES

NELSON REMOLINA ANGARITA

*Profesor Asociado de la Facultad de Derecho de la Universidad de los Andes*

Director de la Escuela de Posgrados, del *GECTI* (*Grupo de Estudios en Internet, Comercio Electrónico, Telecomunicaciones & Informática*) y del Observatorio Ciro Angarita Barón Sobre La Protección De Datos Personales de la citada Facultad. Exsuperintendente Delegado para la protección de datos personales (octubre de 2018 – marzo 31 de 2022) de la Superintendencia de Industria y Comercio de la República de Colombia (Autoridad colombiana de protección de datos personales). Ex presidente de la Red iberoamericana de Protección de datos.

Doctor *Summa Cum Laude* en Ciencias Jurídicas de la Pontificia Universidad Javeriana. Master of Laws del London School of Economics and Political Sciences. Especialista en Derecho Comercial y Abogado de la Universidad de los Andes Ganador del Premio Internacional Protección de Datos Personales de Investigación 2014, conferido por la Agencia Española de Protección de Datos (AEPD).

## *El éxito de la inteligencia artificial (IA) dependerá de la inteligencia humana*

Los creadores de productos de IA tienen una enorme responsabilidad social, ética y humana. Dotar a las computadoras con inteligencia de tipo humano ha sido un sueño de algunos desde los inicios de la computación electrónica. Aunque el término *inteligencia artificial* (IA)

fue acuñado en 1956, sus orígenes se remontan a la década de 1940[11]. La idea de este tipo de inteligencia se cristalizó en el famoso artículo de Alan Turing en 1950, *Computing Machinery and Intelligence*, en el cual se planteó la pregunta: «¿Pueden las máquinas pensar?». También propuso una prueba para responder esa pregunta, y planteó la posibilidad de que una máquina pudiera estar programada para aprender de la experiencia tanto como lo hace un humano[12].

La IA está impactando en muchos aspectos de nuestra sociedad y son inimaginables sus futuros efectos. La ola de progreso y entusiasmo por la IA se ha visto impulsada por la disponibilidad de enormes cantidades de información que es procesada por algoritmos y otras innovaciones cada vez más potentes, sofisticadas y de impacto masivo en la sociedad, la economía, la política, la salud y los negocios[13].

La IA no se crea sola. Los humanos la diseñan, crean y ponen en marcha. Por eso, de la inteligencia y ética de esas personas depende no sólo el éxito de la IA, sino también la protección de los derechos humanos de millones de personas. La mejor forma de proteger un derecho es evitar su vulneración. Por eso es necesario impedir afectaciones a los derechos de las personas. Ello implica que el diseño, desarrollo e implementación de los sistemas de IA esté orientado a cumplir, entre otras, esa finalidad preventiva.

La innovación tecnológica y la evolución acumulativa de técnicas y tecnologías han generado que la IA cada día sea más sofisticada y potente[14]. Muchas técnicas utilizadas para analizar grandes volúmenes de datos fueron desarrolladas por investigadores de IA y ahora se identifican como

[11] Warren S. McCulloch and Walter H. Pitts, "A Logical Calculus of the Ideas Immanent in Nervous Activity," *Bulletin of Mathematical Biophysics*, 5:115-133, 1943.

[12] National Science and Technology Council: Committee on Technology, "Preparing for the Future of Artificial Intelligence", *Government Report.* https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf

[13] Appendix of the AI 100 Report. Peter Stone, Rodney Brooks, Erik Brynjolfsson, Ryan Calo, Oren Etzioni, Greg Hager, Julia Hirschberg, Shivaram Kalyanakrishnan, Ece Kamar, Sarit Kraus, Kevin Leyton-Brown, David Parkes, William Press, AnnaLee Saxenian, Julie Shah, Milind Tambe, and Astro Teller, "Artificial Intelligence and Life in 2030," *One Hundred Year Study on Artificial Intelligence: Report of the 2015-2016 Study Panel*, Stanford University, Stanford, CA, September 2016, http://ai100.stanford.edu/2016-report.

[14] Pamela McCorduck, *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence*, 2nd ed. (Natick, MA: A.K. Peters, Ltd., 2004).

algoritmos y sistemas de *Big Data*[15].

El correcto desarrollo de los productos de IA traerá más beneficios[16], pero la indebida creación y desarrollo de éstos generará graves perjuicios. Por eso sigue siendo válido preguntarnos: ¿todo lo tecnológicamente posible es socialmente deseable?

## *Los datos son el alimento de la inteligencia artificial*

No existe consenso sobre la definición de la IA, pero se han señalado algunas maneras de clasificar lo que ella constituye. En un popular texto sobre el tema, *Artificial Intelligence: A Modern Approach*, se propuso la siguiente taxonomía:

- Sistemas que piensan como humanos (por ejemplo, arquitecturas cognitivas y redes neuronales);
- Sistemas que actúan como humanos (por ejemplo, razonamiento automatizado y aprendizaje);
- Sistemas que piensan racionalmente (por ejemplo, inferencias);
- Sistemas que actúan racionalmente (por ejemplo, agentes de *software* inteligentes y robots incorporados que logran objetivos mediante la percepción, la planificación, el razonamiento, el aprendizaje, la comunicación, la toma de decisiones y la actuación)[17].

La IA involucra la recolección, el almacenamiento, el análisis y el procesamiento o interpretación de enormes cantidades de información que son usados para generar diversos resultados, acciones o comportamientos por parte de las máquinas. En otras palabras, los datos son el alimento o el combustible de la IA a tal punto que podría afirmarse que un proyecto de inteligencia artificial sin datos es como un río sin agua.

[15] National Science and Technology Council: Committee on Technology, "Preparing for the Future of Artificial Intelligence," *Government Report* [...]

[16] Sobre los beneficios se sugiere leer el siguiente texto: Viola, Roberto, *Artificial Intelligence, real benefits*. (2018), Publicado en: https://ec.europa.eu/digital-single-market/en/news/artificial-intelligence-real-benefits.

[17] Stuart Russell and Peter Norvig, *Artificial Intelligence: A Modern Approach*, 3rd Edition, (Essex, England: Pearson, 2009).

## *La inteligencia artificial debe garantizar el debido tratamiento de los datos personales y el respeto de los derechos humanos*

Como es sabido, la protección de los datos personales es un derecho humano reconocido en muchas constituciones y regulaciones del mundo. Actualmente, no menos del 75 % de los países del mundo tienen regulaciones generales sobre protección de datos. El debido y ético tratamiento de datos personales es imprescindible para evitar que con el desarrollo de la IA se vean lesionados o amenazados, según el caso, los derechos humanos y la dignidad.

En línea con lo anterior, no son pocas las iniciativas y organizaciones que han trabajado para exigir el desarrollo de IA respetuoso de los derechos humanos. Veamos dos ejemplos:

En primer lugar, la Global Privacy Assembly (GPA) aprobó en octubre de 2020 la *Resolution on accountability in the development and the use of Artificial Intelligence*. Esa resolución, entre otras, insta a las organizaciones que desarrollan o utilizan sistemas de inteligencia artificial (IA) a considerar la implementación de las siguientes medidas:

- Evaluar el posible impacto en los derechos humanos (incluida la protección de datos personales y los derechos de privacidad) antes del desarrollo y/o uso de la IA;
- Probar la solidez, confiabilidad, precisión y seguridad de los datos de la IA antes de ponerla en uso, incluida la identificación de sesgos en los sistemas y los datos que se utilizan que pueden conducir a resultados injustos;
- Implementar medidas de Responsabilidad Demostrada que sean apropiadas con respecto a los riesgos de interferencia con los derechos humanos;

Previo a ello, en junio de 2019 la Red Iberoamericana de protección de datos (RIPD) publicó *Recomendaciones generales para el tratamiento de datos personales en la inteligencia artificial*[18]. Allí se realizan algunas sugerencias a quienes desarrollan productos de IA, con el fin de orientarlos para que desde el diseño del producto se tengan en cuenta las exigencias de las regulaciones sobre tratamiento de datos personales. Las recomendaciones son:

[18] Texto aprobado por las Entidades integrantes de la Red Iberoamericana de Protección de Datos en la sesión del 21 de junio de 2019, en Naucalpan de Juárez, México. La guía puede consultarse en: https://www.redipd.org/sites/default/files/2020-02/guia-recomendaciones-generales-tratamiento-datos-ia.pdf

- Cumplir las normas locales sobre Tratamiento de Datos Personales (TDP);
- Efectuar estudios de impacto de privacidad;
- Incorporar la privacidad, la ética y la seguridad desde el diseño y por defecto;
- Materializar el principio de responsabilidad demostrada (*accountability*);
- Diseñar esquemas apropiados de gobernanza sobre TDP en las organizaciones que desarrollan productos de IA;
- Adoptar medidas para garantizar los principios sobre TDP en los proyectos de IA;
- Respetar los derechos de los titulares de los datos e implementar mecanismos efectivos para su ejercicio;
- Asegurar la calidad de los datos personales;
- Utilizar herramientas de anonimización;
- Incrementar confianza y la transparencia con los titulares de los datos personales.

Para conocer los detalles de la implementación de algunas de estas recomendaciones, la RIPD ha elaborado unas directrices complementarias y más detalladas contenidas en el documento denominado *Orientaciones específicas específica para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de inteligencia artificial*.

En esos documentos se plantea que la privacidad desde el diseño y por defecto (*Privacy by Design and by Default*) busca garantizar el correcto tratamiento de los datos utilizados en los proyectos que involucren recolección, uso o tratamiento de datos personales. El debido tratamiento de la información debe ser un componente esencial del diseño y puesta en marcha de proyectos de inteligencia artificial.

También es decisivo que la ética, desde el diseño y por defecto, irradie el esquema, desarrollo y uso de los datos en proyectos de IA, teniendo que ser parte fundamental de cualquier aspecto relacionado con esa actividad.

# ¿PROTECCIÓN DE DATOS PERSONALES ARTIFICIALES O REALES? LA ADAPTACIÓN A LA INTELIGENCIA ARTIFICIAL

HUGO ISAAK ZEPEDA

*Coordinador Internacional General urbano de la Secretaría de Relaciones Exteriores*

BRICEIDA CERVANTES

*Experta en Seguridad Nacional*

Hugo Isaak Zepeda es Doctor en Administración Pública por la Universidad Anáhuac – Paris-Sorbonne University, titulado con mención honorífica con el tema: *La vivienda social y el desplazamiento a las Ciudades Inteligentes en México*. Maestro en Administración Pública por el Instituto Nacional de la Administración Pública, también con mención honorífica con el tema: *La integralidad de los ecosistemas digitales para una transversalidad del Medio Ambiente*. Ambos temas han dado paso a la metodología que actualmente desarrolla para pasar de la Ciudad Común a la Ciudad Inteligente.

Se desempeñó como Secretario Técnico de la Comisión de Vivienda en el Senado de la República, Gerente Senior de Desarrollo Inmobiliario en el INFONAVIT, entre otros cargos. Actualmente es Coordinador Internacional General Urbano en la Secretaría de Relaciones Exteriores de México.

En el ámbito académico destaca su posición como catedrático e investigador en la UNAM y la Universidad Anáhuac, donde imparte docencia en materias de Política y Finanzas Públicas, Economía y Política Ambiental, entre otras. Es autor de las obras *Interconectando Ciudades Inteligentes* y *GOV4U Un Gobierno para ti*.

Briceida Cervantes es Licenciada en Criminología con formación en criminalística por la Universidad Autónoma de Querétaro. Cuenta con un Diplomado en Artificial Intelligence: Technology, Governance and Policy Frameworks.

En la Administración Pública ha ocupado los cargos de Coordinadora de Vinculación Estratégica Internacional en la Secretaría de Relaciones Exteriores, Directora de área en la Subsecretaría de Prevención y Participación Ciudadana de la Secretaría de Gobernación, así como Subdirectora en la Dirección General de Política y Desarrollo Penitenciario.

Actualmente se desempeña como Subdirectora de Informática en la Comisión Nacional Bancaria y de Valores.

Ha publicado artículos académicos en revistas arbitradas como *Iter Criminis* y la *Revista Penal México*, ambas del Instituto Nacional de Ciencias Penales, así como en la *Ex Legibus* del Poder Judicial del Estado de México, entre otras. Es articulista en la revista *Tiempo de Derechos*.

Hace cien años no existían dos temáticas que actualmente son parte de nuestra realidad: una con mayor desarrollo y la otra que comienza a consolidarse. La primera de ellas es la protección de datos personales, figura que se ha desarrollado a nivel social, político y jurídico. Sobre esta última, la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* prevé la existencia de dos clases: datos personales y datos personales sensibles. A continuación, los analizaremos.

Los primeros son cualquier tipo de información sobre un humano. Por ejemplo, nombre, estado civil, lugar de nacimiento, entre otros. Son los más básicos y sin duda nos identifican. Incluso otros, como el CURP o el RFC, tiene claves alfanuméricas que, a veces sentimos, nos reducen a un número. Por otro lado, los considerados «datos sensibles» también se refieren a información de la persona, pero de su esfera más íntima, como el hecho de padecer algún tipo de enfermedad, convicciones éticas o religiosas, filiación u opiniones políticas, identidad de género o preferencia sexual, entre otros.

No hace falta un análisis profundo o estricto para darnos cuenta de que los datos personales sensibles merecen mayores niveles de protección, dado que, al referir a categorías sospechosas, como se apunta en el artículo 1.° constitucional, pueden conducir a actos de discriminación en caso de ser filtrados o al caer en las manos equivocadas.

La mayoría de estos datos se concentran y resguardan en bases de datos, las cuales por lo general son seguras, pero no infalibles al ataque de hackers o a que se haga un mal uso de ellos. Surge una pregunta necesaria

¿Cómo podemos generar mecanismos eficientes y eficaces para evitar que los datos personales sensibles se filtren? Las respuestas usuales se presentarán de inmediato: mayor control del personal que los maneja, protocolos para prevenir y evitar el mal uso de los datos personales, sancionar a toda persona que los utilice sin autorización… en fin, lo de siempre y que los estudios criminológicos poco a poco comienzan a dejar de lado.

No obstante, creemos que existen otras vías para lograrlo. Una de ellas es el uso de la inteligencia artificial, considerando que «[…]tiene aplicaciones en diferentes ámbitos de la realidad social, por ejemplo, en el comercial, financiero, educativo, en la política criminal y en la seguridad pública, entre otros»[19]. Nuestra vida diaria, sobre todo en una sociedad ultra conectada, está vinculada con este tipo de tecnología.

La inteligencia artificial, segunda temática que se expresó al inicio del presente escrito, es un lenguaje matemático definido por una estructura de algoritmos para instruir acciones determinadas bajo la función de resolver actividades programadas. Por su estructura compleja, existen dos variables en su comportamiento: defensores y detractores. Estos últimos apuntan a que su uso indiscriminado y malicioso puede implicar la violación de derechos fundamentales y afectar esferas de la vida humana como la privacidad. Lo anterior interesa, sobre todo, cuando existe un responsable de tratamiento de datos personales que utiliza los mismos con fines distintos a los que consintió la persona.

Siguiendo lo apuntado en el párrafo anterior, es cierto que la inteligencia artificial ayuda a procesar información que los usuarios otorgan a una compañía o un sitio web, por lo que existe una preocupación constante y permanente de que los sistemas de *software* y *hardware* lleven, por errores de diseño, a conllevar la violación de derechos humanos[20].

En el otro polo se ubican aquellas personas que consideran que el desarrollo tecnológico siempre será benéfico, pero que depende del uso que le otorguen los operadores. Nosotros nos encontramos en este grupo.

La razón es muy sencilla: el uso y aplicación de tecnología vinculada con inteligencia artificial fácilmente puede ayudar a generar programas y medidas de seguridad que impidan la filtración y robo de datos personales, como medida preventiva.

La inteligencia artificial también puede servir de manera activa en lo

[19] Cervantes, Briceida, «"Cuando el destino nos alcance": Inteligencia artificial y Derechos Humanos», en Revista *Tiempo de Derechos*, N.° 50, junio de 2022, p.38.

[20] Mendoza, Olivia, «El derecho de protección de datos personales en los sistemas de inteligencia artificial», en Ius. *Revista del Instituto de Ciencias Jurídicas de Puebla*, México, vol. 15, N.° 48, julio – diciembre de 2021, p. 180.

que respecta al manejo de los datos personales. Por ejemplo, identificando el uso indebido que se le otorgue a éstos; es decir, ayudaría en la investigación criminal.

Para ello, es necesario contar con los recursos humanos, materiales y financieros suficientes que permitan el desarrollo e implementación de dicha tecnología, ya que sólo a partir de la generación de programas de inteligencia artificial destinados específicamente a ese propósito podrá alcanzarse el objetivo.

Éste es un solo ejemplo ya que, de cara a la transición a Ciudades Inteligentes, donde México comienza a fungir un eje rector para América Latina y el Caribe, se abrirán más espacios en los cuales el manejo y resguardo de datos personales y el uso de tecnología basada en programas de inteligencia serán parte de nuestro día a día.

Comenzamos el trabajo señalando que hace cien años la realidad era diferente a la que hoy vivimos. Lo mismo podemos decir hacia el futuro: nuestro mundo será muy diferente y es poco probable que podamos estar ahí para dar cuenta de ello. Sin embargo, lo que suceda el próximo siglo comienza a gestarse con nosotros, por lo cual es menester que trabajemos desde hoy para que el porvenir sea mejor. Eso lo podemos lograr apostando por la inteligencia artificial como parte de nuestras vidas, sobre todo en cuestiones que se traten de nuestra más sagrada intimidad.

# EL RECONOCIMIENTO FACIAL Y LA PROTECCIÓN DE DATOS PERSONALES: UNA APROXIMACIÓN DESDE EL RGPD

JORGE J. VEGA IRACELAY

*Experto en Tecnología y Sociedad*

Abogado por la Pontificia Universidad Católica Argentina, Maestro en Leyes, Columbia University, Admitido en la Barra de Abogados del Estado de Nueva York. Doctorando en Derecho, Universidad Carlos III, Madrid, ex Assistant General Manager, Microsoft Corp., experto en Tecnología y Sociedad, ensayista, escritor, y conferencista en temas afines.

Es una gran iniciativa del INAI y de las Autoridades del Órgano Garante del Estado de Oaxaca realizar estas Jornadas dentro de la Ruta de la Privacidad, y debatir temas tan acuciantes para la protección de los datos personales, como el impacto de las nuevas tecnologías, y en especial las de carácter disruptivo, como la inteligencia artificial (IA) y las técnicas de reconocimiento facial.

En primer lugar, es necesario dar un poco de contexto al impacto que tiene la IA en nuestras vidas.

Como ha sostenido el McKinsey Global Institute, la revolución de la inteligencia artificial es «diez veces más rápida y tiene una escala 300 veces mayor» que la Revolución Industrial anterior. Es decir, que este *tsunami tecnológico*, como me gusta llamarlo, se distingue de otras innovaciones y disrupciones anteriores por su velocidad y por su magnitud. Es por ello que algunos autores reconocen en la IA al atributo de la Nueva Electricidad del siglo XXI. Estos fenómenos tecnológicos surgen y se retroalimentan, además del *Big Data*, donde la información convertida en dato y procesada por la analítica en metadatos son el nuevo paradigma del nacimiento de

nuevas tecnologías, técnicas y modelos de negocios, y —me atrevería a decir— de una nueva forma de pensar, con un impacto muy profundo, aún no descifrado del todo, en nuestras vidas, y el funcionamiento de nuestras sociedades. Ahora bien, comprender cabalmente el carácter disruptivo de la IA, es decir el alterar un *status quo* preexistente, es imprescindible para analizar su impacto en el Derecho de la Protección de Datos Personales y encontrar respuestas eficaces a los desafíos que nos presenta.

Las miradas existentes sobre la IA oscilan entre los extremos de una visión utópica, que cree a ultranza en los beneficios de ella para la sociedad en general —minimizando sus desafíos— y la visión distópica, que niega o minimiza sus beneficios y magnifica sus riesgos. Estas visiones tienen una estrecha relación con los principios, valores y bienes jurídicos protegidos por las legislaciones vigentes sobre protección de datos personales, y en última instancia de los ciudadanos por ella alcanzados, y los pilares, creencias y dinámicas de los mercados donde se desarrollan estas tecnologías, y sus mercados objetivo.

Como veremos más adelante, no existe una regulación específica y holística sobre el diseño, uso y efectos de la IA en la UE, salvo por algunas referencias normativas indirectas en el Régimen Legal de Protección de Datos que recoge el RGPD (Reglamento General de Protección de Datos), así como en otras disciplinas, como la seguridad de los productos, o sectores, como el de la Sanidad, que por ser de aplicación general o especifica aplican a cualquier aplicación tecnológica. Ello no quiere decir que la IA no presente desafíos únicos que no tienen hoy una respuesta adecuada y eficaz desde la regulación, pero tampoco que hay que legislar desde una base cero a la IA.

El interés de los formuladores de políticas públicas en el tema y la preocupación de los ciudadanos por sus riesgos, así como en general el desconocimiento del funcionamiento de la IA y sus efectos para las personas y sus derechos, han provocado una hiperactividad de análisis, recomendaciones, guías y directrices, lo cual podríamos denominar como *soft law*, y de propuestas de regulación de la IA, en especial en la Unión Europea. Es en esta región donde por su base humanista y centrada en la protección de los Derechos y Libertades fundamentales de las personas se le da una importancia central a ello y a nuestra materia, la protección de los datos personales. Por otra parte, existen iniciativas similares de regulación, aunque con otra aproximación, en los EEUU, y otros esfuerzos no legislativos sobre recomendaciones o guías éticas en la IA por parte de la OCDE, el Consejo de Europa, y la UNESCO por citar los más relevantes.

Hace cuatro años escribimos un breve artículo sobre algunas ideas y

propuestas en esos entonces existentes, algunas de cosecha propia, para esbozar una Gobernanza de la IA, que actualmente en virtud de la hiperactividad señalada sería incapaz de recopilar. Sin embargo, algunas de las ideas que allí comentábamos, como el enfoque en el riesgo de las aplicaciones de IA, han sido ahora formalmente propuestas en algunos de los documentos que antes mencionábamos.

## *La inteligencia artificial*

Ahora bien, la primera dificultad para superar es definir la IA. La IA es una tecnología que encontramos en el nodo de otras innovaciones tecnológicas que la habilitan, como el aprendizaje automático, y sus modalidades, la programación en lenguaje natural, el reconocimiento de imágenes, el cómputo en la nube, y se trata de una nueva capa de innovación y desarrollo sobre otras anteriores. Podríamos decir que existe IA[21] cuando una máquina o sistema imita o emula las funciones cognitivas que los humanos asocian con otras mentes humanas, como aprender y resolver problemas o aprueba el famoso *imitation test* de Turing (es decir, que la otra persona no reconoce que está interactuando con una máquina).

[21] Asimismo, podemos definirla como «Un conjunto de tecnologías que le permiten a los ordenadores percibir, aprender, razonar, asistir en la toma de decisiones, y actuar para ayudarnos a resolver problemas". Alternativamente, podemos tomar otra definición más compleja que ilustra la dificultad de encontrar un consenso en definirla en el ámbito de la UE. Así se la define con referencia a un Anexo, para permitir modificaciones en el futuro y acompañar la evolución tecnológica, en la propuesta de Reglamento sobre IA que presentó la CE en abril del 2021: Artículo 3 Definiciones A los efectos del presente Reglamento, se entenderá por: 1) «Sistema de inteligencia artificial (sistema de IA)»: el *software* que se desarrolla empleando una o varias de las técnicas y estrategias que figuran en el anexo I y que puede, para un conjunto determinado de objetivos definidos por seres humanos, generar información de salida como contenidos, predicciones, recomendaciones o decisiones que influyan en los entornos con los que interactúa. De manera amplia y dinámica, se puede ampliar el Anexo I en el futuro, tecnología neutral, deberíamos analizar si el reconocimiento facial en la etapa de identificación esta capturado en esta definición. Anexo I Técnicas y estrategias de inteligencia artificial mencionados en el Artículo 3, punto 1 *a*) Estrategias de aprendizaje automático, incluidos el aprendizaje supervisado, el no supervisado y el realizado por refuerzo, que emplean una amplia variedad de métodos, entre ellos el aprendizaje profundo. Estrategias basadas en la lógica y el conocimiento, especialmente la representación del conocimiento, la programación (lógica) inductiva, las bases de conocimiento, los motores de inferencia y deducción, los sistemas expertos y de razonamiento (simbólico). Estrategias estadísticas, estimación bayesiana, métodos de búsqueda y optimización. https://eur-lex.europa.eu/resource.html?uri=cellar:e0649735-a372-11eb-9585-01aa75ed71a1.0008.02/DOC_1&format=PDF

## *El Reconocimiento Facial*

Las técnicas de reconocimiento facial se basan en una comparación de plantillas biométricas: la de registro y la comparada. Estas plantillas recogen particularidades únicas de nuestro rostro para identificarnos, como la ubicación y forma de los ojos, cejas, etc., comparándolas con otras semejanzas identificadas. Los algoritmos de reconocimiento facial analizan así las correlaciones entre las imágenes y plantillas biométricas analizadas y establecen un porcentaje de similitud. En consecuencia, si el resultado supera determinado umbral, el sujeto es considerado como positivo.

A modo introductorio, las tecnologías de reconocimiento facial comenzaron en los años sesenta con una tableta *Rand* que tenía una cuadrícula con coordenadas horizontales y verticales, donde se ubicaban de manera manual los rasgos y ubicaciones de ojos, nariz, línea del cabello y boca en esas coordenadas, y luego se insertaban estos datos en una base de datos, que con una nueva fotografía permitía recuperar la foto más parecida a esa persona.

En la actualidad tenemos herramientas más sofisticadas que de manera automatizada y con desarrollos de IA procesan estos datos y mapean las similitudes. Estos *software* utilizan, por ejemplo, algoritmos de aprendizaje profundo para comparar una imagen con la huella facial almacenada y verificar así la identidad de un individuo.

Ahora bien, desde el siglo XX, la aplicación del reconocimiento facial, al pasar de las técnicas manuales a las tecnologías de reconocimiento facial (FRT), para extraer y comparar características automáticamente y cada detalle de su medición a través de la aplicación de la inteligencia artificial (IA), ha mejorado significativamente estas herramientas.

Facebook comenzó a implementarlo desde 2010 para identificar a personas en las fotos subidas a su red. Actualmente, más de 350 millones de fotos se cargan y etiquetan por día mediante el reconocimiento facial en Facebook. Según fuentes periodísticas, en 2011 se instalaron técnicas de reconocimiento facial en las cámaras del aeropuerto de Panamá y fue la tecnología usada para identificar a Bin Laden. En síntesis, el uso de las técnicas de reconocimiento facial está hoy muy expandido. Por ejemplo, para controlar el acceso a un lugar, el embarque en vuelos, desbloquear un dispositivo o acceder a la banca en línea.

Por otra parte, el COVID-19 ha obligado a gobiernos, individuos y empresas a mover sus actividades al mundo en línea, y ha acelerado el diseño, el desarrollo y la implementación de herramientas de identificación

digital y soluciones para evitar el contacto físico. De esta manera, tenemos varios ejemplos de verificaciones de identidad digital en el Servicio de Salud del Reino Unido, o los pasaportes digitales de vacunación que existen en la UE.

Todo ello ha coadyuvado para que los procesos de identificación digital sean más confiables, certeros y seguros para evitar fraude, y hacer más seguras las transacciones en línea.

La identidad digital es una colección de atributos únicos que describen a una persona, capturados y almacenados electrónicamente, en un contexto determinado y que son usados para una transacción electrónica.

Entre estos atributos contamos con el scanner de ojos, los reconocimientos faciales en 3D, mapeados con carnés de identidad emitidos por los Gobiernos, y nuestra conducta digital, como la navegación o actividad en redes sociales, etc.

Ahora bien, el reconocimiento facial puede ser usado con fines de identificación[22], verificación de identidad y autenticación de individuos. Un buen ejemplo es el sector bancario, donde los desafíos de seguridad y de ciberseguridad y de privacidad han llevado a una adopción gradual de identificación y verificación digital de individuos. Pero también en los controles migratorios de aeropuertos como el de Madrid, que hace nuestro escaneo de nuestro pasaporte y verifica mediante una herramienta de reconocimiento facial nuestra identidad.

[22] Sin embargo, la falta de identidad afecta a un billón de personas en el mundo que no pueden acreditar su identidad y por eso, dentro de los objetivos 2030, hay un proyecto del Banco Mundial para ello.

## *El Reconocimiento Facial y su impacto en la privacidad*

Un primer momento es la *autenticación*; por ejemplo, cuando usamos nuestra foto en el móvil para acceder a la banca en línea. Otro es la *identificación*, donde se compara una imagen con las de una base de datos numerosa para analizar la similitud. El primero es menos invasivo para la privacidad que el otro. Una manera de mitigar la invasión en la privacidad es eliminar rápidamente las imágenes escaneadas, y no almacenarlas en un repositorio central. En caso contrario, estos datos pueden ser utilizados para un fin incompatible[23] o darles un tratamiento inadecuado por carecer de consentimiento del titular; o sea, carecer de una justificación o base legal para su tratamiento.

Algunos de los beneficios que ofrecen estas herramientas de reconocimiento facial son prevenir y castigar la comisión de delitos para mantener la seguridad de los ciudadanos y la sociedad con eficiencias y ahorros en costos. Así surgieron en el pasado tecnologías como las cámaras de video para vigilancia, y más recientemente los drones y las de reconocimiento facial y otros datos biométricos. Pero cada tecnología ha impactado en la relación de los ciudadanos con los estados, en especial en sus derechos fundamentales, como su privacidad, intimidad y honor, entre otros.

Cuando estas herramientas son usadas por los poderes públicos, en especial autoridades de cumplimiento de la ley (como Policía, Servicios de Seguridad o Inteligencia, o la Justicia), el escrutinio de los fines, uso y supervisión de las aplicaciones de reconocimiento facial es aún mayor y más complejo.

Las aplicaciones de reconocimiento facial con desarrollos de IA afectan la vida de las personas todos los días, invaden nuestra privacidad y otros derechos humanos. En consecuencia, el desarrollo e implementación masivas sin consideración a sus posibles desafíos podría traer consecuencias nefastas y aún prohibirse su desarrollo e implementación.

[23] Existe un caso interesante en la Justicia de Gales sobre una aplicación de la policía para detectar sospechosos. Si bien eliminaba las imágenes una vez comparadas, el Tribunal entendió que había habido tratamiento de datos y no se había cumplido con los principios legales aplicables; en especial una reutilización compatible de los mismos.

## *Oportunidades y desafíos: Algunas respuestas*

Si estamos convencidos de las numerosas ventajas que ofrecen estas herramientas tecnológicas avanzadas, y ante el incremental desarrollo y demanda de éstas, ¿cómo asegurar el equilibrio entre ellas y el centro en la persona y sus derechos fundamentales, principalmente el de la protección de sus datos personales y los de categoría especial?

En consecuencia, hay un gran debate y escrutinio de estos temas. Las soluciones no son uniformes de país a país, y de estado a estado. Todo ello depende del marco legal aplicable sobre la protección de datos, pero también de las expectativas y aceptaciones por los ciudadanos de una mayor o menor privacidad en la tensión con otros derechos y valores *vis-a-vis* las ventajas de una aplicación tecnológica en particular.

Desde hace ya algunos años, se han encendido muchas críticas y preocupaciones en torno a las herramientas de reconocimiento facial. Cabe citar como ejemplo que en 2019 San Francisco fue la primera ciudad en los EEUU en prohibirlas por parte de la administración local y la policía.

Por otra parte, estas tecnologías son parte del cuestionamiento social existente sobre la vigilancia tecnológica masiva y omnipresente en sus distintos apelativos. El reconocimiento facial, cuando se traduce en vigilancia publica y masiva de la población, puede permitir la geolocalización y control de la conducta en tiempo real y a una escala sin precedentes. Esto es un peligro no sólo para el derecho de la privacidad, sino también la libertad de expresión de esas personas que podrían verse intimadas así a ejercer plenamente su derecho.

En otro terreno de cuestionamientos, las tecnologías de reconocimiento facial se han caracterizado como poco fiables. Por ejemplo, la AEPD (Agencia Española de Protección de Datos) ha publicado en junio de 2020 una nota informativa sobre 14 equívocos con relación a la identificación y autenticación biométrica, y pone como ejemplo las huellas dactilares y las mediciones faciales. Son interesantes los siguientes hallazgos que menciona la AEPD:

- Del tratamiento de datos biométricos se revela más información personal sobre el sujeto que una contraseña o certificado, como las emociones, la salud, o el consumo de sustancias, discapacidades, etc. Por ser esta información de carácter implícita, el usuario no puede impedir la recogida de esa información suplementaria.

- El reconocimiento facial no es 100 % preciso, sino que se basa en probabilidades. Depende de la calidad y cantidad de los datos recogidos, las condiciones de recogida y tratamiento, y de los sesgos del desarrollo.
- No todas las personas pueden ser reconocidas facialmente: hay incompatibilidad biométrica por accidentes, lesiones, y puede ser causa de exclusión social.
- Se puede burlar técnicamente la identificación biométrica.
- La mayoría de las características biométricas están expuestas y pueden capturarse a distancia, como el rostro, o la huella térmica.
- La información biométrica es mayor y está almacenada en lagos de datos que pueden sufrir brechas de seguridad.

En ese sentido, se han destacado preocupaciones con respecto a las tasas de error, falsos positivos o falsos negativos que arrojan estas herramientas. Por ejemplo, en los sistemas de reconocimiento facial en vivo en lugares con miles de personas, aunque la tasa de error sea baja, el efecto negativo puede ser material[24].

Por otra parte, como destaca la AEPD, el reconocimiento facial puede, además del rostro, revelar otros datos sensibles como la etnia, el estado de salud o las emociones.

Asimismo, los sistemas de IA, al ser programados por personas con sus prejuicios, o mediante el aprendizaje automático en entornos discriminatorios, por ejemplo, sistemas entrenados sólo con o en un porcentaje alto con poblaciones masculinas de raza blanca, tienen sesgos, o sea una desviación inadecuada en el proceso de inferencia, y pueden discriminar, incrementando la desigualdad. En otras palabras, algunos algoritmos no sólo no resuelven los problemas del caso, sino que incluso los agravan de manera exponencial.

Los desarrolladores argumentan que los algoritmos, al ser fórmulas matemáticas, son objetivos, asépticos, y en consecuencia no están influenciados por prejuicios o sesgos humanos. Sin embargo, la clave está en los datos utilizados y los criterios para analizarlos, y en la decisión que se tomó en la programación, incluyendo los árboles de decisión, y que afecta los resultados de la decisión del caso.

[24] Vid. Informe de la Agencia EEUU de Derechos Humanos FRA FOCUS, "Facial recognition technology: fundamental rights considerations in the context of law enforcement", adoptado el 21 de noviembre de 2019. pág. 7. Disponible *online* en: https://fra.europa.eu/en/publication/2019/facial-recognition-technology-fundamental-rights-considerations-context-law (última consulta, 2 de julio de 2021).

Dichos sesgos pueden tener efectos discriminatorios no necesariamente de manera intencional por el programador, sino un resultado inevitable de sus prejuicios quizás inconscientes, el diseño de la programación o de la lógica aplicada. No podemos ignorar que los algoritmos utilizados comprenden fórmulas algebraicas en la mayoría de los casos desconocidas, opacas o indescifrables, características que han contribuido a llamarlos cajas negras o *Black box*.

Tampoco existen en la mayoría de los casos mecanismos de supervisión y control humano calificado en su funcionamiento de acuerdo con determinados principios, derechos y garantías. Todo ello compromete los principios y la responsabilidad en la protección de datos, como transparencia, explicabilidad, inteligibilidad, responsabilidad proactiva, entre otros, y los derechos a ellos inherentes[25].

La utilización de técnicas de reconocimiento facial por los poderes públicos, como en reconocimientos para funciones de vigilancia y seguridad pública, ha sido seriamente resistida, y presentado serias críticas por su uso en la Justicia predictiva[26] y su uso militar.

Como tal, la cara se puede mapear y comparar con otros datos que ofrecen una coincidencia e identificación con un individuo. Sin embargo, este reconocimiento puede implicar la introducción de otros datos biométricos, como datos de reconocimiento ocular o del iris. La coincidencia uno a uno proporciona cierta identificación de un individuo en un determinado contexto. Ahora bien, el uso de una imagen identificada en conexión con otros bancos de datos o lagos de datos permite muchas posibilidades y connotaciones de uso. Estas coincidencias que pueden procesar los datos a escala presentan, por otra parte, nuevas posibilidades y complejidades. Por ejemplo, las expectativas de privacidad en un entorno privado de identificación facial frente a un ordenador para acceder al sistema son distintos a una herramienta que compara mis rasgos con una base de datos gigante o lago de datos, o sea en un contexto de *big data*. En otras palabras, no es lo mismo una verificación de un dispositivo que un propósito de vigilancia, por ejemplo, en un espacio público. Así como no es lo mismo esa expectativa en mi vivienda como en un trámite migratorio cruzando una frontera.

[25] Como lo exige el RGPD.

[26] Cfr. El análisis de la utilización de un *software* para determinar la posibilidad de reincidencia criminal y su discriminación en contra de afroamericanos en los EEUU: Angwin, Julia. Propublica. 23 de mayo de 2016. https://www.propublica.org/.../machine-bias-risk-assessments-in-criminal- sentencing (último acceso: 16 de diciembre de 2020).

Con respecto al consentimiento del titular de los datos, un problema central en el reconocimiento facial es la facilidad y falta de percepción del aquél en el registro de su imagen o rostro, y su falta de control sobre su tratamiento. Con el reconocimiento facial no sucede lo mismo que con otros datos como las huellas digitales o el ADN, donde el titular es plenamente consciente de su recolección. De esta manera, el consentimiento del titular de los datos no siempre es libre, explícito e informado.

## *Disposiciones aplicables del RGPD*

El RGPD con una interpretación holística y teleológica da una base sólida para responder a la mayoría de estos desafíos que presentan la IA y las tecnologías de reconocimiento facial.

La discusión sobre la regulación del RGPD de la IA tiende a centrarse en la toma de decisiones individuales automatizadas y la elaboración de perfiles (art. 22), pero también presenta efectos importantes en muchos otros aspectos de los sistemas de IA, incluido el uso secundario, la divulgación y retención de datos personales existentes con el fin de la construcción de conjuntos de entrenamientos (incluidas las disputas sobre la anonimización), el uso de datos recopilados por los sistemas de IA para nuevos conjuntos de entrenamiento (incluidas las cuestiones de consentimiento), el cumplimiento del principio de minimización de datos, entre otros, la explicabilidad de la lógica aplicada en una decisión automatizada, el derecho del titular a obtener intervención humana, expresar su punto de vista y a impugnar la decisión.

Por otra parte, el reconocimiento facial con fines de identificación, al tratarse de datos biométricos en los términos exigidos por el RGPD[27], son datos de categoría especial o sensibles regulados en el artículo 9 y gozan de una protección más robusta. Entre sus medidas está la prohibición de su tratamiento a menos de que exista una excepción legal, como el consentimiento explícito del titular[28].

[27] El RGPD define los datos biométricos como aquellos «datos personales obtenidos a partir de un *tratamiento técnico específico*, relativos a las características físicas, fisiológicas o conductuales de una persona física que *permitan o confirmen la identificación única* de dicha persona, como imágenes faciales o datos dactiloscópicos» (Art 4. 14). En el mismo sentido, la nueva versión del Convenio 108 para la Protección de Individuos con respecto al procesamiento de datos personales incluye [3] entre las categorías especiales de datos a los datos biométricos dirigidos a la identificación unívoca de una persona.

[28] En el caso de España, por ejemplo, no basta el consentimiento del interesado, para levantar la prohibición de tratamiento de los datos de categoría especial, cuando la finali-

Baste recordar que, para que este consentimiento sea válido, tiene que ser libre e informado. Además de los principios, derechos y obligaciones generales que establece el RGPD, al tratarse el reconocimiento facial como se ha analizado de un dato de categoría especial, es obligatorio la realización de la evaluación de impacto para cumplir con el principio fundamental de la privacidad por diseño. La evaluación de impacto es un proceso de identificación de riesgos que derivan del tratamiento de los datos, pero es obligatoria para las aplicaciones de alto riesgo, como el reconocimiento facial en el uso de aplicación de la ley. Así lo ha reconocido la AEPD para el tratamiento de datos de categoría especial conforme a lo dispuesto por el artículo 35 del RGPD. La evaluación[29] debe incluir la necesidad y proporcionalidad de las operaciones con respecto a los objetivos del tratamiento, incluyendo los riesgos para los derechos y libertades, o sea que va más allá de la privacidad.

## *Propuestas de regulación y soft law*

Las tecnologías de reconocimiento facial han despertado el interés y la preocupación de las Autoridades en la UE (Unión Europea), en línea con sus iniciativas de regulación de la IA. Ello es con independencia de las disposiciones legales que existen en la actualidad en el RGPD, que regulan dentro de la protección legal de Datos Personales algunos tratamientos de datos realizados por aplicaciones o soluciones basadas en IA, en especial la elaboración de perfiles y las decisiones automatizadas, y las aplicables al tratamiento de la categoría especial de datos, como los biométricos.

En ese sentido, la CE (Comisión Europea) ha propuesto una iniciativa de regulación de la IA en abril de 2021, y se producirán, asimismo, otros impactos en la materia, entre otros, por la *Ley de Servicios Digitales y de Mercados Digitales* en la UE.

dad principal sea identificar su ideología, afiliación sindical, religión, orientación sexual, creencias origen racial o étnico (Cfr. art. 9.1. *Ley de Protección de Datos* LO 3-2018).

[29] A pesar de algunas iniciativas, como la reciente del Profesor Mantelero, no hay un marco estandarizado de derechos humanos y de requisitos legales que puedan ser facialmente aplicados a los sistemas de reconocimiento facial. Sin embargo, las evaluaciones de impacto en protección de datos personales y derechos humanos, una mayor transparencia, regulación, auditoría y explicabilidad serían de gran ayuda.

De aprobarse esta regulación, ésta tendrá un impacto decisivo para la IA no sólo en la UE sino globalmente (incluyendo los países europeos que no forman parte de la UE pero que sí son parte del Consejo de Europa, y su convenio 108 y otros como México, y de la Convención Europea sobre Derechos Humanos), dado el liderazgo y la extraterritorialidad de muchas de las normas de la UE, como el RGPD. Pero el ámbito de esta iniciativa de regulación excede a la protección legal de datos personales, y otros derechos humanos, si bien los comprende, centrándose en la seguridad de los productos o servicios basados en desarrollos de IA.

Esta iniciativa se sustenta en un enfoque de riesgo, y así determina cuatro tipos de riesgos en las aplicaciones de IA: 1) Prohibidos, 2) Alto riesgo, 3) Bajo riesgo y obligaciones de transparencia, y 4) Bajo riesgo sin obligaciones específicas. Por defecto la mayoría cae en la última categoría.

Dentro de las usos o riesgos prohibidos[30] (y sus excepciones) se comprende al uso de mandos a distancia en tiempo real de sistemas de identificación biométrica en espacios de acceso público, a efectos del cumplimiento de la ley llevada a cabo por las autoridades policiales. Respecto a estos últimos, sólo se permiten para el cumplimiento de la ley, bajo autorización judicial o administrativa.

El Supervisor Europeo de Protección de Datos (SEPD)[31], si bien acoge con satisfacción el proyecto de Reglamento sobre IA, solicita una moratoria sobre la identificación biométrica remota en espacios públicos, incluyendo el reconocimiento facial.

El Comité Consultivo del Convenio del Consejo de Europa para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos Personales (*Convenio 108+*) elaboró, por otra parte, unas Directrices sobre Reconocimiento Facial, dirigidas a legisladores, responsables de la toma de decisiones y empresas.

[30] Aunque no se trate de esta prohibición, el reconocimiento facial podría caer dentro de la categoría de alto riesgo, con las obligaciones de cumplimiento establecidas, si se relaciona con la selección y reclutamiento de personal, decisiones sobre promociones y terminaciones, asignación de tareas y evaluación de desempeño y conducta de personal, y el acceso y goce de servicios privados esenciales y servicios públicos y beneficios, evaluación de crédito y solvencia, prioridades para los servicios de emergencia o respuesta, etc.

[31] El EDPB y el EDPS emitieron una opinión conjunta que abogaba por una prohibición más amplia del uso de tecnologías de identificación biométrica en el espacio público. Concretamente, ambas autoridades apuestan por una prohibición general del uso de tecnologías biométricas que automáticamente capten datos sensibles (no solo el rostro, sino también la voz, el ADN, o huellas dactilares) en el espacio público y «a gran escala».

Estas Directrices identifican ciertos propósitos, o modos de uso, del reconocimiento facial que deben prohibirse o restringirse. El primero se aplica al uso del reconocimiento facial con el único propósito de determinar el color de la piel, las creencias religiosas o de otro tipo, el sexo, el origen racial o étnico, la edad, el estado de salud o la condición social de una persona. En el mismo sentido, el reconocimiento de afecto (el uso de la tecnología para intentar identificar o clasificar las emociones humanas) también debe prohibirse. Por otra parte, el tratamiento de datos biométricos con fines de identificación debe limitarse, en general, a fines policiales y llevarse a cabo únicamente en el ámbito de la seguridad. Estas Directrices son una pieza clave de soft law para evaluar el cumplimiento de las herramientas de reconocimiento facial con los principios de protección de datos del RGPD.

## *Conclusiones*

Como otras herramientas tecnológicas, las herramientas de reconocimiento facial y de IA han avanzado a pasos agigantados en nuestra época y presentan oportunidades y desafíos para los derechos fundamentales, como la protección de los datos personales.

Habrá que analizar en cada caso el contexto, el propósito, y la observancia de los principios y obligaciones establecidos en el RGPD y otras normas locales, en una interpretación armónica, funcional y teleológica. Así, en los aspectos aún no regulados, la iniciativa de la CE sobre un Reglamento sobre IA, si bien ha recibido críticas, algunas de ellas justificadas, se presenta como una alternativa de regulación razonable para llenar al menos algunos vacíos jurídicos, pero que tiene que armonizarse con el RGPD, siendo normativas con ámbitos de aplicación distintos. Pasar una conformidad bajo su normativa no implicaría, por ejemplo, cumplir con el RGPD.

Sin embargo, el RGPD se presenta aún demasiado abierto para una regulación exhaustiva y eficaz, pero tiene por otra parte instrumentos adecuados como la privacidad por diseño y, por defecto, la evaluación de impacto, las reglas para el consentimiento expreso, el derecho a no ser objeto de decisiones exclusivamente automatizadas, la protección reforzad de los datos de categoría especial, etc. Bien instrumentadas, podrían ser eficaces.

Sin embargo, permanecen aún otros riesgos y desafíos específicos para la protección de datos en estos desarrollos de IA en el contexto del *Big*

*Data*, que en nuestro criterio no están abordados de manera completa, holística y eficaz por la regulación en protección de datos personales. Ello se debe, en su mayor parte, a característica propias y muy distintivas de las soluciones de IA, como el volumen, la velocidad, el concepto de metadato, la inferencia analítica como dato, la opacidad de los algoritmos, las consecuencias sociales y para las libertades y derechos fundamentales de las decisiones automatizadas y la elaboración de perfiles, y el sesgo algorítmico, por citar los más relevantes.

En las evaluaciones de impacto en protección de datos personales y derechos humanos, sería de gran ayuda exigir una mayor transparencia, regulación, auditoría y explicabilidad.

En el área específica del reconocimiento facial, existen puertas abiertas para su uso al menos en España, como en el ámbito penal o de las obligaciones laborales, donde con ciertos recaudos estas técnicas son aceptadas. El reconocimiento facial ofrece mayores posibilidades de invasión a la privacidad y abre puertas para la vigilancia masiva. Por ello sería deseable una ley local más clara, especificando las salvaguardas y garantías exigibles en el caso de estar habilitadas.

Como se ha señalado, la tecnología, en este caso la IA, es neutra en sí misma. Es una herramienta a servicio del humano, y en consecuencia el problema central es cómo la han de utilizar las personas y para qué fines. En ese sentido, cabe dotar una máxima importancia a los nuevos sesgos psicológicos que se derivan de su empleo, en especial por el uso de analíticas algorítmicas, que conducen a inferencias injustas con efectos significativos para la vida de las personas. Por ello es necesario prestar especial atención a atribuir responsabilidades específicas y serias a los componentes IA sin supervisión humana; en especial si tratan datos sensibles o en sectores específicos.

Por otra parte, los algoritmos son cada vez más complejos, y en consecuencia ello atenta contra su transparencia y explicabilidad. En ese sentido, el funcionamiento interno de los algoritmos es simplemente muy difícil de comprender y consecuentemente de explicar (*caja negra*) en su estado actual y en el que evolucionará, en muchos casos aún para el responsable o para el desarrollador-encargado. Esta dificultad es de especial preocupación para el interesado, ciudadano común que se puede encontrar indefenso y desconcertado frente a un fenómeno que no comprende, y un lenguaje cifrado inabordable que subyacen a un modelo tecnológico y de negocios que puede afectarlo de manera adversa y socavar sus libertades, garantías y derechos fundamentales más preciados y amenazados en esta era digital.

Como reflexión final, como se sostiene en el considerando 4 del RGPD, el tratamiento de datos personales debe estar concebido para servir a la humanidad, y no es un derecho absoluto, sino que debe interpretarse funcionalmente y conservar su equilibrio con otros derechos fundamentales, como el derecho a la vida o a la salud, observando los principios de necesidad y proporcionalidad. Ésa es la tarea más difícil que tiene por delante el legislador europeo, y me sospecho muchos otros: ponderar y arbitrar equilibrios adecuados, justos y proporcionados entre los derechos y libertades reconocidas en la UE en aras de un fin superior, que es el bien común de sus ciudadanos.

# AVANCES Y PERSPECTIVAS NORMATIVAS DE LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO Y AMÉRICA LATINA

JESSICA MATUS

*Abogada experta en internet y privacidad*

Abogada experta en protección de datos personales con 20 años de trayectoria en el campo de las tecnologías en el sector público, privado y sociedad civil, desarrollando programas de privacidad, difundiendo la importancia de la privacidad, participando en la redacción del proyecto de ley sobre protección de datos en Chile, y en la elaboración de guías, políticas, y evaluación de impacto en Chile y Latinoamérica.

Investigadora en protección de datos, coautora de *La Cesión de Datos Personales* (2006) y varios ensayos publicados sobre la materia. En 2021 fue reconocida por The Legal 500 como Rising Star en la categoría de Data Privacy. Diplomada en Derecho Informático y profesora en diversos Diplomados de la Universidad de Chile, Pontificia Universidad Católica de Valparaíso y Alberto Hurtado. Fundadora de Fundación Datos Protegidos (2015) y presidenta de Internet Society Capítulo Chile (2020-2022). Conduce el podcast *La Comunidad de los Datos* en Radio TXSPlus.

El lunes 25 de julio de 2022 conocimos la noticia de un robot que rompió el dedo a un niño de 7 años en un torneo de ajedrez, durante un torneo en Rusia[32]. En junio, el diario *La Nación* de Argentina titulaba: «Google lanza una herramienta para practicar con un robot tus

[32] «Robot de ajedrez le rompe un dedo a un niño de siete años durante un torneo en Rusia», *Deutsche Welle*, 28.07.2022, [https://p.dw.com/p/4En3D].

entrevistas de trabajo»[33]. También en junio, un estudio dirigido por investigadores de la Universidad Johns Hopkins, el Instituto Tecnológico de Georgia y la Universidad de Washington presenta el primer examen documentado que demuestra que los robots que operan con un modelo de IA aceptado y ampliamente utilizado funcionan con importantes sesgos de género y raza, prefiere sistemáticamente a los hombres sobre las mujeres, a los blancos sobre las personas de color, y saca conclusiones sobre la profesión o la designación de las personas basándose únicamente en una foto de su rostro.

Así podemos encontrar muchos ejemplos de diversos usos e impactos de la inteligencia artificial en la vida de las personas.

## *¿Por qué vinculamos inteligencia artificial y datos personales?*

Ambas materias se encuentran íntimamente ligadas, ya que los datos personales se han convertido en un insumo crucial para el funcionamiento de algunos sistemas informáticos que utilizan esa tecnología. Por lo tanto, la IA debe ajustarse a las garantías, derechos y obligaciones establecidas en la regulación que protege el derecho fundamental a la protección de los datos personales.

Sin embargo, dicha protección puede verse mermada por los bajos estándares normativos, por la ausencia de transparencia en cuanto a la manera en que funcionan los algoritmos que soportan esta tecnología, por los intereses económicos involucrados, por la ausencia de un enfoque de derechos, entre otros obstáculos.

Sobre este tema, el Comité Asesor del Consejo de Derechos Humanos de Naciones Unidas señaló lo siguiente en su Informe denominado *Impacto, oportunidades y retos que pueden tener las tecnologías digitales nuevas y emergentes con relación a la promoción y protección de derechos humanos*:

> No debe considerarse que las amenazas a la privacidad son el precio inevitable del progreso, porque esto debilitaría todo el marco de derechos humanos. Aunque no sea intencionada, la toma de decisiones de la inteligencia artificial puede arrojar resultados discriminatorios si el proceso decisorio se basa en algoritmos sesgados.

[33] Europa Press,«Interview Warmup: Google lanza una herramienta para practicar con un robot tus entrevistas de trabajo», *La Nación*, 1 de junio de 2022 [https://www.lanacion.com.ar/tecnologia/interview-warmup-google-lanza-una-herramienta-para-practicar-con-un-robot-tus-entrevistas-de-trabajo-nid01062022/ ].

## *¿Cómo se encuentra América Latina en materia de protección de datos personales? ¿estamos preparados para hacer frente a los desafíos de la IA?*

Argentina y Uruguay destacan ya que han sido considerados países adecuados bajo el estándar del Reglamento General de Protección de Datos. El primero desde 2003[34] y el segundo desde 2012[35].

En la República Oriental del Urugua**y**, la protección de los datos personales se encuentra regulada a nivel legal a través de la *Ley N.° 18.331*[36], publicada en agosto de 2008, que en 2018 fue complementada por la ley N.° 19.670[37], para adaptarla al Reglamento General de Protección de Datos de la Unión Europea (RGPD).

La responsabilidad proactiva establecida en la *Ley De Protección De Datos Personales* permitiría hacer frente de alguna manera a los desafíos de la IA, ya que exige adoptar las medidas técnicas y organizativas apropiadas: privacidad desde el diseño, privacidad por defecto, evaluación de impacto a la protección de datos, entre otras, a fin de garantizar un tratamiento adecuado de los datos personales.

La Protección de los Datos Personales se encuentra regulada en la República Argentina a través de la acción de habeas data, incorporada en oportunidad de la Reforma Constitucional de 1994 en el artículo 43, tercer párrafo, de la Constitución Nacional. Posteriormente, en 2000 se sancionó la *Ley N.° 25.326*, norma de orden público que regula los principios aplicables en la materia y el procedimiento de la acción de habeas data.

[34] Diario Oficial de la Unión Europea, *DECISIÓN DE LA COMISIÓN de 30 de junio de 2003 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo sobre la adecuación de la protección de los datos personales en Argentina*.[ https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32003D0490&from=ES].

[35] Diario Oficial de la Unión Europea, *DECISIÓN DE EJECUCIÓN DE LA COMISIÓN de 21 de agosto de 2012 de conformidad con la Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección adecuada de los datos personales por la República Oriental del Uruguay en lo que respecta al tratamiento automatizado de datos personales* [notificada con el número C(2012) 5704] (Texto pertinente a efectos del EEE) (2012/484/UE). [https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32012D0484&from=ES]

[36] Disponible en línea: [https://www.impo.com.uy/bases/leyes/18331-2008].

[37] La ley N.° 19.670, de aprobación de rendición de cuentas y balance de ejecución presupuestal, ejercicio 2017, en sus artículos 37 a 40, incorpora la obligación de designar a un delegado de protección de datos, establece sus funciones, el deber de informar vulneraciones de seguridad, entre otros asuntos. Disponible en línea: [https://www.impo.com.uy/bases/leyes/19670-2018].

En noviembre de 2020 se presentó en el Congreso un proyecto de ley[38] que modifica dicha normativa a fin de adaptarse al RGPD y así evitar la eventual pérdida de la calidad de país adecuado que posee. Este proyecto incluye la obligación de realizar una evaluación de impacto relativa a la protección de datos personales, cuando el responsable del tratamiento prevea realizar algún tipo de tratamiento de datos que, por su naturaleza, alcance, contexto o finalidades sea probable que entrañe un alto riesgo de afectación a los derechos de los titulares de los datos, y que deberá realizar de manera previa a la implementación del tratamiento. Será obligatoria en el caso de evaluación sistemática y exhaustiva de aspectos personales de personas que se base en un tratamiento de datos automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas humanas o que les afecten significativamente de modo similar. Aquí podría haber una manera de gestionar el riesgo de la IA.

Por supuesto, México también es un actor relevante en LATAM, a través de la actuación del INAI y gracias a que el 28 septiembre de 2018 se adhirió al *Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal* conocido como Convenio N.° 108 y, de igual manera, al *Protocolo Adicional relativo a las autoridades de Control y a los Flujos Transfronterizos de Datos*, su Protocolo Adicional.

La *Ley General De Protección De Datos Personales* En Posesión De Sujetos Obligados Públicos[39] incluye la obligación de Evaluaciones de impacto. Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales.

Asimismo, Colombia y Perú se han posicionado debido a la existencia de autoridades de control dedicadas a promover, fiscalizar y sancionar a los responsables y encargados de las bases de datos personales, aplicando importantes multas. En Colombia, la Superintendencia de Industria y Comercio, a través de una Delegatura para la Protección de Datos Personales, en 2021, aplicó 173 multas por un total de 13.500 millones de pesos colombianos. Por

[38] Diputados Argentina, Proyecto de Ley de protección de los datos personales. Disponible en: https://www4.hcdn.gob.ar/dependencias/dsecretaria/Periodo2020/PDF2020/TP2020/6234-D-2020.pdf

[39] Cámara de Diputados del H. Congreso de la Unión, «Ley general de protección de datos personales en posesión de sujetos obligados», *Diario Oficial de la Federación*, 26-01-2017. Disponible en: https://www.gob.mx/cms/uploads/attachment/file/455854/Ley_Gral_Protec_Datos_Sujetos_Obligados_26-01-17.pdf

su parte, la Autoridad Nacional de Protección de Datos Personales de Perú impuso multas por más de 6 millones de soles durante 2021.

En Brasil[40], la *Ley General de Protección de Datos Personales*[41] entró en vigor en agosto de 2020. La LGPD se modeló a semejanza del *Reglamento General de Protección de Datos* (RGPD) de la Unión Europea. Por lo tanto, tiene una perspectiva de la protección de los datos personales como derecho humano.

A nivel federal, Brasil ha creado una agencia nacional de protección de datos, la Autoridad Nacional de Protección de Datos (ANPD), que puede exigir a las organizaciones información sobre el procesamiento de datos personales, imponer sanciones y, en general, encargarse de garantizar el cumplimiento de esta ley. En agosto de 2021 entró en vigor el articulado sobre sanciones. También incluye evaluación de impacto.

> Art. 38. La autoridad nacional podrá ordenar al responsable del tratamiento que elabore un informe de impacto sobre la protección de datos personales, incluidos los datos sensibles, referente a sus operaciones de tratamiento de datos, en los términos del reglamento, observando secretos comerciales e industriales.

## *La realidad chilena*

Chile cuenta con una ley de protección de los datos personales, desde 1999, que no consagra una autoridad de control y tampoco sanciones. Esta normativa ha intentado ser modificada en variadas oportunidades, sin éxito.El actual proyecto de ley que busca reemplazarla lleva 5 años de tramitación en el Congreso. Si bien el Ejecutivo ha solicitado suma urgencia en su tramitación, es poco probable que Chile cuente con una nueva ley aprobada este año.

No obstante, el proceso de reforma a la constitución chilena que se encuentra en su etapa final abre una puerta en esta materia, ya que la propuesta incluye la creación de una Agencia Nacional de Protección de Datos con carácter autónomo y facultades de fiscalización y sanción. Además, se reconoce expresamente el derecho a la autodeterminación informativa y a la protección de los datos personales, precisando los derechos de los

[40] FORTRA, «¿Qué es LGPD? Conozca la nueva Ley de Protección de Datos de Brasil», enero 28, 2021, https://www.helpsystems.com/es/blog/que-es-lgpd-conozca-la-nueva-ley-de-proteccion-de-datos-de-brasil

[41] Visitar: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.html

titulares y los principios a los cuales debe sujetarse el tratamiento de estos datos. Pero eso no es todo: el nuevo texto constitucional consagrará el acceso universal a la conectividad digital y a las tecnologías de la información y la comunicación, garantizando el cumplimiento del principio de neutralidad en la red. También reconoce el derecho a la educación digital, al desarrollo del conocimiento, pensamiento y lenguaje tecnológico, y derecho de toda persona a participar de un espacio digital libre de violencia, otorgando especial protección a mujeres, NNA, y diversidades y disidencias sexuales y de género.

Lo anterior se hace cargo de uno de los problemas identificados en el informe del Consejo de Derechos Humanos de Naciones Unidas que expresa: «[…] las nuevas tecnologías están creando un mundo fundamentalmente diferente que no se ajusta de forma exacta a nuestros paradigmas tradicionales. Por ello, es esencial preguntarse de qué manera los tratados, documentos y prácticas de derechos humanos podrían adaptarse mejor a la era digital». El nuevo texto constitucional reconoce el mundo digital y los derechos asociados al mismo, sin perjuicio de las futuras normas de rango legal que deberán aterrizar dichas garantías, teniendo especialmente presente que, en la actualidad, las empresas privadas tienen más información y datos personales sobre los ciudadanos que los gobiernos (así lo señala el citado informe).

Como ha dicho el Relator Especial sobre el derecho a la privacidad, el papel del sector privado es especialmente crítico en el ámbito de la privacidad[42]. Por lo tanto, los principios de responsabilidad, privacidad por diseño y por defecto, minimización de datos, transparencia algorítmica, junto a las evaluaciones de impacto en el tratamiento de datos personales, deben ser la piedra angular de la industria de la inteligencia artificial que utiliza nuestros datos personales, especialmente, en el caso de datos sensibles y de grupos vulnerables.

Con todo, los órganos públicos también deben aportar como sujetos obligados, a la protección de este derecho humano, considerando especialmente el poder que tienen de restringir libertades y realizar acciones de vigilancia que utilizan esta tecnología (IA).

Por último, es necesario realizar esfuerzos regionales de homologación de normativa, ya que los desarrollos en inteligencia artificial también se dan en el ciberespacio, que no conoce de fronteras político-territoriales.

[42] Official Documents System of the United Nations: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G19/307/43/PDF/G1930743.pdf?OpenElement

# PERSPECTIVAS Y PROSPECTIVAS DESDE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y LA PRIVACIDAD

SAIPH SAVAGE

*Colaboradora de Investigación en la UNAM y Directora del Laboratorio de Inteligencia Artificial Cívico en la Facultad de Ciencias de la Computación Khoury, en la Universidad de Northeastern*

La Dra. Saiph Savage es profesora en Northeastern University en Boston, donde es directora del Civic A.I. Lab. Saiph es también colaboradora en la Universidad Nacional Autónoma de México (UNAM). El MIT Technology Review la ha reconocido como una de las 35 innovadoras menores de 35 años, y la UNESCO reconoció su investigación en inteligencia artificial como una de las 100 más impactantes. Tiene experiencia colaborando y asesorando a gobiernos federales y locales a adoptar el diseño centrado en el humano y la inteligencia artificial. Su trabajo ha sido cubierto por la BBC, The Economist y el New York Times. La Dra. Savage ha trabajado en Microsoft Bing, Intel Labs, Carnegie Mellon University, y la Universidad de Washington. Saiph cuenta con numerosas publicaciones científicas y patentes. Estudió Ingeniería en Computación por la UNAM; y doctorado y maestría en Ciencias de la Computación por la Universidad de California, Santa Barbara.

*Big Data* es un término que se ha popularizado en años recientes. Cuando hablamos del *Big data* nos referimos no sólo a datos masivos, sino también a datos que se generan a una gran velocidad (los datos que generan millones de usuarios en redes sociales y que llegan a una alta mucha velocidad a plataformas digitales) y los que pueden ser heterogéneos (datos generados con voz, video texto). El *Big data* se

está utilizando para la innovación, debido a que muchos de los servicios que se están brindado dentro de los gobiernos, empresas o academia coleccionan el *Big data* y lo utilizan para generar nuevos servicios. Por ejemplo, recomendarte películas o identificar qué trámites de gobierno son los más populares para agilizar su procesamiento mediante herramientas digitales nuevas. Usualmente para lograr brindar estos servicios se utiliza la técnica llamada «Analítica de Datos», que se concentra en encontrar patrones a partir de los datos y así ayudar a brindar mejores servicios a las personas.

Ahora bien, un concepto muy relacionado con todo esto es la inteligencia artificial (IA), donde se busca que las computadoras puedan empezar a entender el mundo del mismo modo que los humanos. Lo que se busca es recrear la inteligencia humana: para ello, se estudia el aprendizaje de máquina; es decir, se crean computadoras para que a partir de ciertas experiencias en el ambiente se tomen mejores decisiones y predicciones. Actualmente un aprendizaje de máquina muy popular es el llamado *machine learning*, debido a que se ha mostrado que se pueden crear muchos nuevos servicios de un modo óptimo, por ejemplo, en la fabricación de vehículos autónomos o servicios inteligentes de gobierno digital.

Sin embargo, a pesar de los grandes avances de la inteligencia artificial y los novedosos servicios que está brindando, es crucial entender también los problemas que la inteligencia artificial puede traer. Para poder entender por qué puede ser problemática la IA, el aprendizaje de máquina y la protección de los datos personales (DP), es importante que entendamos cómo es que funciona el aprendizaje de máquina y la IA a grandes rasgos. Primero, se comienza con la recolección de datos masivos (*Big Data*), después se limpian los datos (especialmente cuando provienen de distintas fuentes), posteriormente se buscan patrones en los datos (los datos se modelan y se sacan distintas características de ellos que suelen llamarse *features*), para que por último estos datos modelados puedan alimentar el modelo de IA, que irá aprendiendo a partir de los patrones que va encontrando.

Ahora bien, es importante mencionar que dentro de este proceso puede haber sesgos y problemas respecto a los DP que se tienen. Por ello es importante analizar qué tipo de datos personales es considerado por la IA, porque el sesgo en los datos puede traer sesgos en el tipo de interacciones y servicios digitales que reciben las personas, y esto puede crear una serie de daños. Por tal razón, es muy importante que se analice cada parte de cómo entran y salen los datos personales en la inteligencia artificial para identificar sesgos y pensar a detalle cómo se podría utilizar la información de manera correcta y minimizar daños a las personas.

Esto de analizar a detalle el funcionamiento de la inteligencia artificial con datos personales y los daños que se pueden generar es crucial, especialmente debido a que las máquinas están comenzando a tomar decisiones en lugar de las personas. Por ejemplo, podemos tener algoritmos inteligentes que ahora son los que deciden qué personas van a ser entrevistadas con base en los datos personales que comparten de su carrera laboral. Dado que ya tenemos a la inteligencia artificial operando dentro del mundo real (en vez de sólo en laboratorios cerrados), se debe de analizar a detalle cómo las máquinas están tomando esas decisiones, cómo se está diseñando esa tecnología y analizar si, en su caso, se podría utilizar para crear sesgos en la población e incluso daños significativos (por ejemplo, hacer que ciertas personas pierdan su trabajo o no tengan acceso a trabajos justos sólo porque la inteligencia artificial tiene sesgos que desechan el perfil de ciertas personas, como podrían ser las mujeres). Por esto es sumamente importante que se diseñe tecnología inteligente de modo adecuado.

En el flujo de cómo funciona la IA, es muy importante pensar cómo asegurarnos que nuestras máquinas piensen éticamente utilizando los DP sin aterrorizar a la ciudadanía. Un modo de lograrlo es integrando constantemente a diversos ciudadanos para que con ellos se pueda entender e identificar los sesgos que puede tener la inteligencia artificial.

## *Inteligencia artificial, Datos Personales e Infraestructura Computacional Pública*

Dentro de este contexto es importante también considerar que, con miras a utilizar la IA y los DP dentro del gobierno para crear innovación, es importante crear infraestructura pública para que el gobierno en conjunto con la ciudadanía, las Organizaciones No Gubernamentales e industria puedan compartir, utilizar y acceder a datos y también estén en posibilidades de realizar investigaciones de IA e innovar. Lo anterior es crucial debido a que actualmente son las grandes empresas de tecnología (Google, Facebook, Microsoft) las que realmente tienen más acceso a la infraestructura computacional necesaria para innovar en el área de inteligencia artificial. Sin embargo, esto crea sesgos en el tipo de investigaciones e innovaciones que se realizan (estas grandes empresas van a favorecer siempre sus propias ganancias que ver por el bien social). Por ello, se considera importante que el gobierno comparta cierta infraestructura computacional pública para que más ciudadanía y más instituciones puedan hacer sus propias investigaciones e innovaciones en la IA.

## *Inteligencia artificial y Datos Personales en Gobierno*

Adicional a lo mencionado, se debe combinar DP con IA para brindar mayores servicios de innovación a la ciudadanía. Por ejemplo, la Secretaría de Relaciones Exteriores con nuestro laboratorio en la UNAM se encuentra trabajando en el diseño de asistentes virtuales inteligentes para que tomen el control de ciertas actividades y trámites en los casos en que para la persona empleada de gobierno la atención a la ciudadanía resulte muy repetitiva. Sin embargo, el asistente virtual va a manejar gran cantidad de datos personales de la ciudadanía, por lo que resulta sumamente importante tener buena ciberseguridad.

Asimismo, la Secretaría de Mujeres de la Ciudad de México, también en colaboración con nuestro laboratorio de la UNAM, está ayudando a víctimas de violencia doméstica, y por ello resguardan DP de las personas. Nosotros con el laboratorio de aceleración de las Naciones Unidas creamos interfaces inteligentes que ayudan a las servidoras públicas a tomar mejores decisiones de cómo dar seguimiento a las mujeres que sufren violencia a efecto de reducir la cantidad de feminicidios en la ciudad y proteger sus datos personales.

Es importante pensar en la IA con DP como algo interactivo, algo que constantemente se debe de estar mejorando para que se puedan detectar los diversos sesgos que pueden existir, a efecto de evitar discriminación, brindar mejores servicios, crear cambio e impacto social, y así brindar mayor apoyo a la ciudadanía.

La transmisión de conocimientos sobre estos temas abonará sin duda a la toma de conciencia sobre la corresponsabilidad en el tratamiento de datos personales; lo cual desde mi punto de vista es el valor intrínseco de la Ruta de la Privacidad. Tuve el gusto de compartir espacio con el órgano garante de Tlaxcala, quien a través de su impulso y convicción sobre la materia nos permitió a todos los participantes del evento difundir la relevancia de la interacción armónica entre tecnología y privacidad, pero, sobre todo, insisto, en la necesidad de hacer un frente común para garantizar la protección de datos personales a favor de la sociedad.

# IDENTIDAD DIGITAL

LORENA NARANJO GODOY

*Directora de la Maestría en Derecho digital e innovación y docente de la Universidad de las Américas de Ecuador*

PhD cum laude en Ciencias Jurídicas y Políticas y Máster en Derecho de Nuevas Tecnologías por la Universidad Pablo de Olavide, Sevilla. Investigadora, consultora BID, docente y autora de artículos académicos. Autora y líder del proceso de aprobación de la *Ley de Protección de Datos Personales* para el Ecuador y de otras normas que permitieron su implementación en el Sistema Nacional de Registro de Datos Públicos cuando fue Directora Nacional de DINARDAP.

Ejerció como Directora de la Escuela de Derecho de la UDLA; Subsecretaria de Desarrollo Normativo del Ministerio de Justicia, Derechos Humanos y Cultos; asesora de la Presidencia de la Corte Nacional de Justicia; y Directora Nacional de la Dirección de Registro de Datos Públicos. Actualmente, es directora de la Maestría en Derecho Digital e Innovación de la UDLA, y líder del Área de Derecho Digital y Protección de Datos Personales de Spingarn & Marks S.A.

Históricamente, la primera aproximación del derecho a la identidad se encuentra en la Declaración de los Derechos Humanos de 1948, que alude a la personalidad jurídica como el reconocimiento de que todos los humanos son titulares de derechos, para lo cual es necesario individualizarlos.

Posteriormente, en el Argentina las abuelas de la Plaza de Mayo exigían que los niños y niñas separados de sus padres en la época de la dictadura pudieran ser informados sobre las condiciones de sus adopciones y quiénes eran sus progenitores para desarrollar un ejercicio de identidad basado en el derecho a la verdad.

De otro lado, la inscripción obligatoria en el Registro Civil se transforma en una obligación estatal de recopilar atributos de la personalidad para identificar a un ciudadano a un derecho fundamental, el derecho a la identidad, que se reconoce desde el nacimiento, artículos 7 y 8 de la Convención sobre los Derechos del Niño (1989). A través de la inscripción de nacimiento y de la gestión de los atributos de la personalidad en los registros civiles se contribuye a la conformación de la identidad (Claverie, 2021). En Ecuador, la identidad es derecho un derecho reconocido en el artículo 66 numeral 28 de la Constitución que incluye elementos como «nombre y apellido, debidamente registrados y libremente escogidos; conservar, desarrollar y fortalecer las características materiales e inmateriales de la identidad, tales como la nacionalidad, la procedencia familiar, las manifestaciones espirituales, culturales, religiosas, lingüísticas, políticas y sociales». Podemos concluir que en la identidad confluyen los atributos de la personalidad como elementos que permiten la individualización, un sentido existencial de «quién soy» y una proyección en sociedad.

La identidad como derecho fundamental tiene una dimensión material y una digital. Es decir, no sólo debe ser garantizada en el mundo físico, sino también entornos digitales. La primera se obtiene a través de una identificación física, realizada mediante la inscripción el Registro Civil de cada país. La segunda, la identidad digital que a su vez se divide en identidad digital legal e identidad digital universal (BID, 2017). Cobra principal importancia la identidad digital, pues un país digital es aquel conformado por un gobierno digital, empresas y ciudadanos digitales (BID, 2021). Y para construir un país digital, como lo menciona el ex presidente de Estonia, Toomas Hendrik Ilves, el primer pilar es la identidad digital.

En este sentido, la identidad digital legal tiene dos manifestaciones. La primera, a través de asignación de un usuario y contraseña para el acceso a servicios digitales gubernamentales. Los Estados suelen centralizar la atención a sus ciudadanos a través de una ventanilla única de trámites digitales, a la que se puede acceder a través de una identidad digital que se genera mediante una clave de acceso y de mecanismos de seguridad (BID, 2017).

La segunda se produce a través de la firma electrónica, que además de la identificación y la autenticación permite la manifestación de voluntad del ciudadano y la asunción de responsabilidades de conformidad con la Ley.

De otro lado, la identidad digital universal se forma del rastro o huella digital que va definiendo las características con las cuales se individualiza a una persona (Naciones Unidas, 2019); de la propia proyección al mundo; y de la percepción pública. Esta última difiere del contenido esencial del

derecho a la identidad física y en cambio es intrínseca de la identidad digital universal. Es decir, la reputación en línea que puede ser positiva o negativa es parte de este cúmulo de información digital que se define como identidad digital.

Asimismo, los derechos nacidos en el mundo físico se complejizan en el mundo digital pues su contenido pareciera chocar con otros derechos fundamentales, lo que suele generar confusión, que dificultan su exigibilidad, ya que se considera que sólo se está perjudicando a un derecho cuando en realidad se puede estar afectando varios derechos simultáneamente. (Naranjo Godoy, 2017). Una misma acción puede significar una transgresión al derecho a la identidad: por ejemplo, el robo de identidad; una afectación al derecho a la propiedad, en el caso del *phishing*; un derecho a la imagen, las *deepfake*; el derecho a la identidad sexual de niños, niñas y adolescentes, el *grooming*, adulto que se hace pasar por un niño y genera una identidad falsa que le habilita el cometimiento de un delito.

Estos derechos en el mundo digital tienen como manifestación básica al dato personal. Por lo que podríamos sostener que a través del derecho a la protección de datos personales se pudiera llegar a proteger otros derechos como la identidad digital y la reputación en línea. Esto en la medida en la que, protegiendo los datos personales o incluso fragmentos de datos personales, con los que se pueden construir perfiles completos de una persona, se puede garantizar la autodeterminación informativa de un individuo (Naranjo Godoy, 2017). Sin duda, el derecho a la protección de datos personales puede usarse para proteger a la persona cuando no existe un reconocimiento de la naturaleza digital de la identidad o de las caracterizaciones o dimensiones digitales de la identidad, pero desde una visión garante de la dignidad humana es necesario construir nuevos paradigmas o completar los existentes para garantizar una verdadera protección.

Por lo tanto, en un mundo cada vez más tecnologizado se debe invocar la dimensión digital de los derechos fundamentales y de ser necesario reconocer expresamente nuevas manifestaciones y dimensiones como la identidad digital legal que permita el ejercicio de derechos, especialmente frente a la digitalización de los estados; y la identidad digital universal que proteja al humano de las diversas formas de transgresión en línea. Es decir, que desde un enfoque de defensa del libre desarrollo de la personalidad y de la autoconstrucción de la persona en sociedad se proteja de forma integral la dignidad humana que ahora también es digital.

## *Referencias:*

Naciones Unidas. *Informe sobre la Economía Digital 2019. Creación y captura de valor: Repercusiones para los países en desarrollo*. Conferencia de las Naciones Unidas sobre el Comercio y Desarrollo, (2019) https://unctad.org/es/system/files/official-document/der2019_overview_es.pdf

Naranjo Godoy, L. (2018). El dato personal como presupuesto del derecho a la protección de datos personales y del habeas data en el Ecuador. *Foro: Revista De Derecho*, 1(27), 63–82. Recuperado a partir de https://revistas.uasb.edu.ec/index.php/foro/article/view/501

Roseth, B., Reyes, A., Antiso, C. (Eds)., Farias, P., Porrúa, M., Villalba, H., Acevedo, S., Peña, N., Estevez, E., Lejarraga Linares, S., y Fillotrani, P. *El fin del trámite eterno: Ciudadanos, burocracia y gobierno digital*. Inter-American Development Bank, (2018). http://dx.doi.org/10.18235/0001150

García Mejía, M., Molina, A., Reyes, A., y Roseth, B. *Gobiernos simples y digitales para servir al ciudadano: Número 7: Construyendo un Estado orientado al ciudadano: Lecciones aprendidas del Plan Nacional de Simplificación de Trámites de Ecuador*. Inter-American Development Bank, (2018). http://dx.doi.org/10.18235/0001223

e-Estonia. (s.f.) entrar a e-Estonia: la sociedad digital más impresionante. [Archivo PDF]. e-Estonia. https://e-estonia.com/wp-content/uploads/e-estonia-191126-konekaartidega-es.pdf

Diario Oficial de la Unión Europea. *Reglamento (UE) No 910/2014 del Parlamento Europeo y del Consejo*. (2014) Recuperado de https://www.boe.es/doue/2014/257/L00073-00114.pdf

Banco Interamericano de Desarrollo. *Gobierno Digital.* 2.ª Edición. [Material de estudio]. https://cursos.iadb.org/es/indes/gobierno-digital

Pareja, A., Pedak, M., Gómez, C. y Barros, A. *La gestión de la identidad y su impacto en la economía digital*. (2017) http://dx.doi.org/10.18235/0000786

Claverie, D. (s.f). Violencia y Derechos de Niñas, Niños y Adolescentes… construyendo entornos de paz. [Material de estudio].

Naranjo Godoy, L. «Situación de la protección de datos personales en Ecuador». *Cálamo/ Revista de Estudios Jurídicos*, (13), 2020,6-33. https://calamo.ec/number/13

# WOMEN AND RIGHT TO INFORMATION AND DATA PROTECTION

ZAHRA MOSAWI

*Ex Comisionada de la Comisión de Acceso a la Información de Afganistán*

Zahra Mousawi completó su educación primaria en la tierra de la emigración y, a pesar de varios años de privación de educación, se graduó de la escuela Sarullah de afganos que viven en Irán con una licenciatura en Matemáticas y Física.

Después de regresar a casa, ingresó en la Facultad de Filosofía y Sociología de la Universidad de Kabul y, con su gran interés en las discusiones sociológicas y filosóficas, culminó sus estudios superiores. Durante y después de sus estudios, se involucró en actividades de los medios y publicó numerosos artículos en los campos de la mujer, la cultura y la sociedad. Comenzó su carrera mediática en el periódico *Vazin Rah-e Nejat* en 2005 como periodista y editor de *Today's Family*. Trabajó como periodista de éxito en otros medios impresos del país, como el periódico *Cheragh*, el semanario *Jame'e*, el periódico *Mandegar*, el semanario *Avae Mehr* y el periódico *Nakhl*.

Desde 2010, fue editora en jefe del Ministerio de Asuntos de la Mujer durante 6 años. *Ershad Al-Neswan* es la primera revista para mujeres en Afganistán (el primer número de la cual se publicó durante el reinado de Shah Amanullah. Apareció en estos medios como una mujer comprometida con los problemas y preocupaciones de las mujeres, enfatizando el empoderamiento de las mujeres en la publicación de artículos y entrevistas con mujeres de élite y conocedoras.

Mientras trabajaba para el Ministerio de Asuntos de la Mujer, recibió una beca a la India para estudiar durante dos años, complementando con éxito su maestría en sociología por la Universidad de Bangalore. Posteriormente, tuvo una corta experiencia en la oficina de la GIZ (cooperación alemana con Afganistán) como consultora de relaciones públicas, hasta

que fue nombrada miembro de la Comisión de Acceso a la Información durante cinco años por decreto del presidente de Afganistán.

El desempeño de sus funciones en la Comisión de Acceso a la Información ha impulsado temas sobre libertad de expresión y medios de comunicación, con el fin de fortalecer la cultura de la información en su país.

My participation in the *Privacy Route* took place on the occasion of the invitation made by the Executive Secretariat of the Jalisco's State Anticorruption System from Mexico in order to commemorate the International Women's Day. For me, as ex Commissioner of Access to Public Information in Afghanistan was such a pleasure to have had this opportunity in the Women's Day.

Women have always been victims of discrimination and inequality in some way. We have been fighting for equality for years and have forced the government decision-makers to accompany them to achieve their rights. Inequality and discrimination cause women to be deprived of their fundamental rights. For this reason, women's empowerment has been placed on the agenda and considerable progress has been made at the national and international levels.

This has caused women achieve economic self-sufficiency, have a meaningful presence at the leadership level, and be involved in policy making. But there is still a long way to go to make gender equality a reality. However, despite women's achievements in different areas, no significant work has been done to empower women in exercising Right to Information and data protection.

Personal Data Protection, as the right to information or Access to Information Right are keys and empowering rights.

Those rights are enables people to know, protect and exercise their rights. There is a prerequisite for human fundamental rights Through these rights, it is possible to empower the citizenship to full exercise their rights and make public authorities accountable. From this perspective, those can play a key role in empowering women and gender equality.

Access to information and personal data is vital for women's empowerment. Because is significant to ensure women are able to push power holders more accountable and guarantee their rights, as education, health, security, or access to a better life. For example, these rights enable them to change the injustice situation and help to understand and exercise their fundamental rights, an also to participate in political decisions, recognize gender inequalities and provide solutions to eliminate them.

These fundamental rights are power for the Women. The exercise and

guarantee of these rights should not be excluded from the list of priorities for women's empowerment. Information is considered as a power in digital age, and more access to information, public and personal, means more success and progress in various fields. It is essential for women to have access to full and accurate information at each step of the decision-making process. It makes them to engage and influence the process.

Despite of importance of access to information in women's lives, but evidence demonstrate that women do not effectively exercise their right to information at the same rate as men. Women are most in need of information to combat all forms of inequalities, but there are structural obstacles and barriers that undermine their ability to fully exercise this right.

Obviously, the potential benefit of the right of access to information is limited to men in patriarchy societies. Illiterate, poor, or rural women face more restrictions to exercise this right. In fact, all the obstacles that women face in a discriminatory society cause them to face challenges in exercising their right to freedom of information. This shows that in practice, the implementation of gender equality policies has not been effective enough and there are varied factors which prevent women from accessing this right.

Unfortunately, the gendered dimensions of the right of access to information and data protection has not been given enough attention. It is necessary to look at this critical issue from different perspectives. Women are both vulnerable and suffer the greatest due to the limited access to information and this requires affirmative action. A set of policies and practices must be applied to include women in exercising right to know and providing meaningful information to address women's issues. While the opportunities for women are not equal and they face many obstacles to use their rights, affirmative action should be used to equalize opportunities.

Gender equality is a goal that governments must act under Sustainable Development Goals (SDG) commitments, and it could be reached with the access of public information and guarantee the data protection of the vulnerable groups as the women are.

Governments have the duty to define effective plans and mechanisms to implement and evaluate these commitments as a priority. Civil society organization expects to advocate for women's access to information and data protection, identify limitations and obstacles in exercising their right, monitor progress on freedom of information for women and support affirmative action. As well as RTI organizations need to have a specific policy to encourage women to exercise right to know and Women's rights organization should pay more attention in this regard.

Finally, despite all efforts, women still suffer from gender inequality, and achieving equal opportunities for women in society is still associated with many challenges. It is necessary to use all capacities to empower women and listen to women's voices to eliminate discrimination and inequalities. Desirable changes will be visible only when there is a collective action and women are fully aware of their rights and be motivated to end gender inequality. Of course, in this way, the role of policy makers in accompanying women is quite effective and undeniable.

I wish for success of women's movements around the world. Be victorious and successful!

# MUJER: DERECHOS A LA INFORMACIÓN Y DE PROTECCIÓN DE DATOS PERSONALES

Mi participación en la Ruta de la Privacidad se dio con motivo de la invitación que me hizo la Secretaría Ejecutiva del Sistema Estatal Anticorrupción de Jalisco de México, derivado de la conmemoración del Día Internacional de la Mujer. Para mí, como ex Comisionada de Acceso a la Información Pública en Afganistán, fue un placer haber tenido esta oportunidad en el Día de la Mujer.

Las mujeres siempre han sido víctimas de discriminación y desigualdad de alguna manera. Llevamos años luchando por la igualdad y hemos obligado a los decisores gubernamentales a exigirles para alcanzar nuestros derechos. La desigualdad y la discriminación hacen que las mujeres se vean privadas de sus derechos fundamentales. Por esta razón, el empoderamiento de las mujeres se ha puesto en la agenda y se han logrado avances significativos a nivel nacional e internacional. Esto ha provocado que las mujeres alcancen la autosuficiencia económica, tengan una presencia significativa a nivel de liderazgo y participen en la formulación de políticas. Pero todavía queda un largo camino por recorrer para hacer realidad la igualdad de género. Sin embargo, a pesar de los logros de las mujeres en diferentes áreas, no se ha realizado un trabajo significativo para empoderar a las mujeres en el ejercicio del Derecho a la Información.

La Protección de Datos Personales, como derecho a la información o

Derecho de Acceso a la Información, es derecho fundamental y habilitante.

Esos derechos son los que permiten a las personas conocer, proteger y ejercer sus derechos. Hay un requisito previo para los derechos humanos fundamentales. A través de estos derechos, es posible empoderar a la ciudadanía para ejercer plenamente sus derechos y responsabilizar a las autoridades. Desde esta perspectiva, pueden jugar un papel clave en el empoderamiento de las mujeres y la igualdad de género.

El acceso a la información y la protección de datos personales es vital para el empoderamiento de las mujeres. Porque es importante asegurar que las mujeres tengan la capacidad de responsabilizar más a las personas en el poder y que éstas exijan cuentas y garanticen sus derechos, como la educación, la salud, la seguridad o el acceso a una vida mejor. Por ejemplo, estos derechos les permiten cambiar la situación de injusticia y ayudan a comprender y ejercer sus derechos fundamentales, así como a participar en las decisiones políticas, reconocer las desigualdades de género y brindar soluciones para eliminarlas.

Estos derechos fundamentales son poder para las Mujeres. El ejercicio y garantía de estos derechos no debe quedar excluido de la lista de prioridades para el empoderamiento de las mujeres. La información es considerada como un poder en la era digital, y más acceso a la información, pública y personal, significa más éxito y progreso en varios campos. Es esencial que las mujeres tengan acceso a información completa y precisa en cada paso del proceso de toma de decisiones. Les hace participar e influir en el proceso.

A pesar de la importancia del acceso a la información en la vida de las mujeres, la evidencia demuestra que las mujeres no ejercen efectivamente su derecho a la información al mismo ritmo que los hombres. Las mujeres son las que más necesitan información para combatir todas las formas de desigualdades, pero existen obstáculos y barreras estructurales que socavan su capacidad para ejercer plenamente este derecho.

Obviamente, el beneficio potencial del derecho de acceso a la información se limita a los hombres en las sociedades patriarcales. Las mujeres analfabetas, pobres o rurales enfrentan más restricciones para ejercer este derecho. De hecho, todos los obstáculos que enfrentan las mujeres en una sociedad discriminatoria hacen que enfrenten desafíos en el ejercicio de su derecho a la libertad de información. Esto demuestra que, en la práctica, la implementación de políticas de igualdad de género no ha sido lo suficientemente efectiva y diferentes factores impiden que las mujeres accedan a este derecho.

Lamentablemente, no se ha prestado suficiente atención a las dimen-

siones de género del derecho de acceso a la información y de protección de datos personales. Es necesario mirar este importante tema desde diferentes perspectivas. Las más vulnerables que más sufren por el acceso limitado a la información son las mujeres y requerían acciones afirmativas. Se debe aplicar un conjunto de políticas y prácticas para incluir a las mujeres en el ejercicio del derecho a saber y proporcionar información significativa para abordar los problemas de las mujeres. Si bien las oportunidades para las mujeres no son equitativas y enfrentan muchos obstáculos para ejercer sus derechos, la acción afirmativa debe utilizarse para igualar las oportunidades.

La igualdad de género es una meta que los gobiernos tienen que tomar acción bajo los compromisos de los Objetivos de Desarrollo Sostenible (ODS), y podría alcanzarse con el acceso a la información pública y garantizar la protección de datos de los grupos vulnerables como son las mujeres.

Los gobiernos tienen el deber de definir planes y mecanismos efectivos para implementar y evaluar estos compromisos de manera prioritaria. Se espera que las organizaciones de la sociedad civil aboguen por el acceso de las mujeres a la información y la protección de datos, identifiquen las limitaciones y obstáculos en el ejercicio de su derecho, monitoreen el progreso en la libertad de información para las mujeres y apoyen la acción afirmativa. Además, las organizaciones deben tener una política específica para alentar a las mujeres a ejercer el derecho a saber y las organizaciones de derechos de las mujeres deben prestar más atención a este respecto.

Finalmente, a pesar de todos los esfuerzos realizados, las mujeres aún sufren la desigualdad de género, y lograr la igualdad de oportunidades para las mujeres en muchas sociedades todavía está asociado con muchos desafíos. Es absolutamente necesario utilizar todas las capacidades para empoderar a las mujeres y escuchar las voces de las mujeres para eliminar la discriminación y las desigualdades. Los cambios deseables serán visibles sólo cuando haya una acción colectiva y las mujeres sean plenamente conscientes de sus derechos y tengan motivación para acabar con la desigualdad de género. Por supuesto, de esta manera, el papel de los hacedores de políticas en el acompañamiento de las mujeres es bastante efectivo e innegable.

Deseo el éxito en los movimientos de mujeres en todo el mundo. ¡Que sean victoriosas y exitosas!

# RUTA de la PRIVACIDAD

# EJE TEMÁTICO II

## *LA INTELIGENCIA ARTIFICIAL Y SUS IMPLICACIONES PRÁCTICAS*

# BUENAS PRÁCTICAS Y EVALUACIONES DE IMPACTO

HÉCTOR E. GUZMÁN RODRÍGUEZ

*Socio del área de protección de datos personales y privacidad en BGBG Abogados*

Licenciado en Derecho por la Universidad Iberoamericana; Diplomado en Derecho Corporativo por la Universidad Iberoamericana; Máster en Derecho de la Unión Europea por la Universidad Complutense de Madrid y Licenciado en Derecho por la Universidad de Zaragoza.

Miembro del Comité Editorial de *Global Privacy Law Review*.

Colaborador en la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares. Comentada*, editada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Experto certificado CIPP/E (Certified Information Privacy Professional / Europe) de la International Association of Privacy Professionals (IAPP); miembro de la Academia Mexicana de Derecho Informático (AMDI), del Colegio de Abogados de Madrid (ICAM), de la Asociación Profesional Española de Privacidad (APEP) y colaborador del Observatorio Iberoamericano de Protección de Datos (OIPRODAT).

Coautor ganador del «Premio Protección de Datos Personales de Investigación (Accésit- 2014), otorgado por la Agencia Española de Protección de Datos», y «Premio Investigación en Protección de Datos» (2018), otorgado por la Agencia Vasca de Protección de Datos.

Ha prestado servicios de asesoría y consultoría sobre protección de datos personales a diversas empresas multinacionales de origen o con presencia en México y España. Ha sido Delegado de Protección de Datos (Privacy Officer) en el Ministerio de Defensa español y ha realizado proyectos de adecuación y auditoría en materia de protección de datos personales para diversas Administraciones Públicas de España.

A la vista de los años transcurridos desde su publicación en julio de 2010, el impacto y la influencia de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (LFPDPPP) es innegable. Ello no significa que nuestro país haya sufrido una transformación radical en esta materia. No es posible afirmar —aún— que la «cultura de protección de datos personales» ha permeado en todos los aspectos de nuestro día a día, que todo titular conoce y ejerce de manera cotidiana sus derechos, ni que la mayoría de los responsables y encargados de datos personales cumple con las obligaciones que les corresponden.

Sin embargo, es indudable que los aspectos esenciales de esta ley (y de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* [LGPDPPSO]) ya están presentes en diversos ámbitos y con diferentes niveles de «intensidad».

En este sentido, son pocas las personas que aún no han escuchado hablar de un Aviso de Privacidad, y es posible afirmar que el número de denuncias y procedimientos de protección de datos personales tramitados ante el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) aumenta año con año.[43]

En este entorno y plazo de consolidación, dentro del cual nuestra LFPDPPP no ha experimentado modificaciones ni actualizaciones de ningún tipo, existen dudas razonables sobre la capacidad de esta ley (y de su Reglamento) para afrontar los retos que supone el avance e implementación de la inteligencia artificial y de los algoritmos en que ésta descansa. ¿Deben estos algoritmos y su aplicación en los ámbitos en que son utilizados cumplir con las disposiciones de la LFPDPPP? ¿Son todos los principios relativos al tratamiento de datos personales, y los deberes de seguridad y confidencialidad, aplicables a la inteligencia artificial?

Nuestra posición es que, aun dentro del margen de maniobra existente, nuestra LFPDPPP goza de una amplia aplicabilidad a todo tipo de tratamientos de datos personales, pues los principios y deberes en ella consignados deben ser aplicados a cualquier actividad de tratamiento, con independencia de la tecnología empleada para ello.

Tales evaluaciones son definidas en la LGPDPPSO como los documentos a través de los cuales:

> […] los sujetos obligados que pretendan poner en operación o modificar políticas públicas, programas, sistemas o plataformas informáticas, aplicaciones electrónicas o cualquier otra tecnolo-

[43] Cfr. Informes de Labores del INAI, en https://micrositios.INAI.org.mx/informesINAI/

> gía que implique el tratamiento intensivo o relevante de datos personales valoran los impactos reales respecto de determinado tratamiento de datos personales, a efecto de identificar y mitigar posibles riesgos relacionados con los principios, deberes y derechos de los titulares, así como los deberes de los responsables y encargados, previstos en la normativa aplicable.

Como hemos indicado, no están previstas en la LFPDPPP, con la consecuente falta de obligación para ser realizadas por parte de los «particulares» en los casos descritos.

Esta situación no es extraña para nuestro garante nacional y, durante la Mesa de Diálogo en que tuve el honor de participar, pudimos recordar que el INAI ha emitido, con sumo acierto, su *Guía para la elaboración de evaluaciones de impacto a la privacidad*[44].

Esta Guía aclara que sus disposiciones no tienen carácter mandatorio, sino orientador, y que la misma se emite para proporcionar un apoyo técnico a los responsables del tratamiento de datos personales y con la intención de que éstos puedan incorporar, como una *buena práctica*, la realización de evaluaciones de impacto a la privacidad de manera previa al lanzamiento de nuevos tratamientos de datos o la modificación sustancial de tratamientos existentes.

Hablamos de tratamientos o modificaciones que están sumamente relacionados con el uso e implementación de la inteligencia artificial, y que la Guía del INAI identifica como:

> Tratamientos de datos personales que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañen un alto riesgo para los derechos de los titulares, o
> Nuevas modalidades de tratamiento de datos personales, que, por su naturaleza, alcance, contexto o finalidades, sea probable que entrañen un alto riesgo para los derechos de los titulares.

Al carecer de exigibilidad para los «particulares», el uso de este tipo de evaluaciones no está extendido y no forma parte de los objetivos que actualmente persigue la mayoría de los responsables de datos personales al implementar y lanzar productos relacionados con la inteligencia artificial y

[44] Disponible en: https://home.inai.org.mx/wp-content/documentos/DocumentosSector-Privado/guiaeip.pdf

otras tecnologías que podrían entrañar un alto riesgo para los derechos de los particulares. Es un reto enorme difundir esta buena práctica, aunque algunos ya lo hemos aceptado: la difundimos y promovemos.

Finalmente, deseamos indicar que en esta Guía el INAI expresa la misma opinión que sostenemos, al menos, desde hace cinco años:

> […] a fin de contar con un marco legislativo y normativo adecuado en materia de protección de datos personales en posesión de los particulares, atendiendo los diversos criterios judiciales y jurisprudenciales que han surgido con motivo de su aplicación, la reforma a la LFPDPPP y a su Reglamento resultaría deseable para acreditar una conformidad plena del régimen jurídico mexicano en materia de protección de datos personales.

Esperamos que tal reforma ocurra pronto, para que nuestro país mantenga el nivel de protección y desarrollo que en esta materia ha desarrollado en beneficio, especialmente, de los titulares y de México.

# CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES DEL TURISTA

BERNARDO CUETO RIESTRA

*Secretario de Turismo del Gobierno del Estado de Quintana Roo*

Es Licenciado en Derecho por la Universidad Anáhuac México y Maestro en Gobierno y Administración Pública por la Universidad Complutense de Madrid. En el sector público, se ha desempeñado en los tres niveles de gobierno.

Durante el trienio 2009-2012, fungió como Jefe de Departamento en la Dirección General Jurídica y de Gobierno y como Director de Cultura Cívica de la Dirección General de Desarrollo Social de la entonces Delegación Cuajimalpa en la Ciudad de México.

A nivel federal, ocupó el cargo de Jefe de Oficina de la Delegación Oportunidades (SEDESOL) en la Ciudad de México. En el ámbito estatal, laboró como Director de Enlace del Gobierno del Estado de Querétaro ante la CONAGO y como Director General del Instituto para el Desarrollo y Financiamiento del Estado de Quintana Roo.

Dentro del Poder Legislativo, fungió como Asesor Parlamentario en la LXI Legislatura de la Cámara de Diputados. Actualmente, se desempeña como Secretario de Turismo del Gobierno del Estado de Quintana Roo.

Anteponiendo un cordial saludo, me permito compartir mi experiencia con relación a lo que se está haciendo en Quintana Roo en materia turística, ante este importante foro del Sistema Nacional de Transparencia; a partir del eje temático de «La Inteligencia Artificial y sus implicaciones prácticas».

Como se ha señalado, la innovación tecnológica es muy beneficiosa para el sector turístico, permitiendo que las nuevas tecnologías cambien la forma de viajar. Esto se ha convertido en una tendencia que pretende ofrecer experiencias personalizadas con el objetivo de conseguir satisfacción, a través de reservar o comprar producto turístico, involucrando

elementos como la inteligencia artificial, la automatización y el *big data*: permitiendo que dichas experiencias sean cada vez más eficientes y accesibles para todas las personas.

La contingencia sanitaria aceleró el proceso de la digitalización y conectividad en varios sentidos, por lo que la protección de datos personales se convierte en un tema importante, principalmente porque vivimos en un constante cambio y evolución tecnológica, de modo que los fraudes cibernéticos han aumentado, considerablemente, la vulnerabilidad de los turistas y de los prestadores de servicios turísticos en nuestros destinos. En este sentido, es primordial el trabajo coordinado con la iniciativa privada, fomentando la incorporación de protocolos de actuación que incluyan, entre otros, instrumentos de certificación digital que autentiquen la identidad de cualquier sitio web y habilite una conexión cifrada, infraestructura idónea en mecanismos técnicos y de seguridad, políticas en materia de seguridad cibernética, gobernanza de datos y estándares de transparencia. Con ello, se busca hacer frente al fraude cibernético.

Por lo anterior, desde la Secretaría de Turismo de Quintan Roo seguiremos impulsando la Estrategia Estatal de Protección del consumidor de Productos Turísticos y motivando a otras entidades federativas para que se sumen a esta práctica y así, de manera general en el país, podamos enfocar esfuerzos en torno a la protección de los turistas y visitantes, pero también de las empresas y prestadores de servicios. Todo ello con la firme convicción de fortalecer la imagen y competitividad turística de nuestros destinos.

De igual forma, la inteligencia artificial tiene una fuerte influencia en la actividad turística, permitiendo elevar la calidad del servicio, por lo que se espera que en el futuro tendrá un papel protagonista en innumerables procesos. Esto acelerará nuestros procesos en la toma de decisiones, por lo que será fundamental hacerlo de manera ordenada. Es vital que, como sector, reconozcamos que en Quintana Roo se busca fortalecer la calidad y confianza para generar mayor competitividad y que, sobre todo, nuestra oferta turística no decaiga.

En materia de promoción, a través del Consejo de Promoción Turística de Quintana Roo se ha potencializado el uso de canales digitales para generar conexión con nuestros mercados. Con base en el Sistema de Inteligencia e Innovación de Mercado, se analiza la percepción de nuestros principales mercados en temas como producto, seguridad y satisfacción, entre otros; permitiendo desarrollar estrategias, acciones en *marketing* y promoción específicos para cada uno de nuestros 12 destinos.

También desde la Secretaría de Turismo nos hemos enfocado en man-

tener e impulsar el liderazgo turístico de nuestros destinos. En este sentido, la recientemente reformada *Ley de Turismo del estado de Quintana Roo* establece las bases para operar la Plataforma Estatal de Servicios Turísticos *Retus Q*, un catálogo público oficial de los prestadores de servicios turísticos del Caribe Mexicano que permitirá la mejora de la gestión de la actividad turística, brindando una mejor oferta, seguridad y certeza a los turistas y visitantes, y que incluye mecanismos para la verificación de cumplimiento y la aplicación de sanciones, en caso de ser necesario.

Sin duda, las nuevas tecnologías están generando un gran valor añadido a los destinos turísticos, por lo que se debe seguir apostando por su uso y así facilitar la inversión e innovación en los nuevos modelos de negocio; promoviendo la inversión en tecnologías alternativas por parte del sector público y privado. Para Quintana Roo, la tecnología y la actividad turística son consideradas como un binomio de alta concurrencia y completa dependencia, clave para la competitividad de los destinos turísticos del Caribe Mexicano.

Agradezco al Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales por la invitación.

# LA INTELIGENCIA ARTIFICIAL Y SUS IMPLICACIONES PRÁCTICAS

CARMEN QUIJANO DECANINI

*Socia fundadora de Bufete Quijano*

Es abogada egresada de la Universidad Iberoamericana en México, donde se graduó con mención honorifica en 1996.

Es maestra en Derecho comparado por la Universidad de Nueva York y doctora en Derecho por el Instituto de Investigaciones Jurídicas de la UNAM, de donde se graduó en 2019 también con mención honorifica por su tesis titulada *La Privacidad en Internet*, que fue publicada por la Editorial Tirant Lo Blanch en 2022.

Realizó estudios de género en El Colegio de México. Ha impartido cursos y clases sobre Derecho mercantil, societario, Derechos humanos y Protección de datos personales en diversas universidades del país. Actualmente es miembro del comité editorial de la *Revista de Derecho Comparado* y la *Revista de Cuestiones Constitucionales* del Instituto de Investigaciones Jurídicas de la UNAM.

Es miembro de la Junta de Honor de la Barra Mexicana, Colegio de Abogados, A.C., en la que coordinó la Comisión de Transparencia y Protección de Datos de dicho colegio durante el bienio 2018-2020.

Carmen Quijano es socia fundadora de Bufete Quijano, una firma boutique especializada en Derecho corporativo, Competencia económica, Tecnologías de la información, Protección de datos y derechos humanos en el ámbito comercial. Ha sido reconocida por su grado de especialización y atención personalizada en las áreas mencionadas.

Vivimos una simulación tolerada por todos los agentes del ecosistema digital: tanto por los reguladores, como por los gobiernos, las empresas y los usuarios. Seguimos insistiendo en la aplicación de reglas y normas jurídicas que fueron creadas para otro entorno social, que han demostrado no ser eficaces para proteger la privacidad en línea.

Las normas de protección de datos fueron creadas antes de que existieran las redes sociales, cuando un ciudadano común y corriente no tenía el poder de comunicación que tiene actualmente y no podía afectar a otra persona como puede hacerlo hoy.

Como usuarios, sabemos que para acceder a cierta información necesitamos aceptar las políticas de privacidad y aceptamos dichas políticas sin leerlas porque ganamos tiempo y porque confiamos en que los responsables del tratamiento de datos, al tener una política de privacidad vigente, usarán nuestra información de manera adecuada. Pero en el fondo sabemos que no siempre es así.

El compromiso más importante de la carga de protección de datos recae en el usuario, que es el agente más débil del ecosistema a pesar de que debiera recaer en las empresas, las organizaciones de la sociedad civil y los gobiernos que tratan la información personal. El individuo, al dar su consentimiento sin leer y entender las múltiples políticas de privacidad de todos los servicios digitales que requiere día a día, adquiere responsabilidades legales sin percatarse de ello. Por su parte, los responsables del tratamiento de datos usan el aviso de privacidad como una liberación de responsabilidad más que como un compromiso de lealtad y respeto con sus clientes.

Es perverso y anacrónico decir que todo lo que ocurre en Internet es público porque prácticamente toda la vida de un humano transcurre en Internet de alguna forma. Basta con pensar en el papel que juega el teléfono celular de una persona en su quehacer cotidiano y podemos concluir que no hay nada más privado y accesible a la vez.

Algunos ejemplos que ilustran lo anterior son:

## *La vigilancia masiva por parte del Estado*

Se ha documentado que periodistas y defensores de derechos humanos son vigilados por los Estados mediante programas de intervención a sus dispositivos y teléfonos celulares sin obtener una orden judicial previa para ello y con programas de *software* contratados por los gobiernos con fines de seguridad pública.

Con relación a este tema, se consulta el reporte denominado «Gobierno Espía» de *R3D: Red en Defensa de los Derechos Digitales*, Artículo 19 y SocialTIC, realizado en 2017 y accesible en la Web. [45]

[45] Red en Defensa de los Derechos Digitales, «Vigilancia sistemática a periodistas y defensores de derechos humanos en México», *Gobierno espía*, https://r3d.mx/2017/06/19/

## *La huella digital y la comercialización de los hechos de la vida íntima o vigilancia masiva desde el sector privado*

Existe tecnología a la mano de cualquier empresa para que, con tan sólo cuatro datos (nombre, domicilio, teléfono celular y ubicación geográfica), puedan decidir en pocos minutos si otorgan una fianza o un crédito. Esa información se adquiere a través de programas de rastreo y perfiles digitales.

El riesgo de lo anterior es que sucedan situaciones como el caso «Cambridge Analytica», en el que, por el uso indebido de cientos de perfiles de Facebook, se influyó en las decisiones del electorado para las elecciones presidenciales de Estados Unidos de América; o un caso reciente en el que una empresa importante dedicada a recopilar y comercializar datos de localización geográfica empezó a vender en ese país información sobre mujeres que acudieron a clínicas especializadas en aborto (cuándo acudieron, de dónde son, cuánto tiempo permanecieron en la clínica, a qué grupos pertenecen, etcétera). Todo esto en el contexto de que la Suprema Corte de ese país analizaba la posibilidad de modificar las normas relacionadas con el derecho a abortar. Dicha información podría usarse para un sinfín de objetivos, desde dirigir campañas o anuncios a esas mujeres hasta penalizarlas.

## *El derecho a la privacidad entre pares*

En la era digital, cualquier persona puede afectar la privacidad de otras sin que necesariamente sea un responsable de protección de datos. Por ejemplo, los casos conocidos en México con el *hashtag Lady* o *Lord*, en los que ciudadanos comunes comparten información sobre hechos ocurridos en muy diversos contextos y esa información se hace viral.

Ése fue el caso conocido como *#Ladyprofeco*, en el que la hija del entonces titular de la Procuraduría Federal de Protección al Consumidor (Profeco) amenazó al personal de un restaurante con ordenar el cierre del establecimiento por no darle una mesa y el restaurante se clausuró por unas horas. Alguien filmó el incidente y lo subió a la Red. Algunos periódicos y medios de comunicación participaron muy activamente en la difusión de los hechos, despertando la indignación de la población al tratarse de prácticas que considerábamos propias de políticos del pasado

gobierno-espia/

y que ahora eran realizadas por un gobierno de la oposición. El titular de la Profeco perdió su trabajo y tuvo que disculparse públicamente. A pesar de que esto sucedió en 2013, si ahora se busca en Internet *Lady Profeco*, se encuentra de forma inmediata toda esta información.

El análisis de todo lo anterior tiene como objetivo generar consciencia para establecer herramientas de protección del derecho humano a la privacidad en la era digital.[46]

Es urgente establecer mecanismos para exigir y verificar que se cumplan los cientos de declaraciones de buena voluntad que han firmado las empresas y los gobiernos como parte de la llamada «Gobernanza de Internet».

En los últimos 20 años se realizó un esfuerzo muy importante de autorregulación en esta materia porque se creía que ésa era la mejor forma de abordar los retos del respeto a los derechos fundamentales ante el avance de la tecnología. Sin embargo, se ha demostrado que no es efectiva la autorregulación sin un mecanismo de rendición de cuentas.

Lamentablemente, es poco probable que en el futuro próximo se llegue a un acuerdo global vinculante con relación al comercio digital y a la privacidad en línea. Por eso nuestra legislación debe establecer medidas de protección para los ciudadanos mexicanos como por ejemplo la jurisdicción local competente cuando se afecte la privacidad de un connacional y la transparencia en el sector privado respecto del uso de la información privada de los mexicanos. Conocer a profundidad cómo se usa nuestra información es esencial para proponer una buena regulación y hacer valer nuestros derechos.

Los responsables del tratamiento de datos personales deben poner mayor énfasis en el principio de lealtad y en el concepto de confianza y no tanto en el principio de consentimiento. Para ello se requiere modificar la normatividad vigente con el fin de que el usuario tenga la posibilidad real de dar su consentimiento libre e informado para el uso de su información privada en el ciberespacio.

Cabe destacar que estoy a favor de las redes sociales y de los avances tecnológicos. El Internet de las Cosas ha traído muchos beneficios a la Sociedad, pero urge un cambio radical que permita proteger las libertades del humano en este nuevo entorno digital.

Sí es posible gozar a la vez del avance tecnológico y de los derechos humanos. Ése es el reto de nuestra era. Para lograrlo hay que crear y promover alianzas nacionales e internacionales que permitan fortalecernos y

[46] Quijano Decanini, Carmen, *El derecho a la Privacidad en Internet*, México, Tirant lo Blanch, 2022.

hacer efectivos nuestros derechos.

Hay que abonar a los esfuerzos que ya se han hecho en este tema. Por ejemplo, el Convenio 108 de Europa, que ya fue suscrito por México, o los esfuerzos de la Asociación Internacional de Profesionales de Privacidad (IAPP), que coinciden en que:

> La responsabilidad siempre recae en el individuo para dar su consentimiento, o no, con políticas de privacidad muy complejas de leer. Necesitamos adoptar un enfoque diferente: la empresa debe garantizar la equidad. El usuario debe tener la capacidad de elegir, no sentirse obligado a dar su consentimiento.[47]

Hace sólo unos días, el presidente de Microsoft, Brad Smith, dijo en una reunión internacional en Londres que «regular no va a ser fácil, no va a ser ni será algo bonito, pero podemos hacerlo lo mejor posible».[48] Así lo decía también el doctor Jorge Carpizo: «Legislar respecto a la información es políticamente un problema difícil y delicado...» y «la peor política al respecto es la de dejar hacer, dejar pasar, porque entonces unas cuantas empresas logran imponer sus intereses particulares a los de la sociedad».[49]

Puedo sostener, sin temor a equivocarme, que la Privacidad será el derecho humano más importante de este siglo. La Privacidad en su nueva acepción evolucionada, como derecho a la autodeterminación informativa y a construir la propia identidad, será esencial para hacer valer otros derechos humanos como el derecho a decidir libremente.

Los exhorto a insistir en continuar trabajando para lograr una reforma que promueva una autorregulación regulada y normas locales e internacionales que exijan transparencia en el sector privado y respeto a la privacidad en línea.

Con un sistema fortalecido, nadie podrá sostener nunca que la privacidad en Internet no existe. El derecho a la privacidad en línea existe, está y estará más vivo que nunca.

[47] Visitar: https://iapp.org/conference/iapp-data-protection-intensive-uk/

[48] *Ibidem*.

[49] Carpizo, Jorge, «Constitución e información», en Hernández Antonio, María y Valadés, Diego, *Estudios sobre federalismo, justicia, democracia y derechos humanos, homenaje al maestro Pedro J. Frías*, México, UNAM, Instituto de Investigaciones Jurídicas, 2003, p. 50.

# LA INTELIGENCIA ARTIFICIAL: RIESGOS A LA PRIVACIDAD

DIEGO GARCÍA RICCI

*Profesor Investigador de la Universidad Iberoamericana*

Abogado por la Escuela Libre de Derecho, Maestro y Doctor en Derecho por la Universidad de Toronto, Canadá. Es miembro del Grupo Consultivo de Privacidad de Facebook LATAM y del Sistema Nacional de Investigadores. Es profesor-investigador del Departamento de Derecho de la Universidad Iberoamericana, donde también se desempeña como Procurador de Derechos Universitarios y Director de la revista *Jurídica Ibero*.

Ha sido profesor en la Escuela Libre de Derecho, en la Facultad de Derecho de la Universidad Autónoma del Estado de México (UAEM) e INFOTEC. En el servicio público ha trabajado en el CIDE, IFAI y CNDH.

Es autor de *El Derecho a la Privacidad* (Nostra, 2017) y de diversas publicaciones relacionadas con los derechos a la información, a la privacidad y a la protección de datos personales. La más reciente, *Privacidad e Identificación Forense de Personas Desaparecidas*, fue financiada por la Cooperación Alemana al Desarrollo Sustentable (GIZ).

Al reflexionar sobre el tema de inteligencia artificial, recordé que hace algunas décadas, con el advenimiento de la sociedad de la información en los años sesenta del siglo pasado, empezaron a darse los primeros procesamientos de información personal. Como sucede actualmente con el uso de algoritmos, las sociedades de los sesenta comenzaron a tener nuestras mismas preocupaciones: ¿el tratamiento de datos personales dará más poder a quien lo lleve a cabo? La tecnología siempre ha sido una constante en el desarrollo de las civilizaciones. El advenimiento de una nueva era —esto es, la era de la inteligencia ar-

tificial— nos presenta nuevamente esa vieja pregunta. Sólo que ahora nos enfrenta a un reto nuevo: la ausencia de una regulación específica en materia de inteligencia artificial.

La inteligencia artificial se refiere a la teoría y el desarrollo de sistemas de cómputo capaces de llevar a cabo ciertas tareas que usualmente requieren de la inteligencia humana, como la percepción visual, el reconocimiento de voz, la toma de decisiones o la traducción de idiomas. El concepto de *machine learning* o aprendizaje automático va de la mano con la inteligencia artificial y refiere a la habilidad que tienen los *software*s de aprender sin estar específicamente programados.

Entre los beneficios sociales de la inteligencia artificial podemos identificar que ésta cambia la manera en que los individuos y los grupos de ciudadanos se relacionan entre sí. Organizaciones defensoras de derechos humanos como Artículo 19 y Privacidad Internacional han señalado que la inteligencia artificial moldea la forma como la gente accede a la información, interactúa con dispositivos electrónicos, comparte información personal e incluso entiende otros lenguajes.

## *Riesgos de la inteligencia artificial*

A pesar de que la inteligencia artificial nos ofrece grandes comodidades digitales en el mundo moderno, también nos pone frente a escenarios que desafían nuestra privacidad. La inteligencia artificial tiene la capacidad de identificarnos y rastrearnos a partir de los datos que nosotros generamos, lo que representa riesgos en el ejercicio de nuestros derechos y libertades fundamentales, entre los que podemos destacar:

- *Acceso a la Información:* Solemos acceder a la información en línea a través de redes sociales digitales y motores de búsqueda que utilizan sistemas de inteligencia artificial y algoritmos que controlan la información con la cual interactúan los usuarios. Dichos sistemas funcionan, no obstante, de forma poco transparente. El riesgo de estos diseños es que la opinión que puede formarse un usuario podría no estar apegada a la realidad, pues los mecanismos que utilizan los motores de búsqueda pueden tener información falsa desactualizada o fuera de contexto.
- *Derecho a la Privacidad y a la Protección de Datos Personales:* La inteligencia artificial ha desvirtuado el gozo que sentimos en el espacio público a través del anonimato. Los sistemas de reconocimiento facial —que utilizan algoritmos—trastocan esa sensación de anonimato, debido a su capacidad para identificarnos.

Otro derecho que se pone en riesgo es el derecho a la protección de datos personales, pues los algoritmos tienen capacidad de recolectar una gran cantidad de datos y pueden hacerlo sin el consentimiento de las personas.

En 2018, la American Civil Liberties Union llevó a cabo un experimento que resultó perturbador. Utilizó el sistema de reconocimiento facial de Amazon y, al comparar los rostros de 335 miembros del Congreso con un universo de 25,000 personas que habían sido arrestadas y tratar de ver quiénes de ellos coincidían, encontraron 28 coincidencias falsas. Ahora, si nosotros traducimos una coincidencia falsa a sistemas que utilizan el reconocimiento facial para fines sociales como puede ser la administración de justicia, el tema se vuelve más preocupante, como ya se dio en EEUU, donde las policías empezaron a usar sistemas de inteligencia artificial para tratar de perseguir el delito. Si el uso de estos sistemas da lugar a reconocimientos falsos, estaríamos en problemas mucho más complejos. Hoy por hoy, EEUU ha empezado a dejar atrás el uso de sistemas de inteligencia artificial de reconocimiento facial precisamente porque ofrecen muchas fallas, por lo que es necesario actuar con cautela.

> *No Discriminación:* Existen sesgos discriminatorios con base en los cuales se construyen los algoritmos de la inteligencia artificial. Por ejemplo, la UNESCO y la organización Equals, que busca promover la igualdad de las mujeres, encontraron que casi todas las asistentes de voz de Amazon, Microsoft, Apple, usaban nombres de mujeres: Alexa, Cortana, y Siri. Esta situación refleja el estereotipo de que las mujeres son las asistentes; algo que, como sociedad, hemos ido trabajando para desvirtuar.

## *¿Cuáles podrían ser las soluciones?*

Lo cierto es que todavía no hemos creado el sistema normativo adecuado para regular el uso de la inteligencia artificial. Existen, no obstante, algunos avances destacables. Me referiré a dos relevantes:

Los valores éticos desarrollados por el Grupo Asesor sobre Ética de la Unión Europea[50], los cuales prevén los principios de la dignidad, la libertad, la autonomía solidaridad, la igualdad, la democracia, la justicia

[50] European Commission, "Ethics guidelines for trustworthy AI", *Shaping Europe's digital future*, Publication 08 April 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai

y la confianza. Si vamos a construir sistemas de gobernanza a través de marcos normativos que orienten el desarrollo de los sistemas de inteligencia artificial, no podemos perder de vista estos principios orientadores.

Las Directrices de la OCDE de 2020 respecto a la inteligencia artificial[51], las cuales prevén el deber de construir sistemas de inteligencia artificial que respeten la libertad, la dignidad, la autonomía, la diversidad, la protección de datos personales, la no discriminación, la equidad, la justicia, así como los derechos laborales internacionalmente reconocidos.

Me parece muy importante que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y los organismos garantes del derecho a la protección de datos personales de todo del país hayan creado la Ruta de la Privacidad, la cual consistió en la celebración de diversas jornadas en las que diversos especialistas discutieron problemas vinculados con nuestra privacidad. Es necesario promover en México estos espacios de reflexión y divulgación del conocimiento de nuestros derechos a la privacidad y a la protección de datos personales, con una visión de largo plazo, en la que podamos tomar conciencia de cuáles son sus grandes desafíos, los cuales, en este caso, estuvieron relacionados con la inteligencia artificial.

[51] Jamie Berryhill, Kévin Kok Heang, Rob Clogher, Keegan McBride. «Hola mundo: La Inteligencia Artificial y su uso en el sector público», *Documentos de trabajo de la OCDE sobre gobernanza pública*, N.° 36, https://www.oecd.org/gov/innovative-government/hola-mundo-la-inteligencia-artificial-y-su-uso-en-el-sector-publico.pdf

# LA INTELIGENCIA ARTIFICIAL Y EL CONTROL DE LOS DATOS PERSONALES

JONATHAN MENDOZA ISERTE

*Secretario de Protección de Datos Personales*
*Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*

Es Doctor y Maestro en Derecho por el Centro de Estudios de Posgrado en Derecho y Licenciado en Derecho por la Universidad Nacional Autónoma de México. Cuenta con un Máster en el Reglamento General de Protección de Datos de la Universidad Nacional de Educación a Distancia y con un certificado de aptitud en el curso de especialización Cibersecurity Summer Bootcamp - Policy Makers, organizado por la Universidad de León, España, y el Instituto Nacional de Ciberseguridad (INCIBE). Actualmente se desempeña como Secretario de Protección de Datos Personales en el INAI.

Nos encontramos rodeados de nuevas tecnologías y sistemas de inteligencia artificial (IA) que prometen facilitar y mejorar nuestra experiencia como usuarios de los diversos servicios digitales que existen en el ecosistema. Desde la aplicación para realizar nuestras compras habituales, como el seguimiento y monitoreo de salud en los diversos dispositivos inteligentes que utilizamos.

Lo anterior representa un riesgo si como usuarios no somos conscientes de la información que compartimos y los permisos que concedemos para el tratamiento de nuestros datos personales a estos servicios digitales, que podrían repercutir en vulneraciones a nuestra información.

Hemos volcado nuestros discursos hacia los graves riesgos derivados de las tecnologías que conllevan el uso de sistemas de IA. Sin embargo, debemos detenernos a pensar que, más allá del uso de estos sistemas, debemos

orientar la discusión al valor agregado que tendría que los desarrolladores reflexionaran ante cada nueva oportunidad sobre el respeto a los derechos a la privacidad y la protección de datos personales. Un mecanismo útil para ello son los esquemas de privacidad por diseño que actualmente se materializan a través de las tecnologías que ayudan a mejorar la privacidad (PET, en inglés).

Este hecho ha quedado plasmado en las legislaciones en materia de protección de datos personales y privacidad que han sido promulgadas en los últimos años. Como hemos visto, contemplan además el principio de responsabilidad demostrada como un mecanismo necesario para la rendición de cuentas en el desarrollo de innovación tecnológica con sistemas de IA.

Tal ha sido la importancia dada a este tema, que actualmente forma parte no sólo de las agendas de trabajo de las autoridades de protección de datos alrededor del mundo: además se ha convertido en tema de organizaciones internacionales que lo señalan como una cuestión pendiente de regular y para la que ya han sido promulgados lineamientos y principios a nivel global y regional.

Ejemplo de lo anterior es el trabajo que ha venido realizando la Asamblea Global de Privacidad (GPA, en inglés), a través de su resolución adoptada sobre la rendición de cuentas responsable (y demostrable) en el desarrollo y la utilización de la inteligencia artificial de 2020 y su grupo de trabajo; los principios de la Organización para la Cooperación y el Desarrollo Económicos (OCDE) sobre inteligencia artificial de 2019; así como las Recomendaciones Generales para el tratamiento de datos en la inteligencia artificial y las Orientaciones específicas para el cumplimiento de los principios y derechos que rigen la protección de los datos personales en los proyectos de inteligencia artificial, de la Red Iberoamericana de Protección de Datos de 2019.

Es así como la constante evolución tecnológica y el uso masivo de información hacen que los cuerpos normativos nunca se encuentren a la par del avance tecnológico. Dicha situación tiene un efecto adverso en la tutela efectiva del derecho a la protección de datos personales. Sin embargo, existen mecanismos complementarios planteados desde ópticas que utilizan principios aplicables de forma general a cualquier situación imprevisible que la rigidez normativa no permite resolver actualmente. Por ejemplo, las estrategias nacionales sobre inteligencia artificial (Brasil) o los marcos éticos digitales (Colombia).

Bajo esta perspectiva pueden construirse marcos regulatorios y normativos que sean flexibles y se adecuen a las nuevas realidades con las que nos enfrentamos, permitiendo garantizar de una mejor manera la protección de

nuestros datos personales. Para llegar a ello, es necesario realizar ejercicios previos que permitan evaluar las fortalezas y debilidades de esas decisiones legislativas. Ejemplo de ello son los entornos de prueba (*Sandboxes)* o los laboratorios de investigación en colaboración público-privada (*Open Loop*).

La importancia de que los humanos generen algoritmos neutrales, equitativos y con perspectiva de derechos humanos es uno de los grandes retos que enfrentamos en la actualidad. En ese mismo sentido, garantizar que existan mecanismos que permitan la intervención del humano en la toma de decisiones que pudieran ser trascendentales y constituyan salvaguardas de los derechos humanos en la era digital.

Como bien señala Marc Rotenberg, experto en la materia, «si vamos a tener una IA centrada en el humano, entonces los humanos deben mantener el control de la IA, y nosotros debemos mantener el control de nuestros datos personales».

# INTELIGENCIA ARTIFICIAL Y SUS IMPLICACIONES

KARLA BELEM NEGRETE HUELGA

*Profesora-Investigadora de la Facultad de Ciencias Políticas y Sociales de la Universidad Autónoma de Querétaro*

Profesora-Investigadora de la Facultad de Ciencias Políticas y Sociales de la Universidad Autónoma de Querétaro. Coordinadora Técnica del Laboratorio de Ciudadanía Digital de la UAQ. Doctoranda en Investigación de la Comunicación por la Universidad Anáhuac México; Maestra en Comunicación y Cultura Digital por la Universidad Autónoma de Querétaro; Licenciada en Comunicación y Periodismo por la Universidad Autónoma de Querétaro.

Sus reconocimientos: Finalista en los Premios de Investigación en Comunicación Digital 2019, por la Universitat Autónoma de Barcelona; Premio al Mérito Académico 2017 por la Universidad Autónoma de Querétaro; Primer lugar del XVIV Premio Nacional de Trabajos Recepcionales de Comunicación 2010 por el Consejo Nacional para la Enseñanza y la Investigación de las Ciencias de la Comunicación.

Ha publicado en revistas académicas y libros de México, España y Chile. Sus líneas de investigación son: Comunicación Política, Gobierno Digital, Ciudadanía Digital y Comunicación Digital.

La sociedad de la información y el conocimiento se caracteriza por interconectar países, comunidades y personas a través de la innovación tecnológica, a través de la digitalización de procesos industriales, sociales, políticos y económicos que modifican la manera en la que funciona la sociedad, desde sus instituciones hasta las prácticas cotidianas de sus individuos. En un mundo global interconectado, la transformación digital implica un cambio de prácticas para optar por sistemas cada vez más automatizados, que busca imitar al pensamiento

racional humano. Así es como trabaja la inteligencia artificial.

La inteligencia artificial involucra una serie de beneficios entre los que se encuentran: combatir condiciones climáticas, mejorar los procesos agrícolas, crear sistemas pluviales más eficientes y optimizar la afluencia de tráfico de las ciudades. Esto gracias a su aportación de resultados predictivos que son precisos y reducen el error humano. Su adopción en la industria, por ejemplo, es favorecedora al optimizar procesos, aumentar la productividad y tomar mejores decisiones.

Sin embargo, tras las conveniencias de su uso, es necesario comprender que su funcionamiento es resultado algoritmos programados para aprender comportamientos e ir mejorando próximos resultados. Para funcionar, entonces, se requiere de datos que son recopilados en grandes volúmenes y que pueden provenir de diversas fuentes, entre las que se encuentran las humanas. Por tanto, los usuarios de la tecnología aportan información cada vez que utilizan sus dispositivos y navegan por Internet. De esa manera, bajar una aplicación, registrarse en una plataforma, crear un correo electrónico y otras actividades más que realizamos día a día aportan datos a los algoritmos, por lo que toda acción digital genera un rastro que se comparte con diversos corporativos.

La inteligencia artificial, entonces, muestra un conflicto con la privacidad. Es inherente crear consciencia en los usuarios de las implicaciones del uso tecnológico. En un ejemplo, el acceso de redes socio-digitales requiere de la aceptación de los términos y condiciones en los que se establece el consentimiento del usuario para hacer uso de sus datos de navegación y utilización. Así, las plataformas ofrecen sus servicios de manera gratuita a cambio de datos, ya que sus modelos de negocios funcionan gracias a ellos.

El problema se deriva en la poca lectura de estos términos, en los procesos de vigilancia masiva a través de la información personal y los datos biométricos, así como el mal uso de la información para beneficios económicos o políticos. En un esfuerzo por combatir estos riesgos, la Oficina de Derechos Humanos de la ONU[52] reconoce que la inteligencia artificial afecta el derecho a la intimidad y hace un llamado a no usarla de manera ilimitada, así como incrementar la transparencia en el desarrollo de sistemas de inteligencia artificial.

Ante la oleada de automatización de procesos, es importante reflexionar y equilibrar la balanza entre sus riesgos y oportunidades en torno al uso de la información. Sin olvidar que la inteligencia artificial se desarrolla con el objetivo de hacer el bien común en las sociedades, el buen uso de

[52] Visitar: https://www.ohchr.org/en/privacy-in-the-digital-age

la información se convierte en un reto para los modelos de negocio de los grandes corporativos de las tecnologías de la información y la comunicación, que requieren de consideraciones éticas para la defensa de los derechos digitales, como el derecho a la privacidad digital.

Por una parte, sería válido afirmar que contribuir como usuarios para el desarrollo de una mejor sociedad es pertinente mientras el uso de la inteligencia artificial no viole la protección de los datos personales. Por otra, es necesario fomentar la defensa de los derechos digitales, lo que implicaría la creación de reglas y legislaciones para la protección de los datos digitales, así como de proyectos de alfabetización informacional para desarrollar usuarios más conscientes del uso de Internet y la información que consumen y comparten, ya que son ellos a través de sus prácticas los que ofrecen su información.

La inteligencia artificial llegó para quedarse, pero su uso responsable es de gobiernos, instituciones, corporativos, organizaciones y usuarios.

# LA PROTECCIÓN DE DATOS Y LA INTELIGENCIA ARTIFICIAL EN LOS PUEBLOS Y COMUNIDADES INDÍGENAS

MARÍA MAGDALENA PÉREZ GARCÍA

*Oficial de Protección de Datos del Órgano Garante de Acceso a la Información Pública, Transparencia, Protección de Datos Personales y Buen Gobierno del Estado de Oaxaca (OGAIPO)*

Oaxaca es el quinto estado más grande a nivel nacional, con una extensión territorial de 95,364 kilómetros cuadrados. El 90 % del suelo es accidentado, pues confluyen en los conjuntos montañosos de la Sierra Madre del Sur, la Sierra Madre de Oaxaca, la Sierra Madre de Chiapas y la Sierra Atravesada.

El estado está conformado por 570 municipios, 30 distritos y 8 regiones: Cañada, Costa, Istmo, Mixteca, Papaloapan, Sierra Norte, Sierra Sur y Valles Centrales. De estos municipios, 152 eligen a sus autoridades por partidos políticos y 418 de acuerdo con sus sistemas normativos internos, llamado Usos y Costumbres. Según el Censo 2010, el 33.9 % de la población de 3 años y más habla alguna lengua indígena: amuzgos, chatinos, chinantecos, chontales, cuicatecos, huaves, mazatecos, mixes, mixtecos, nahuas, popolucas, triquis, zapotecos, zoques, ixcatecos y chochos; estos dos últimos ya con muy pocos hablantes. El 90 % de los indígenas se dedica a actividades primarias, agrícolas y ganaderas.En 1998 entró en vigor la *Ley de Derechos de los Pueblos y Comunidades Indígenas del Estado de Oaxaca*, teniendo una reforma que entró en vigor el 11 de diciembre de 2021. El 10 de agosto de 2019 entró en vigor la reforma al artículo 2 constitucional, en la cual se reconoce a los pueblos afromexicanos como parte de la composición pluricultural de la nación.

Con los antecedentes mencionados; en Oaxaca se tiene el compromiso de dar a conocer a las personas pertenecientes a los pueblos originarios

el Derecho a la Protección de Datos Personales. La realización de estos eventos, como la Ruta de la Privacidad, nos permite ver los avances en materia de datos personales. Pero también las necesidades que existen en cada una de las comunidades, en este caso, en nuestro estado.

Cómo órgano garante se realizan acciones dirigidas a la sociedad civil: talleres dirigidos a las y los ciudadanos para que conozcan cómo ejercer sus derechos de acceso, rectificación, cancelación, oposición y portabilidad de sus datos personales, la decisión que tienen de decidir a quién y para qué proporcionen su información personal.

Sin embargo, es necesario que estas acciones lleguen a las comunidades tomando en cuenta el contexto de cada una de ellas. Esto es, si no complicado, algo que requiere de recursos humanos, materiales y económicos. Para llegar a las comunidades, debe considerarse:

- Acciones de sensibilización con las autoridades municipales, para que establezcan medios que garanticen el adecuado uso de la información personal que tratan,
- Socialización del derecho a la protección de datos personales con las personas pertenecientes a los pueblos originarios, dirigida a niñas, niños, adolescentes, adultos, adultos mayores; tomando en cuenta la lengua hablante de cada una de las comunidades; y de manera efectiva las personas conozcan este derecho humano en su propia lengua, decidan sobre el uso de su información, y ejerzan de manera plena su derecho a la protección de datos personales.

Cabe mencionar que el órgano garante realiza actividades de capacitación dirigidas a las y los servidores públicos municipales para el cumplimiento de sus obligaciones en materia de datos personales. Se abarca el mayor número posible de municipios del estado, asesorándolos para la elaboración de sus avisos de privacidad y, en su momento, su documento de seguridad.

También se programan acciones de capacitación dirigidas a las y los estudiantes de educación básica, media superior y superior, atendiendo al mayor número posible de instituciones educativas.

Como Oficial de Protección de Datos Personales del Órgano Garante de Acceso a la Información Pública, Transparencia, Protección de Datos Personales y Buen Gobierno del Estado de Oaxaca, considero que la sensibilización hacia las y los servidores públicos es una acción indispensable y necesaria para garantizar que los datos personales que tratan estén debidamente protegidos. No podemos hablar de inteligencia artificial si el derecho a la protección de datos personales no ha sido socializado en cada una de las comunidades indígenas.

# PROTECCIÓN DE DATOS PERSONALES Y CIBERSEGURIDAD EN EL SECTOR TURÍSTICO

TERESA DEL CARMEN CÁRDENAS VERA

*Experta en Ciberseguridad*

El pasado mayo, tuve el privilegio de participar como ponente en el Foro la Ruta de la Privacidad, el cual tuvo lugar en la ciudad de Chetumal, Quintana Roo. A este importante evento se sumaron figuras como el gobernador, Lic. Carlos Joaquín González, quien tuvo a bien introducirnos en la necesidad del importante tema de protección de los datos personales en el Sector Turístico.

De igual forma, compartí la mesa de ponentes con importantes figuras y maestros que, desde su propia visión y perspectiva, tocaron la relevancia que actualmente tiene la información de las empresas, pero dando mayor enfoque a los Datos Personales de los Turistas, ya que entregan su información personal para la compra, cotización de un paquete vacacional, hotel, vuelo, tour, dejando en manos de éstas el cuidado, transparencia, legitimidad, entre otras variantes del uso de la información.

Es importante mencionar que la información en la actualidad es uno de los activos más importantes que tiene una empresa, sin importar el tamaño de ésta. Permítanme usar la expresión «es el nuevo oro» para muchas personas que quisieran obtener la información para beneficio propio, ya sea usando o vendiendo esa información. También es relevante decir que la información da poder, da poder de decisión a quien la posee, pero también da poder de destrucción en las manos equivocadas.

Justo de lo anterior, detona lo importante que es implementar en torno a la información de nuestros clientes, colaboradores, proveedores, sin dejar a un lado la información propia del negocio, medidas de seguridad que van desde las políticas del uso hasta los controles que tienen que implementarse para mantenerla a salvo de manos que quieran obtenerla.

La seguridad de la información contempla leyes y normas a las que estamos obligados cumplir como empresa. Es el caso en nuestro país de la *Ley de Protección de Datos Personales en Posesión Particulares* (LFPDPPP) si recabamos, tratamos, almacenamos y/o usamos los datos personales de nuestros clientes. Valga aquí mencionar que, si aún no estamos acatándola, nunca es tarde para empezar a hacerlo.

En contexto, para cumplir la LFPDPPP no sólo es importante poner a disposición de nuestros turistas el aviso de privacidad cuando recabemos sus datos, sino además contar con un sistema de gestión de seguridad de los datos personales donde se implementen controles y se adhiera tecnología a las mejores prácticas de seguridad para mantener los datos de los clientes resguardados, capacitar a nuestros colaboradores sobre el uso adecuado de los datos personales, su resguardo y las amenazas que existen alrededor de ésta. Un sistema de gestión es cíclico y conlleva la mejora continua.

En Grupo Xcaret es muy importante la información de nuestros clientes y por ello adoptamos normas internacionales como la ISO 27001, que marca las mejores prácticas para el manejo de información. También estamos alineados a la LFPDPPP para salvaguardar la información de nuestros clientes. Detrás de esa preocupación existe un área encargada de definir la estrategia para seguir robusteciendo la protección de los datos personales de nuestros visitantes, huéspedes y socios.

Ahora bien, ¿para qué nos sirve implementar controles, tener políticas, alinearnos a la LFPDPPP? La respuesta es simple: todas estas acciones se vuelven relevantes para evitar que los datos que ponen a nuestro cuidado caigan en manos de la delincuencia cibernética, que hacen que nuestros turistas compren paquetes vacacionales ilegítimos y pierdan sus ahorros o las vacaciones de sus sueños. Implementar estas acciones ocasiona que, si por algún error o descuido humano, tuvimos un percance en torno a la información de nuestros clientes, y en caso de que el INAI nos audite, nuestras sanciones sean menores al tener controles implementados. Pero también nos hace una empresa segura, comprometida y responsable con nuestros clientes para que repitan su compra con nosotros y para que nos recomienden.

Para finalizar, dejo un par de pautas para comenzar a implementar acciones en pro de la seguridad de los datos personales de nuestros clientes: iniciemos con el inventario de datos personales que contemple dónde estamos pidiendo datos, dónde la estamos almacenando, quiénes la usan, para qué la usan y cómo la cuidamos hoy. Esto debe ser de información física y digital. Recordemos que, a lo que no conocemos, no lo podemos controlar. Ya con el inventario delimitemos con base en la criticidad de

los datos, hagamos una matriz de riesgos de esta información e implementemos los controles. También pongamos a disposición de nuestros clientes nuestro aviso de privacidad, donde le digamos qué información le solicitamos, qué hacemos con su información, por cuánto tiempo y cómo la cuidamos, siempre siendo sencillos y claros con las palabras. Busquemos siempre recabar el mínimo de información y sólo la esencial para la operación y brindar el servicio. Entre más información recabemos de nuestros turistas, mayor riesgo debemos asumir.

# RETOS NORMATIVOS DE LA PROTECCIÓN DE DATOS PERSONALES EN MÉXICO

ISABEL DAVARA F. DE MARCOS

*Socia Fundadora de Davara Abogados*

Doctora en Derecho y Licenciada en Derecho y en Ciencias Económicas y Empresariales por la Universidad Pontificia Comillas de Madrid. Abogada en México y en Madrid. Vicepresidenta del Ilustre y Nacional Colegio de Abogados de México, Consejera del Consejo General de la Abogacía Mexicana. Socia Fundadora de DAVARA ABOGADOS, Firma legal especializada en Derecho digital, tecnología e innovación.

Profesional certificada bajo el Esquema de Certificación de Delegados de Protección de Datos de la Agencia Española de Protección de Datos y por la International Association of Privacy Professionals (CIPP-E/US/CIPM y FIP). Profesora y Coordinadora del Diplomado en Derecho Digital, Tecnología e Innovación en el ITAM y profesora invitada en diversas instituciones académicas nacionales y extranjeras. Ponente en más de 400 foros especializados. Autora y coautora de más de 15 libros y más de 150 artículos y ensayos.

Actualmente, la normatividad de protección de datos personales en México enfrenta diversos retos para hacer frente a la incursión de numerosos y complejos tratamientos de datos personales, tanto en el ámbito empresarial como en el gubernamental, en los que las tecnologías emergentes como la inteligencia artificial (IA), el aprendizaje de máquinas (también conocido como *machine learning*), el *Big Data*, el Internet de las Cosas (IoT por sus siglas en ingles), el *blockchain*, entre otras, juegan un papel predominante que impulsa a legisladores, autoridades de protección de datos personales, industria y sociedad civil a replantearse las reglas existentes para legitimar el tratamiento de datos

personales.

En nuestro entorno geográfico, actualmente hay una fuerte tendencia de reforma de los marcos legales existentes, acompañada de la emisión de nuevas leyes de protección de datos en gran parte inspiradas y/o basadas en el estándar europeo impuesto por el Reglamento General de Protección de Datos (RGPD). Así, por ejemplo, la *Ley General de Protección de Datos* de Brasil, la *Ley 81* de Panamá, la *Ley Orgánica de Protección de Datos Personales* en Ecuador. Asimismo, están en proceso de discusión algunas modificaciones a ordenamientos existentes, como en el caso de Argentina, Chile, Costa Rica y Paraguay, también siguiendo en líneas generales el estándar europeo. Nuestro país no es la excepción, y en los últimos tres años hemos visto pasar casi 40 propuestas de reforma al marco jurídico existente, ya sea para la regulación del sector privado o la del público.

De esta suerte, en México existe una innegable necesidad de reformar la normatividad existente, principalmente la del sector privado, pues, en este sentido, vale la pena reconocer que la normatividad vigente para el sector público —al ser de incursión más reciente (enero, 2017) — incluye conceptos novedosos que la actual *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* (LFPDPPP), aplicable para el sector privado, no incorpora.

Además del entorno complejo en el que se desarrollan las actividades del sector empresarial en México, la necesidad de reformar la normatividad existente se debe, por un lado, a que México ya ha firmado el Convenio 108 del Consejo de Europa, se encuentra buscando la firma del Convenio 108+, y ha iniciado los trámites para ser reconocido como país con nivel adecuado de protección, reconocimiento que la Comisión Europea puede otorgar únicamente si México garantiza, entre otras cosas, que sus normas son sustancialmente equivalentes a las del esquema europeo (RGPD) y cuenta con un andamiaje institucional y político propicio para la tutela de los derechos humanos en general.

Por otro lado, la reforma a la LFPDPPP se requiere también para seguir posicionando a nuestro país como un importante referente en esta materia. En los últimos años, México ha marcado la pauta para otros países en nuestro entorno más directo, y nuestra autoridad federal (el Instituto Nacional para el Acceso a la Información y la Protección de Datos, INAI) es reconocida como una de las más activas de la región, siendo referente tanto en su confección institucional derivada de su autonomía constitucional como en la ejecución de tareas de divulgación, investigación, sanción y cooperación internacional, con el propósito de garantizar el derecho de protección de datos personales de la ciudadanía mexicana.

En particular, analizando la LFPDPPP se pueden identificar diversas áreas de oportunidad que incluyen la necesidad de delimitar con mayor claridad el ámbito de aplicación territorial de la Ley, la necesidad de incorporar otras bases de legitimación del tratamiento como el interés legítimo, la especificación de medidas concretas para cumplir con el principio de responsabilidad proactiva, la previsión de los derechos a la portabilidad, oposición a mercadotecnia directa, oposición a la elaboración de perfiles y tratamientos automatizados, así como la definición de un régimen más claro para la práctica de las transferencias internacionales de datos.

Asimismo, uno de los retos principales es que la normatividad, además de incorporar los conceptos, principios y obligaciones mínimas que las empresas deben observar según estándares internacionalmente aceptados en esta materia, considere las necesidades internas y características del entorno en el que se pretende ejecutar la regulación y permita cierta flexibilidad con miras a que las organizaciones asuman estándares de cumplimiento adecuados y adopten medidas de responsabilidad proactiva para demostrar su compromiso de cumplir con la normatividad vigente.

Si bien la fácil integración de la tecnología en la vida cotidiana reporta numerosos beneficios para las personas, también puede suponer riesgos específicos para la garantía de derechos como la privacidad y la protección de datos personales. Por ello es indispensable que las organizaciones conozcan las obligaciones que tienen cuando hacen uso de datos personales, y que las normas vigentes otorguen una protección adecuada a las personas, permitan la innovación tecnológica y faciliten el flujo de datos personales imprescindible para el desarrollo de la economía y ecosistema digitales, estableciendo asimismo estándares de cumplimiento que tengan en consideración la «ética digital» como un eje rector del tratamiento de datos personales para salvaguardar los derechos de las personas y evitar tratamientos de datos que resulten contrarios a la ética humana y tengan el potencial de afectar los derechos de las personas.

# EL SIGNIFICADO DE PRIVACIDAD

JUAN CARLOS CARRILLO

*Director de Ciberseguridad y Privacidad de Datos, PwC México*

Licenciado en Administración de Sistemas Computacionales, egresado de la Universidad del Valle de México y Maestro en Finanzas del Instituto Tecnológico de Estudios Superiores de Monterrey. Está certificado como Profesional de Privacidad de la Información (CIPT), Ingeniero Certificado en Soluciones de Privacidad de Datos (CDPSE), Certificado como Administrador de Identidad y Acceso (CIAM) y Certificado en Seguridad en la Nube (CCSK).

¿Qué significa la privacidad? Bueno, depende de a quién le preguntes. La privacidad es el derecho a que lo dejen en paz o a estar libre de interferencias o intrusiones. La protección de la información es controlar cómo se recopila y utiliza su información personal. Si preguntamos a la mayoría de las personas en estos días qué piensan sobre la privacidad, tristemente de lo que hablamos es de fugas de datos o de ciberataques. Es probable que dichas conversaciones sean sobre fugas masivas de datos, tecnología portátil, redes sociales y errores publicitarios dirigidos, sin mencionar las revelaciones como la de la SEDENA.

Además, varias culturas en el mundo tienen puntos de vista muy diferentes sobre cuáles son los derechos de una persona respecto a la privacidad y cómo debe regularse.

## *¿Por qué es importante la privacidad?*

Con la innovación tecnológica tan rápida, la protección de los datos personales y su impacto en la privacidad se vuelven cada vez más complejos a medida que se recopilan e intercambian más datos. A medida que la tecnología se vuelve más sofisticada, y tristemente

más invasiva, también lo hace el uso de los datos. Además, eso deja a las empresas, enfrentando una matriz de riesgo increíblemente compleja para garantizar que la información personal esté protegida. Como resultado, la privacidad ha surgido rápidamente como quizás no el problema de protección de los ciudadanos más importante, si no un problema de protección del consumidor en la economía global de la información.

## *Privacidad vs. seguridad… ¿no es lo mismo?*

Realmente no. Lo he dicho en muchas ocasiones: la privacidad y la seguridad son primas, no son hermanas.

La privacidad de los datos se centra en el uso y la gobernanza de los datos personales, cosas como la implementación de políticas para garantizar que la información personal de los consumidores se recopile, comparta y use de manera adecuada. La seguridad se enfoca en proteger los datos de ataques maliciosos y explotar los datos robados para obtener ganancias. Si bien la seguridad es necesaria para proteger los datos, no es suficiente para abordar la privacidad. Un marco de gobierno de privacidad debería contener al menos 10 dominios:

- Estrategia y Gobierno
- Gestión de políticas
- Transferencias transfronterizas
- Gestión del ciclo de vida del dato
- Gestión de incidentes
- Derechos del titular (o derechos ARCO)
- Privacidad por diseño (*Privacy by design*)
- Ciberseguridad
- Responsabilidades del procesador de datos
- Capacitación y concienciación

Por otro lado, una estrategia de protección de datos debería tener cuatro columnas vertebrales:

- Gobierno de los datos
- Descubrimiento de los datos
- Protección de los datos
- Minimización de los datos

## *¿Dónde encaja la Autoridad?*

Las organizaciones que no «cumplen con los derechos de privacidad» corren el riesgo de la aplicación del gobierno, demandas colectivas, ruina financiera, reputación dañada y pérdida de la lealtad del cliente. La privacidad es ahora una necesidad para hacer negocios.

El INAI ha realizado un trabajo espectacular en ser una autoridad que no busca el castigo como base de operaciones, sino que busca educar, capacitar y hasta evangelizar constantemente en materia de protección de datos y privacidad.

La autoridad se enfrenta al reto de tocar al menos a tres áreas que se han dedicado en los últimos años a la privacidad y protección de datos personales:

- Los oficiales de protección de datos o CPO
- Los oficiales legales
- Los oficiales de seguridad o CISO (Chief Information Security Officer)

No me queda duda de que el Instituto es y seguirá siendo una luz y una guía en el camino para lograr que estas áreas y muchas más busquen la protección de los ciudadanos en su información y su esfera más íntima.

He tenido el placer de compartir en distintos momentos y con distintos comisionados, directores y miembros del Instituto, y siempre he visto una calidad moral y una búsqueda fundamental de la protección de los ciudadanos, siempre buscando proporcionar un foro de discusión y educación sobre la privacidad.

# LA INTELIGENCIA ARTIFICIAL Y SU APROVECHAMIENTO

NUHAD PONCE KURI

*Consejera Presidenta del Consejo Consultivo del INAI*

Socia fundadora de la firma Ponce Kuri, S.C. Es titular de las áreas de Derecho Corporativo, Protección de Datos Personales y Seguridad de la Información. Licenciada en Derecho, egresada de la Universidad Panamericana.

Cursó la Maestría en Derecho de la Empresa en la Universidad Panamericana, titulada con Mención Honorífica. Está Certificada por «Normatividad y Certificación Electrónica, S.C.» (NYCE), como Profesional Certificado en Protección de Datos Personales, nivel Senior.

Es miembro de la International Association of Privacy Professionals. Cursó diversos Diplomados y Especialidades en Contratos y Negocios Mercantiles, y en Protección de Datos Personales y Seguridad de la Información. Es Primer Vicepresidente del Consejo Directivo Nacional de la Asociación Nacional de Abogados de Empresa, Colegio de Abogados, A.C. (ANADE). Desde 2010, está certificada como abogado de empresa por dicho Colegio.

Es miembro del Consejo de la Asociación Jurídica Mexicano Libanesa, Al Muhami, A.C. Es Presidente Honorífico del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Es Presidente de la mesa de Ciberseguridad del Consejo Coordinador Empresarial (CCE) y miembro de la Consejería Jurídica de la Confederación Patronal de la República Mexicana (COPARMEX). Es considerada una de las abogadas más influyentes de México, por la revista *Foro Jurídico*. Es Catedrática de licenciatura, especialidad y maestría de diversas universidades en la República Mexicana.

En el mundo en el que vivimos, la tecnología ha cobrado un papel relevante. Sin duda las soluciones tecnológicas aplicadas a distintas profesiones, como el Derecho, logran una mejora en la eficiencia de los servicios jurídicos, pero es importante tener contemplados los términos y condiciones del uso de esa inteligencia artificial.

Hablando de tecnología, no puede dejarse de lado la importancia de la protección de datos personales relacionado con el *Big Data*. Ya que, como sabemos, la recopilación y el análisis de datos de manera masiva tiene por objeto obtener información de interés para un cierto sector. Este proceso implica la utilización de medios informáticos y sistemas de inteligencia artificial. Esta recopilación de datos personales que puede englobar un sinfín de información de nuestras actividades, interacción en medios digitales, información personal, almacenamiento de datos, entre otros, se ha convertido en un reto para los usuarios y las autoridades: si bien la tecnología ha venido incorporándose en nuestra vida y la administración pública también ha gozado de sus atributos, gran parte de los usuarios desconoce cuáles son los riesgos que esto conlleva. En todo momento, el desarrollo de tecnologías debe cuidar y proteger el derecho a la privacidad y la protección de los datos personales.

La inteligencia artificial permite la automatización de una gran variedad de procesos. Existen numerosos ejemplos de esta automatización que ya tenemos y que se han potencializado durante la pandemia que recién vivimos, como el uso de autos con conducción autónoma, el uso de la inteligencia artificial en electrodomésticos, entre muchos otros.

La inteligencia artificial, sin duda, da una oportunidad para mejorar nuestras actividades diarias y para transformar sociedades, siempre que se tenga en primer lugar la ética como principio rector del uso de esta herramienta tecnológica. Para ello, lo primero que necesitamos es tener una cultura y educación de la sociedad para el uso de estas tecnologías. Si queremos tener una ciudadanía y autoridades que puedan hacer frente a los retos en un contexto ético, la capacitación continua es clave para la formación de criterios con sentido ético y crítico sobre la dirección a tomar en el uso de ellas.

Sus ventajas son muchísimas. Sólo por mencionar algunas: se prevé que el impacto de la inteligencia artificial en las empresas ayude al aumento de la productividad, a hacer eficientes los procesos internos, a mejorar la calidad de vida de los trabajadores, a tener un mejor y mayor conocimiento del cliente, lo que propiciará una mejor experiencia como consumidor, entre otros. Pero los retos para el uso ético, la protección de los datos y la información se vuelven aún mayores.

De esta manera, es importante conocer las herramientas que como titulares de datos personales tenemos, saber que como sujetos obligados y responsables del tratamiento de datos debemos garantizar el debido cumplimiento de los ocho principios rectores de la legislación mexicana vigente y los deberes ahí contenidos. Debemos buscar capacitación de manera continua y constante, buscando además la profesionalización del personal involucrado en el tratamiento de datos personales.

Finalmente destaco que Ruta de la Privacidad es precisamente la vía para que contemos con las condiciones necesarias para que se tenga una estrategia de privacidad y protección de datos personales, entre ciudadanía y autoridades. En este sentido, la capacitación es muy importante para ello, y el INAI ha sido punta de lanza en información, talleres, eventos, elaboración de infografías, concursos y herramientas para que se tenga el conocimiento y cultura sobre la protección de nuestros datos personales y de nuestra información. Fortalezcamos a nuestras instituciones que garantizan los derechos fundamentales de protección de datos personales, acceso a la información y transparencia.

# PRONADATOS Y PROTECCIÓN DE DATOS PERSONALES

MARCELA TRUJILLO ZEPEDA

*Socia Administradora de RVA Abogados, S.C.*

Es Socia Administradora de RVA Abogados, S.C. Actualmente cursa el doctorado en la Universidad Nacional de México con la Tesis doctoral *Gobierno Corporativo en Petróleos Mexicanos*. Es licenciada con mención honorífica en Derecho por la Universidad Anáhuac, Ciudad de México, con estudios de especialización en Inversiones Extranjeras. Está involucrada en la práctica del Derecho corporativo y transaccional, representando a compañías mexicanas y extranjeras, en la estructuración y negociación de operaciones comerciales y financieras. Su práctica se enfoca a fusiones y adquisiciones, inversiones extranjeras, inmobiliario, protección de datos personales, transparencia, políticas de cumplimiento y buenas prácticas, gobierno corporativo y derecho bancario.

Es miembro de la Barra Mexicana de Abogados, donde fue coordinadora de la Comisión de Derecho Mercantil (2000- 2003). Fue presidenta de la Comisión de Estudios de Equidad y Género (2003-2007) y representante de la Comisión Mercantil de la Barra Mexicana de Abogados ante el Centro Nacional de Evaluación (Ceneval), Coordinadora del Comité de la Ciudad de México (2015-2016) y actualmente integrante de la Junta de Honor.

El 3 de abril de 2019 tomó protesta ante el Senado de la República como Consejera Honorífica del Consejo Consultivo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para desempeñar durante 7 años a partir de su designación un cargo de participación ciudadana, no remunerado, en apoyo a las labores de transparencia, rendición de cuentas y protección de datos personales de este Órgano Autónomo.

Tuve la oportunidad de ser invitada, en mi calidad de integrante del Consejo Consultivo del INAI, a uno de los múltiples foros regionales organizados por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia.

En este breve ensayo intentaré sintetizar algunas conclusiones de la enriquecedora discusión y reflexiones derivadas del foro correspondiente a la Región Centro, llevado a cabo en Pachuca, Hidalgo, en febrero de 2022, conjuntamente con el Instituto de Transparencia, Acceso a la Información, Política Gubernamental y Proyección de Datos Personales del Estado de Hidalgo (ITAIH), el cual lleva a cabo, como los demás órganos garantes de todas las entidades federativas, acciones transcendentales para garantizar el ejercicio de los derechos de acceso a la información y protección de datos personales.

Éste, como muchos de los proyectos realizados por los organismos garantes en nuestro país, busca posicionar en la agenda pública nacional temas de especial relevancia para la Protección de Datos Personales, partiendo desde luego del principio de cooperación federal previsto para el Sistema Nacional de Transparencia y de la participación de los sectores privado, público y social.

Mi participación en el trabajo *Memorias de la Ruta de la Privacidad* me otorga un espacio idóneo para difundir el compromiso de incorporar al PRONADATOS, como una de las políticas públicas más relevantes en el marco del Sistema Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, pero especialmente lograr un mayor apoyo para su total y exitosa implementación.

No puedo dejar de reconocer el esfuerzo permanente de PRONADATOS para mejorar las acciones tendientes a ampliar la base de usuarios de los derechos de acceso, rectificación, cancelación y oposición de los datos personales, al tiempo de promover y fortalecer su protección. Sin embargo no debemos soslayar el hecho de que el nuevo PRONADATOS requiere de acciones adicionales y específicas para potenciar los beneficios del programa, así como de la asignación de importantes recursos materiales y humanos para consolidar el cumplimiento de sus objetivos.

Lamentablemente, el PRONADATOS 2022-2024 identifica nuevamente problemas diagnosticados en su primera edición. Los temas de fortalecimiento institucional, la profesionalización y la difusión de los procedimientos de garantía progresiva de los derechos de protección de datos aún no están superados.

El Programa Nacional de Protección de Datos Personales es el instrumento de coordinación interinstitucional que define las bases de la política pública para la garantía de este derecho a nivel nacional para el sector público. El fundamento jurídico se encuentra en la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* (LGPDPPSO).

Su objetivo general es fortalecer institucionalmente la profesionalización y los procedimientos de garantía progresiva de los derechos de protección de datos personales, la utilización, cuidado y denuncia de uso indebido de los datos personales bajo las mismas reglas en el ámbito público en los tres niveles de gobierno, que sean comunicados a terceros legalmente y bajo el consentimiento de las personas titulares.

El PRONADATOS 2018-2022 logró una importante difusión entre la sociedad de los temas de protección de datos personales, mejoró notablemente el desempeño de los responsables y el mejoramiento del marco normativo, así como en promover la educación y cultura de la protección de datos personales en México. Sin embargo, estamos aún muy lejanos de lograr consolidar para todos el derecho humano de la protección de datos personales. Si bien es cierto se han incorporado nuevos sistemas de seguridad y mecanismos de protección de datos personales, queda por hacer un trabajo considerable para sensibilizar y dotar de herramientas tecnológicas a los responsables y órganos garantes para cumplir cabalmente con este objetivo.

La realidad exige de la implementación urgente de medidas de seguridad y el tratamiento de datos ante las nuevas tecnologías de la información que permitan a los Sujetos Obligados desarrollar e implementar herramientas y metodologías eficientes para los sistemas de gestión de seguridad a la que están obligados.

Deben desarrollarse soluciones informáticas que apoyen a los responsables en la elaboración de los documentos base para la identificación del debido cumplimiento al deber de seguridad en la protección de datos personales.

En esta segunda etapa del PRONADATOS, el objetivo nacional debe ser lograr la plena socialización de las políticas públicas con esquemas de buenas prácticas entre los Sujetos Obligados, propiciando sinergias con la sociedad civil, las instituciones académicas y por supuesto con los órganos garantes que deriven en la identificación de los problemas y la búsqueda de soluciones para mejorar las capacidades de los Sujetos Obligados en el cumplimiento de una cultura de la privacidad y protección de datos personales.

Es impostergable el fortalecimiento institucional y la profesionalización

de recursos humanos tendientes a la protección y garantía de los derechos humanos que permitan incrementar la gobernanza institucional y fortalecer el Estado de Derecho. Dichos aspectos ya habían sido considerados en el PRONADATOS anterior. Para este nuevo PRONADATOS 2022-2024 se requiere del compromiso de los Sujetos Obligados y de la innegable asignación de recursos materiales y humanos, así como de una firme voluntad política para alcanzar el objetivo de consolidar al PRONADATOS como un mecanismo guía que permita a todos los participantes dar un seguimiento puntual y evaluar el alcance de sus compromisos en materia de protección de datos personales.

Como integrante del Consejo Consultivo del INAI, me siento entusiasmada de participar en estos valiosos esfuerzos para socializar y reflexionar permanentemente sobre el derecho humano de protección de datos personales, uniendo las voluntades de los sectores público, privado y social, así como los tres ámbitos de gobierno en el cumplimiento de estos importantes objetivos.

# PERSPECTIVAS Y PROSPECTIVAS DESDE EL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES Y LA PRIVACIDAD

OLIVIA ANDREA MENDOZA ENRÍQUEZ

*Profesora de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas*

Licenciada en Derecho, Maestra en Derecho con especialidad en Derecho Económico y Doctora en Derecho con distinción *Ad Honorem* por la Benemérita Universidad Autónoma de Puebla. Especialista en Derechos Humanos y Máster en Derecho Constitucional por la Universidad Castilla-La Mancha (UCLM), España. Profesora Investigadora Asociada del Centro de Investigación y Docencia Económicas (CIDE). Miembro del Sistema Nacional de Investigadores, nivel I.

Se desempeñó por seis años como Profesora Investigadora Titular de Tiempo Completo del Centro de Investigación e Innovación en Tecnologías de la Información y Comunicación, INFOTEC (Centro Público CONACYT). Fungió como Coordinadora Académica y miembro del Núcleo Académico Básico de la Maestría en Derecho y TIC. Se ha desempeñado como Coordinadora Académica de la Maestría en Regulación y Competencia Económica de las Telecomunicaciones, impartida a servidores públicos del Instituto Federal de Telecomunicaciones IFT. Participó en la creación y desarrollo de dicho programa.

Su línea de investigación es Regulación y Tecnología, particularmente relacionada con el Derecho a la Protección de Datos Personales. Se destaca la relevancia de esta iniciativa, considerando que la autonomía constitucional del INAI, otorgada en 2014, le convierte en un ente nacional que tiene como reto mayor la descentralización de derechos

como el de acceso a la información y protección de datos personales para articular un verdadero «Sistema Nacional» que permita la reflexión, análisis y abordaje de problemas complejos desde un modelo de inclusión, traspolando un efectivo federalismo para estos dos derechos humanos relevantes e indispensables para el Estado Constitucional y Democrático de Derecho en México.

## *Introducción*

La inteligencia artificial sin duda es una tecnología que ha revolucionado la forma en la que interactúan y toman decisiones los humanos. Tiene diversos usos que van desde la agricultura, la medicina, la educación, el transporte, el control de la pandemia COVID, etc.

La incorporación de sistemas de inteligencia artificial ha permitido hacer más eficientes los procesos y la toma de decisiones dentro de las organizaciones. Un elemento necesario para su funcionamiento es la información que se suministra a los sistemas inteligentes.

Considerando que, dentro de la información que es materia prima para la inteligencia artificial existen datos personales, surge una preocupación constante respecto del uso masivo de estos sistemas. Esto advirtiendo las prácticas acontecidas en un mundo cada vez más conectado, como el tratamientos indebidos de datos (falta de cumplimiento normativo o de incorporación de límites éticos), la falta de medidas de seguridad, algoritmos que son entrenados con información errónea y graves fallas en el diseño de la técnica, que podrían traer la violación de derechos humanos: desde el derecho a la vida, el derecho a la no discriminación, el derecho a la salud, hasta el derecho a la privacidad y a la protección de datos personales, por enunciar algunos.

Derivado de lo anterior, no se puede obviar el evidente impacto de la inteligencia artificial a dos derechos humanos específicos que se analizan en las siguientes líneas: el derecho a la privacidad y el derecho de protección de datos personales.

## *Concepto de inteligencia artificial*

Como ha quedado establecido, el término «inteligencia artificial» aparece desde los años 50 en algunas investigaciones de ciencias de la computación. El concepto fue utilizado por primera vez en 1955 en el proyecto de investigación de John McCarthy, Marvin L.

Minsky, Nathaniel Rochester y Claude Shannon.[53]

También el término de inteligencia artificial en la dimensión atribuida por la informática[54] ha sido explorado por la ciencia jurídica desde 1960. Los primeros documentos jurídicos que hablan de inteligencia artificial lo hacen para referirse a la transcripción de medios de prueba en una forma legible por computadoras para obtener un procesamiento eficiente de la información[55], así como para procesar la información proporcionada por un cliente a un abogado y determinar la probabilidad de ganar un caso, la cantidad estimada de daños si los hubiere, el análisis de la legislación legal, así como la jurisprudencia.[56]

En recientes fechas, el Grupo de Alto Nivel en Inteligencia Artificial creado por la Comisión Europea para desarrollar la Estrategia Europea en Inteligencia Artificial ha aplicado el concepto de inteligencia artificial a «sistemas que manifiestan un comportamiento inteligente, al ser capaces de analizar el entorno y realizar acciones, con cierto grado de autonomía, con el fin de alcanzar objetivos específicos».[57]

El verdadero alcance del concepto de inteligencia artificial no puede entenderse sin analizar nuevas posibilidades de procesamiento de información como la computación cuántica, y nuevas formas de obtener datos, como las posibilidades que plantean las neurociencias.

[53] McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E., 2006. "A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence", August 31, 1955. *AI Magazine*. Consultado el 20 de marzo del 2020. Disponible en: https://doi.org/10.1609/aimag.v27i4.1904.

[54] En palabras de Vicenç Torra, la inteligencia artificial es una de las ramas de la Informática con fuertes raíces en otras áreas como la lógica y las ciencias cognitivas. Más información disponible en http://www.fgcsic.es/lychnos/es_es/articulos/inteligencia_artificial

[55] M. Gibbs, E. Adams, "A Report on the Second National Law and Electronics Conference." M.U.L.L. *Modern Uses of Logic in Law*, pp. 215-223. Consultado el 20 de marzo de 2020. Disponible en: http://heinonline.org/HOL/Page?handle=hein.journals/juraba3&start_page=215&collection=journals&i d=225

[56] S. Winston, "The Law and Legal Education in the Computer Age." *Journal of Legal Education*, pp. 159-168. Consultado el 15 de marzo de 2020. Disponible en: http://heinonline.org/HOL/Page?handle=hein.journals/jled20&start_page=159&collection=-journals&id=17 1

[57] Artificial Intelligence for Europe, Comisión Europea. Disponible en: https://ec.europa.eu/digital-single-market/en/artificial-intelligence

## *El derecho de protección de datos personales en los sistemas de inteligencia artificial*

Cuando se habla del derecho de protección de datos personales, es usual pensar que es un derecho nuevo que nace a partir de la economía digital, del uso de Internet y del vertiginoso desarrollo de las Tecnologías de la Información y Comunicación.

No obstante, si bien es un derecho de reciente reconocimiento en la Constitución Política de los Estados Unidos Mexicanos (2009), tiene antecedentes importantes en la época de posguerra en Europa.

Pensemos así en una Alemania nazi que trató los datos de miles de judíos a través de un censo realizado por el Estado, con la ayuda de las tarjetas perforadas de la empresa IBM, con el objetivo de identificar a esta población y planear su exterminio de forma más efectiva[58].

A partir de atrocidades como éstas, se volvió evidente la necesidad de establecer límites del Estado frente a la vida privada de las personas. Ejemplo de ello está manifestado en el artículo 12 de la Declaración Universal de Derechos Humanos (en adelante DUDH).

El reconocimiento que ha hecho México del derecho de protección de datos personales como un derecho humano tiene interesantes consecuencias ya que, derivado de la reforma constitucional en materia de derechos humanos de 2011, el Estado mexicano se ve comprometido a salvaguardar y promover este derecho. Incluso la aplicación de principios como el de progresividad de los derechos humanos compromete a México a evolucionar normativamente en favor de este derecho.

No obstante lo anterior, para el Estado mexicano la salvaguarda del derecho de protección de datos personales en el ámbito tecnológico resulta bastante compleja. Esto atendiendo a que se ha depositado una enorme responsabilidad en las corporaciones para que sean éstas las que decidan los términos y condiciones en los que garantizarán los derechos humanos. Es decir, espacios ubicuos como Internet o un sistema de inteligencia artificial hacen inminente la reducción de la figura tradicional de Estado-Nación, cuando se trata de garantizar y promover los derechos humanos, ya que estas acciones quedan mayormente en manos de las corporaciones.

Ante este panorama, cada vez se vuelve más necesario incorporar el principio de escrutinio de los derechos humanos como habilitador para el Estado de un mecanismo efectivo para la supervisión, garantía y ejer-

[58] Black, Edwin, IBM y el Holocausto. *La alianza estratégica entre la Alemania Nazi y la más poderosa corporación norteamericana*, (Buenos Aires: Atlántida, 2001) p. 18

cicio de los derechos humanos a la luz del desarrollo tecnológico. En este sentido, un caso interesante sobre desarrollo de instrumentos de control estatal que permite la salvaguarda de los derechos humanos en la inteligencia artificial es el Consejo de la Unión Europea, que presentó en febrero de 2019 unas conclusiones relativas al *Plan Coordinado sobre la Inteligencia Artificial*, entre las que destaca la importancia de garantizar el pleno respeto de los derechos de los ciudadanos mediante la aplicación de directrices éticas para el desarrollo y uso de la inteligencia artificial.[59]

Desde del derecho público, particularmente para el caso de México, también podemos plantear la siguiente interrogante: ¿los Estados deben impulsar e incidir en la transparencia en el desarrollo de algoritmos y sistemas de funcionamiento general de la inteligencia artificial? El planteamiento tiene miras a hacer posible que la autoridad tenga claros los temas de vigilancia y cumplimiento que deben seguir las corporaciones respecto de la explotación de la información.

Ante tal panorama, el derecho humano de protección de datos personales tiene retos complejos que superar frente la inteligencia artificial, los cuales radican primordialmente en recuperar la parte humanística relacionada al mismo, para así otorgar certidumbre, generar confianza y ofrecer un entorno digital ético a los usuarios.

Reforzando esta idea, es necesario invocar la Declaración de Principios de la Cumbre Mundial sobre la Sociedad de la Información, en la que se estableció el compromiso de construir una sociedad basada en la persona, en la que todos pudiéramos crear, consultar, utilizar y compartir la información y el conocimiento, para impulsar el desarrollo sostenible y mejorar la calidad de vida sobre la base de los propósitos y principios de la Carta de las Naciones Unidas, y respetando plenamente y defendiendo la Declaración Universal de Derechos Humanos.[60]

Derivado de lo anterior, podemos afirmar que la idea de dignidad humana debe estar más presente que nunca en el desarrollo tecnológico y en la forma en la que se configura la regulación en torno a dicho rubro.

[59] Manuel Jesús López Baroni, «Las narrativas de la Inteligencia Artificial». *Revista Bioética y Derecho*, Universidad de Barcelona, p. 13. Disponible en: https://revistes.ub.edu/index.php/RBD/article/view/27280

[60] Adelantando un poco la respuesta respecto a los principios ahí establecidos y el resultado de la sociedad digital construida, podemos mencionar el informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos de 2014, denominado *El Derecho a la Privacidad en la Era Digital*, que deja en relieve la responsabilidad que hasta ahora han tenido las empresas para vulnerar la privacidad de las personas en el ciberespacio. Disponible en: https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Privacy-In-digital-Age-Spanish-version.pdf Fecha de consulta enero, 2016.

Uno de los grandes desafíos de no hacerlo es la paradoja de la coordinación y fragmentación de procesos desiguales de desarrollo[61]. Es decir, el desarrollo tecnológico debe preservar un equilibrio entre la libertad y la dignidad humana, el cual podría lograrse a través de un humanismo sólido y del respeto de dicha dignidad como eje de cualquier avance científico: la tecnología como herramienta para empoderar a las personas, pero no como el único fin.

## *Derecho a la privacidad en los sistemas de inteligencia artificial*

El concepto *privacidad* no es un concepto terminado y depende del contexto y circunstancias de los casos particulares poder acotarlo. Es decir, lo que en un país puede considerarse como una situación del ámbito privado, en otro no[62]. En virtud de lo anterior, el término *privacidad* no es fácil de definir, ya que hasta el momento no se tiene una idea clara de sus alcances. Esto se confirma con lo dicho por el Tribunal Europeo de Derechos Humanos, que considera la privacidad como un concepto amplío, no susceptible de una definición exhaustiva[63].

Para el caso de México, la Suprema Corte de Justicia de la Nación (SCJN) estableció que las afirmaciones contenidas en las resoluciones nacionales e internacionales relacionadas con la privacidad o vida privada son útiles en la medida en que no se tomen de manera descontextualizada, emerjan de un análisis cuidadoso de los diferentes escenarios jurídicos en los que la idea de privacidad entra en juego y no se pretenda derivar de ellas un concepto mecánico de vida privada, de referentes fijos e inmutables. Lo único que estas resoluciones permiten reconstruir, en términos abstractos, es la imagen general que evoca la idea de privacidad en nuestro contexto cultural[64].

[61] Giddens, A., *Consecuencias de la Modernidad*, (Madrid: Alianza, 1993) p. 162.

[62] Mendoza Enríquez, O. Andrea, *Definición de privacidad*, *Diccionario Protección de Datos Personales*, INAI, 2020, p. 672. Consultado el 15 de marzo de 2020. Disponible en: http://inicio.INAI.org.mx/PublicacionesComiteEditorial/DICCIONARIO_PDP_digital.pdf

[63] Véase Piñar, J. «¿Existe privacidad?, Lección magistral impartida en la Apertura Solemne del Curso Académico en la Universidad San Pablo-CEU de Madrid», en *Protección de Datos Personales*, *Compendio de lecturas y legislación*, (México. Editorial Tiro Corto, 2010). p. 16.

[64] 165823. 1a. CCXIV/2009. Primera Sala. Novena época. *Semanario Judicial de la Federación* y su *Gaceta*. *Tomo xxx*, diciembre de 2009, p. 277. «Derecho a la Vida Privada. Su

En términos generales podemos decir que la privacidad es el ámbito más íntimo o profundo de la vida de una persona, que puede comprender sus sentimientos, pensamientos, emociones, vida familiar o relaciones personales y el derecho a la privacidad, el poder que tiene la persona frente a cualquier intromisión de un tercero que pudiera manifestarse (incluido el propio Estado). El derecho a la privacidad es el poder de decisión de una persona sobre su espacio privado, con quién lo comparte, qué debe formar parte de lo público y qué de lo privado[65].

La privacidad y derecho a la privacidad no necesariamente refieren a lo mismo: la privacidad es un elemento consustancial a la dignidad humana y por ende debe ser protegido por el derecho, y el derecho a la privacidad es aquél que todo individuo tiene a separar aspectos de su vida privada del escrutinio público[66].

Por otro lado, los conceptos de privacidad y vida privada se han redefinido a partir del vertiginoso desarrollo tecnológico, el cual hace posible la sobreexposición de ámbitos que hasta hace unas décadas eran meramente del ámbito privado.

Una vez que hemos tratado de definir o al menos dar una aproximación conceptual de la privacidad, vida privada y derecho de privacidad, podríamos estar preguntándonos entonces: ¿por qué es tan importante preservar la privacidad en tiempos de inteligencia artificial?

Una primera respuesta es que el valor de la privacidad tiene un componente privado, pero también es un *social good* en la medida en la que es necesaria para la pervivencia de la democracia y la libertad.[67] Por ejemplo, no podríamos imaginar un estado constitucional y democrático de derecho, frente a censos que utilicen la inteligencia artificial para procesar información de la población que deriven en un exterminio masivo de personas,

contenido general y la importancia de no descontextualizar las referencias a la misma». Disponible en: http://sjf.scjn.gob.mx/sjfsist/Documentos/Tesis/165/165823.pdf. Fecha de consulta: 20 de agosto de 2018.

65 El derecho a la privacidad no es un derecho absoluto y estará limitado a apreciaciones establecidas en precedentes judiciales como el grado de exposición pública de una persona, la trascendencia en las actividades que realiza, los alcances de protección de la libertad de expresión, el interés público, etc.

66 Ricci, D. «Artículo 16 Constitucional. Derecho a la privacidad», en Ferrer Mac-Gregor, *et al* (coord.). *Derechos Humanos en la Constitución: comentarios de jurisprudencia constitucional Interamericana II*. Instituto de Investigaciones Jurídicas. UNAM, p. 1045. Disponible en: https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf. Fecha de consulta: 20 de agosto de 2018.

67 Contreras Gómez, Carlos, *El papel del gobierno en la era digital: un enfoque de economía pública*, 1.ª ed, (Madrid: Centro de Estudios Ramón Areces 2017).

como sucedió en la Alemania nazi durante el Holocausto.

Una segunda respuesta sobre la importancia de preservar la privacidad en tiempos de inteligencia artificial tiene que ver con la enorme capacidad técnica de las organizaciones para recabar grandes cúmulos de información en tiempo real, procesarla y tomar decisiones, lo cual sobre lo que expone aspectos privados de la vida de las personas, como los hábitos de consumo de un hogar, los ingresos económicos de una persona o su ideología política o religiosa, por mencionar algunos. Esta sobreexposición y concentración de información por parte de unos cuantos deja a los usuarios de sistemas de inteligencia artificial particularmente desprotegidos frente al poder acumulado por las corporaciones. Ejemplos como el de *Cambridge Analytica*[68] hacen evidente la necesidad de vigilar el comportamiento de tecnologías como la inteligencia artificial.

La tercera respuesta está relacionada con el párrafo anterior, ya que el rol de las corporaciones como actores que ostentan el poder en la economía digital propicia la eventual disminución del Estado Nación y la no intervención, a través de su rectoría, para la salvaguarda de derechos humanos, como el derecho a la privacidad.

Como podemos advertir de las líneas anteriores, el rápido desarrollo tecnológico hace que cada vez sea más complejo garantizar el derecho a la privacidad, ya que la información que se genera a partir del uso de Internet y de sistemas de inteligencia artificial se encuentra susceptible a ser sometida a tratamientos masivos, y muchas veces sin contar con el conocimiento y consentimiento informado del titular del dato. En este punto es conveniente resaltar que actualmente la inteligencia artificial permite en algunos casos hacer tratamiento de datos legales pero poco éticos, ya que, si bien los sistemas son programados para cumplir en el mejor de los casos con los requisitos mínimos de las normas (en materia de protección de datos personales sería el consentimiento de los titulares de la información), este consentimiento no es verdaderamente informado, o no se propician los mecanismos necesarios para que los titulares de datos alcancen a entender la dimensión de la autorización[69].

[68] Este caso consistió en que la empresa Cambridge Analytica tuvo acceso a los datos de unos 87 millones de usuarios de Facebook, según reveló la red social. La información fue obtenida a través de una aplicación que ofrecía realizar un *test* de personalidad, pero que en realidad usó ese acceso para recopilar datos de los usuarios y de sus redes de amigos hasta sumar hasta un 15 % de la población de Estados Unidos. La empresa utilizó este material para elaborar perfiles psicológicos de cada usuario y diseñar mensajes hechos a medida para tratar de influir en las elecciones presidenciales de Estados Unidos de 2016. Información consultada en: https://www.bbc.com/mundo/noticias-43971491

[69] En este punto, es fácil escuchar discursos que criminalizan a los usuarios de sistemas

## *Conclusiones*

Si bien existe un marco legal robusto en materia de datos personales en México, se identifican desafíos para la salvaguarda de este derecho cuando se trata de entornos tecnológicos, específicamente en la inteligencia artificial.

Estos desafíos, relacionados con la extraterritorialidad de la norma, la no existencia de fronteras físicas, las múltiples jurisdicciones interactuando, la reducción del Estado-Nación, y la responsabilidad otorgada para que sean las corporaciones las que salvaguarden derechos humanos como el de privacidad y datos, diluyen en un mundo digital global el alcance que tiene el derecho de protección de datos en el mundo físico. Esto particularmente desde los países periféricos, que no actúan en bloque regional y que no tienen mecanismos efectivos de obligatoriedad y cumplimiento de sus normas nacionales.

Aunado a lo anterior, se ha identificado la necesidad de reconocer la configuración de nuevas manifestaciones del derecho de protección de datos personales, atendiendo la forma en la que funciona, y se incorporan los sistemas de inteligencia artificial, como el derecho de reclamación frente a decisiones automatizadas, el derecho a no ser sometido a tratamientos de datos a través de inteligencia artificial y el derecho a que la persona no sea identificada en lo tratamientos a través de esta técnica.

Por otro lado, frente al crecimiento exponencial de la inteligencia artificial, nos encontramos que los sistemas son programados para cumplir requisitos formales normativos para el tratamiento de datos personales, sin que esto signifique que sean tratamientos éticos. Es decir, estamos frente a tratamientos lícitos, pero en muchos casos no éticos.

de inteligencia artificial por otorgar el consentimiento sin comprender las dimensiones del tratamiento de la información, pero se debe tener en cuenta, primero la falta de educación digital de los usuarios (porque existe muy poca política pública efectiva de educación e inclusión digital en México); en segundo lugar, los condicionamientos para la prestación de servicios necesarios, incluso aunque sean contrarios a las normas nacionales; en tercero, la instrumentación de cláusulas de adhesión en los contratos; y en cuarto, la responsabilidad final y única de las corporaciones para insertar aspectos éticos en el tratamiento de datos, que pudieran generar confianza.

# EL AVANCE DE LAS TECNOLOGÍAS PARA LA INFORMACIÓN

PEDRO VICENTE VIVEROS REYES

*Integrante del Comité de Participación Social de Jalisco*

Licenciado en Estudios Políticos y Gobierno por la Universidad de Guadalajara, es Maestro en Gobierno y Administración Pública Municipal y Estatal por el Colegio de Jalisco. Actualmente cursa un Doctorado en Sistema de Justicia y Anticorrupción. Además cuenta con diplomados en diversas áreas del conocimiento, destacando las siguientes: Transparencia, Acceso a la Información y Rendición de Cuentas en la Administración Pública; Ética Pública, Transparencia y Anticorrupción; Reglamentación Municipal; Gobierno y Gestión Local, entre otros.

A lo largo de su vida profesional, se ha desempeñado en diversos cargos, como: Secretario Técnico de la Secretaría General de Gobierno; Jefe de Gabinete del Ayuntamiento de San Pedro Tlaquepaque; Consejero Ciudadano del Instituto de Transparencia, Información Pública y Protección de Datos Personales del Estado de Jalisco; Director General de Vinculación, Coordinación y Colaboración con Entidades Federativas del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI); Jefe de Departamento en la Unidad de Transparencia del Instituto Electoral y de Participación Ciudadana del Estado de Jalisco; Secretario Técnico del Consejo para la Transparencia y la Ética Pública en el Municipio de Guadalajara; Asesor de Regidores en el Ayuntamiento de Guadalajara; Profesor de Tiempo Completo en el Centro Universitario del Norte de la Universidad de Guadalajara; y es actualmente integrante del Comité de Participación Social (CPS) del Sistema Anticorrupción del Estado de Jalisco.

En el mundo, tanto a través de las empresas como en las funciones de gobierno, todo tiende hacia la automatización. El desarrollo de inteligencias artificiales que atiendan las necesidades de las

personas en tiempo real es una constante que no hace más que crecer. Sin embargo existe una brecha que hay que subsanar, aunque empresas y gobiernos tienen la tendencia de que las inteligencias artificiales atiendan a su público, la brecha de analfabetismo digital debe reducirse para que dicha automatización sea efectiva y garantice la seguridad de las personas que usan estos servicios y plataformas.

La automatización de procesos a través de las inteligencias artificiales y el avance de las tecnologías de la información son medios para mejorar la vida cotidiana de los ciudadanos. Debemos reconocer que su avance es imparable, progresivo, exponencial, y que cada vez son más intuitivas y de más fácil acceso, teóricamente haciendo más fácil la resolución de problemas cotidianos. Sin embargo, esto también tiene un lado oscuro: estas herramientas promueven deliberadamente ataques y malos manejos por parte de especialistas que buscan las partes más vulnerables de diversos sistemas para hacer uso indebido de la información pública y de violentar la privacidad de las personas, usurpando su personalidad e invadiendo su privacidad, lo cual es un riesgo a su seguridad, y un amplio espectro de delitos que parece que avanzan a la misma velocidad que la automatización de todos los sistemas.

Vigilar, controlar y asegurar todo el gran flujo de datos que circula a través de las tecnologías de la información es una necesidad urgente, ya que este tipo de delitos rebasa fronteras y excede los controles legales, volviéndose muy difícil ubicar, o sancionar la comisión de estos llamados delitos cibernéticos. Además, no sólo hay que cuidar a los usuarios de los delincuentes digitales, sino también garantizar que las grandes corporaciones hagan un uso ético en el trato y manejo de los datos personales que se encuentran en sus servidores; un asunto que ha llegado hasta los congresos de las naciones más tecnologizadas del mundo, como la que obligó a la plataforma Facebook a responder sobre la venta de información de su *Big Data* a empresas privadas, sin el consentimiento ni conocimiento de sus usuarios.

Actualmente, existe una disparidad en las velocidades en el avance de la tecnología y la adecuación normativa para prevenir y sancionar los delitos informáticos o el mal uso de datos personales por parte de privados. Por ello es indispensable e ineludible potencializar los esquemas de la educación en las tecnologías de información y la alfabetización tecnológica de los usuarios con el fin de prevenir este tipo de actitudes ilegales e inmorales, así como construir una ruta para lograr que instituciones como la nuestra cumplan su función de proteger a los ciudadanos.

Para lograr esto es necesario incorporar al sistema educativo estos

temas para que, desde la educación básica y media básica, se incorporen unidades de estudio específicas, con miras a prevenir a los usuarios y futuros usuarios de las malas prácticas, y garantizar que no caigan en malas manos sus datos personales. La información personal es una propiedad que debe ser cuidada, garantizada y vigilada como cualquier propiedad privada, e incluso más, debido a su intangibilidad y vulnerabilidad. En el contexto actual se vuelve prioritario saber proteger todos los datos que garantizan nuestra seguridad digital y nuestra seguridad personal. Es un derecho fundamental para mantener nuestra identidad e integridad tanto digital como física.

Desde los sistemas anticorrupción se busca coadyuvar con todos los órganos garantes para, en conjunto, potencializar los esfuerzos que abonen a esta inmediata, ardua y permanente tarea. La facilidad del uso de los medios digitales puede hacer que las personas sean descuidadas o negligentes en materia de protección. Desde nuestra trinchera, debemos garantizar que las personas tengan la educación suficiente para dimensionar la importancia que tiene el cuidado de sus datos; para que estén alerta sobre los engaños que existen en los medios electrónicos; y tengan la seguridad de que existen mecanismos para denunciar y sancionar las malas prácticas y para que sepan que cuentan con el apoyo institucional.

# RUTA de la PRIVACIDAD

# EJE TEMÁTICO III

## *FORTALECIMIENTO INSTITUCIONAL A TRAVÉS DE LA RUTA DE LA PRIVACIDAD*

# RUTA DE LA PRIVACIDAD

ADRIÁN ALCALÁ MÉNDEZ

*Comisionado del INAI*

Licenciado en Derecho y Maestro en Amparo. Ha sido conferencista, panelista y articulista en temas de derecho de acceso a la información y protección de datos personales.

Catedrático en la Universidad Nacional Autónoma de México, docente en materia de transparencia y acceso a la información en diversos diplomados, programas y talleres, así como expositor y conferencista en eventos tanto nacionales como internacionales desde 2009.

En 2011, fue Consejero Propietario del Instituto de Transparencia y Acceso a la Información Pública del estado de Baja California, siendo el primer Consejero Presidente. También fue electo Coordinador de la Asamblea Regional Norte de la entonces Conferencia Mexicana para el Acceso a la Información Pública.

De 2014 a 2020 fue designado Secretario de Acceso a la Información. Actualmente es Comisionado del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Las jornadas que forman parte del proyecto denominado Ruta de la Privacidad se han realizado con motivo de la conmemoración del Día Internacional de Protección de Datos Personales, que se celebra el 28 de enero de cada año.

El proyecto de mérito es un esfuerzo interinstitucional de socialización entre el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, y los organismos garantes de las entidades federativas, en colaboración con el Sistema Nacional de Transparencia, cuyo propósito es concientizar y promover la importancia del derecho fundamental a la protección de los datos personales.

En ese sentido, en el marco de estas actividades, he tenido el agrado de participar en diversos foros y eventos impulsados por los organismos

garantes de los estados de Querétaro, Michoacán y Quintana Roo, donde el tema principal fue enfocado a la ciberseguridad o seguridad informática, así como a la protección de los datos personales. Inclusive, en este último caso se adicionó un tema de suma importancia: la protección de datos personales de los turistas.

Durante mis intervenciones tuve la oportunidad de precisar que la ciberseguridad o seguridad informática es la disciplina encargada de identificar vulnerabilidades, así como proteger los dispositivos y sistemas electrónicos, situación que se relaciona estrechamente con el derecho fundamental a la protección de los datos personales, toda vez que se vincula con las medidas de seguridad físicas, técnicas y administrativas que los responsables deben implementar para salvaguardar la información de carácter personal.

Lo anterior con independencia de los sectores de la población en los que se encuentren, como es el caso de las entidades federativas que tienen una mayor afluencia de turistas como parte de sus actividades económicas; desde agencias de viajes y prestadoras de servicios de transporte terrestre o aéreo, hasta hotelería e, incluso, algunas instancias gubernamentales tratándose de viajes internacionales, principalmente.

En esa tesitura, tanto la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* como la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* y la normatividad que de ellas derivan contemplan la existencia del deber de seguridad, de acuerdo con el cual los responsables del tratamiento deben tomar en cuenta una serie de factores y llevar a cabo diversas acciones para el establecimiento e implementación de medidas de seguridad que permiten proteger los datos personales contra daño, pérdida, alteración, destrucción, uso, acceso o tratamiento no autorizado.

Ahora bien, de acuerdo con los resultados de la *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2020*, se pudo advertir la alta inserción que tiene en la actualidad el uso de Internet entre la población mexicana y, en consecuencia, la importancia de conocer aspectos esenciales en materia de ciberseguridad y protección de datos personales para llevar a cabo una navegación segura, sin que ello pueda eliminar en su totalidad la posibilidad de ser víctima de toda clase de ataques o técnicas de ingeniería social.

Dichos aspectos pueden abordarse desde un enfoque preventivo o reactivo; es decir, educar, concientizar y brindar herramientas para minimizar los riesgos, amenazas y vulnerabilidades que pueden presentarse en medios electrónicos, así como inhibir conductas que pudieran generar afectaciones a la esfera jurídica de las personas titulares a partir del establecimiento de sanciones de diversa índole, como consecuencia de actos u omisiones que

vulneren la regulación aplicable. Asimismo, en el ámbito internacional ha tomado especial importancia la cantidad de incidentes de seguridad y actividades ilícitas, como las filtraciones y *hackeos* cometidos a través de medios electrónicos, motivo por el cual fue adoptado por el Comité de Ministros del Consejo de Europa el *Convenio de Budapest*, mismo que entró en vigor el 1 de julio de 2004 y es el tratado internacional más importante relacionado con el combate a la ciberdelincuencia.

Sobre el particular, resulta esencial precisar que las conductas específicamente relacionadas con la ciberdelincuencia no se encuentran comprendidas dentro del ámbito del derecho a la protección de los datos personales, toda vez que son situaciones de naturaleza penal tipificadas como delitos, cuya investigación, persecución y sanción corresponde a las instancias competentes en esa materia, como las fiscalías y los juzgados penales.

Lo expuesto anteriormente reviste especial importancia en la medida en que los avances tecnológicos tienden hacia el desarrollo de un «Gobierno Digital», entendido como las acciones basadas en las tecnologías de la información y comunicación, especialmente Internet, que el Estado implementa para aumentar la eficiencia de la gestión pública, mejorar los servicios ofrecidos a la población y proveer a las acciones de gobierno de una mayor transparencia.

Finalmente, no debemos perder de vista que, en la misma medida que la tecnología nos permite automatizar y generar impactos positivos en la calidad de vida de los gobernados, también podemos encontrar una proporción equivalente sobre las amenazas y riesgos a los que estamos expuestos en el entorno digital.

# EL PODER DE PROTEGER NUESTROS DATOS

NORMA JULIETA DEL RÍO VENEGAS

*Comisionada del INAI*

Integrante del Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI), el máximo órgano garante en México, encargado de tutelar los derechos de Acceso a la Información y de Protección de Datos Personales.

Con estudios de Licenciatura en Administración de Empresas por el Instituto Tecnológico de Zacatecas, es Maestra en Administración Pública por la Universidad Autónoma de Fresnillo, Zacatecas, y Doctora en Administración Pública por el Instituto Internacional del Derecho, en coordinación con la Universidad Autónoma de Zacatecas.

Es integrante de las 11 Comisiones temáticas del Sistema Nacional de Transparencia (SNT), así como de 4 de las 11 Comisiones permanentes del INAI, coordinando tres de ellas: Indicadores y Evaluación; Tecnologías de la Información —de la cual depende la Plataforma Nacional de Transparencia (PNT)— y la de Vinculación y Promoción del Derecho.

Bajo la coordinación de las Comisiones permanentes se implementaron buscadores temáticos de la PNT, se desarrolló un chatbot con inteligencia artificial llamado CAVINAI para ofrecer asesoría a las y los ciudadanos como parte del Centro de Atención a la Sociedad (CAS). Asimismo, es presidenta del Comité Editorial del INAI, a través del cual se publican cuadernos, diccionarios y libros especializados en la materia.

En los últimos 31 años ha trabajado en áreas relacionadas con la transparencia, la fiscalización y la rendición de cuentas. Fue comisionada del Instituto Zacatecano de Transparencia, Acceso a la Información y Protección de Datos Personales (Órgano Garante Local), de 2015 a noviembre de 2020, siendo en 2018 la primera comisionada presidenta. Coordinó los trabajos preparativos de la primera ley de acceso a la información públi-

ca en dicha entidad e impulsó una reforma a la misma. Fue Contralora General del Gobierno del Estado de Zacatecas y coordinadora nacional de la Comisión Permanente de Contralores Estados Federación del país.

Actualmente escribe y colabora en 10 medios de comunicación en México, entre los que destacan los periódicos *El Heraldo*, *El Universal*, *El Financiero* y *El Sol de México*.

La evolución tecnológica, si bien ha contribuido al desarrollo de la sociedad, también ha sido fuente de malas prácticas que en la actualidad se posicionan directamente en las agendas de naciones democráticas como la nuestra. Los grandes fraudes financieros, el hackeo de plataformas empresariales o el robo de datos en servicios bancarios, entre otros, han hecho evidente la necesidad de poner sobre la mesa los peligros que enfrentamos en el ciberespacio. No existe un terreno neutral en la red, de ahí que visibilizarlos resulta en medidas de contención que nos pueden dar mayor seguridad a la hora de usar el internet.

La privacidad se posiciona entonces como una preocupación legítima en nuestra sociedad. De los avances tecnológicos y la digitalización de la comunicación interpersonal aparecen riesgos para tener en cuenta: aquí inicia el necesario estudio que nos lleve a desarrollar barreras de contención que nos permitan emplear los avances a través de prácticas seguras e informadas. Tan sólo en México existen cerca de 88.6 millones de usuarios de internet, los que, en perspectiva, representan 75.6 % de la población[70]. Esto significa que cada usuario de la red es un objetivo potencial susceptible de vulneración o sustracción de información personal.

Ante este escenario, es apremiante desarrollar iniciativas como la Ruta de la Privacidad, en la que buscamos aportar sustantivamente a la discusión de los retos en torno a la protección de datos personales. Se trata de un proyecto beneficioso que surge del INAI y del SNT, el cual reúne a académicos, estudiantes y especialistas en protección de datos personales, así como órganos garantes de todo el país para enriquecer el debate. Sin duda, el trabajo de la Comisionada Josefina Román Vergara, del Comisionado Francisco Javier Acuña y de la Comisión de Protección de Datos Personales, coordinada por Arístides Rodrigo García, ha sido fundamental.

Con la Ruta de la Privacidad buscamos estar a la vanguardia en la evolución digital: saber a qué nos enfrentamos, no sólo como ciudadanos usuarios de tecnología de manera cotidiana, sino también como autori-

[70] Visitar: https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2022/OtrTemEcon/ENDUTIH_21.pdf

dades, en un compromiso urgente para el desarrollo de políticas públicas eficaces, preventivas y no correctivas, pensadas específicamente para el usuario mexicano.

Nos enfrentamos a tecnologías desafiantes: por ejemplo, la inteligencia artificial, el metaverso o el llamado *Big Data*. Sin embargo, como órganos garantes nos corresponde intervenir y proponer soluciones en una nueva dinámica del flujo que coloca a los datos personales como el principal activo de esta era tecnológica.

Entendámoslo: la vulneración de nuestra información y la irrupción en nuestra privacidad tiene el potencial de afectar nuestro patrimonio, integridad y seguridad personal. La idea no es ir en contra de la tecnología, sino estar preparado y navegar en un mismo sentido a la hora de convivir con ella, puesto que su integración en nuestras vidas está pensada para aportar beneficios; de ahí que debemos exigir que las legislaciones integren iniciativas pensadas en estos avances, para así informarnos y conocer los datos que proporcionamos a terceros.

Desde atender al aviso de privacidad, hasta dar acceso a nuestros datos biométricos, requiere que prestemos atención a quién, cómo y dónde se resguarda nuestra información personal. Poner especial atención «a la letra pequeña» es de suma importancia.

El resultado de las diversas ediciones de la Ruta de la Privacidad ha permitido fortalecer la comunicación entre ciudadanos y expertos. Así, distintos sectores se han sumado al proyecto y logramos avanzar hacia la construcción de comunidades más participativas que analizan, preguntan y actúan desde la virtualidad. Éste es justamente el objetivo de estas charlas: sumar a los distintos sectores sociales para visibilizar los riesgos que existen en la red, además de apropiarse de nuestro derecho a la protección de datos personales.

Ésa es la ruta que debemos seguir para construir entornos digitales seguros para todas y todos. El camino está dicho: ahora nos toca tomarlo en el sentido correcto.

# LA RUTA DE LA PRIVACIDAD EN MICHOACÁN

ABRAHAM MONTES MAGAÑA

*Comisionado del Instituto Michoacano de Transparencia, Acceso a la Información y Protección de Datos Personales (IMAIP)*

Comienzo estas líneas recordando con gran gusto las cuatro ocasiones en las que pude asistir y participar en el extraordinario ejercicio organizado por el INAI, por conducto de la Comisionada Dra. Josefina Román Vergara y el Comisionado Dr. Francisco Javier Acuña Llamas; así como por el Comisionado Presidente del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales y Coordinador de la Comisión Temática de Protección de Datos Personales de nuestro querido SNT, Dr. Arístides Rodrigo Guerrero García, artífices de este proyecto tan exitoso pero sobre todo efectivo para acercar a las entidades federativas el derecho fundamental de la protección de los datos personales, sensibilizando y concientizando a las autoridades y a la ciudadanía sobre la importancia y el cuidado que requerimos y debemos tener para salvaguardar nuestra *Privacidad*.

En el caso de su servidor, tuve la oportunidad de participar como ponente primeramente el 31 de enero de 2022 en la Ruta de la Privacidad en el estado de Yucatán. En esa ocasión, la Ruta tuvo como eje central «La Inteligencia Artificial, el internet de las cosas y los riesgos de la información confidencial a través del internet». Tuve a bien participar en el panel denominado «El derecho humano de la protección de datos personales en el avance de las tecnologías de la información».

En ese tenor, expuse cómo las tecnologías de la información avanzan a una altísima velocidad, el riesgo al que todos los días se enfrentan nuestros datos personales y los múltiples desafíos ante su exposición masiva, con diversos escenarios y consecuencias. Destaca el caso del ya conocido robo de identidad, fenómeno catalogado como el más peligroso para la

humanidad en el rubro tecnológico y que se incrementó de una manera exponencial derivado de la pandemia del COVID-19. De igual manera, señalé la necesidad de fortalecer nuestro marco normativo sin interponer el desarrollo de la ciencia, pero sí regulando y legislando sobre temas trascendentales, cotidianos y de alto riesgo ante una posible intromisión a la privacidad de las personas.

Por otra parte, el 11 de marzo de 2022 participé en la Ruta de la Privacidad en el estado de Nuevo León, particularmente en el panel «Implicaciones para la Protección de datos personales en una ciudad inteligente (*Smart City*)», en el cual expuse cómo la inteligencia artificial se ha convertido en una de las herramientas más poderosas en la época moderna y con potencial para mejorar la existencia de la humanidad. No obstante, paradójicamente al mismo tiempo ella amenaza con incrementar las brechas sociales, poner en peligro nuestra privacidad y nuestros datos personales, y con posibilidades de ocasionar la desaparición de millones de empleos a nivel mundial.

Asimismo, sostuve que las ciudades inteligentes ejemplifican cómo la innovación tecnológica puede ayudar a resolver problemas sociales, mejorar la calidad de vida en las ciudades, reducir el impacto ambiental, proporcionar información útil y estratégica para tomar mejores decisiones, mejorar la prestación de servicios y utilizar los datos que generan los individuos para beneficio de la colectividad.

No obstante lo anterior, las ciudades inteligentes requieren de una cantidad macro de datos de las personas que residen en ellas. Estos datos incluyen su ubicación, movilidad, uso de servicios públicos, hábitos de consumo, entre muchas otras posibilidades para la generación de información e inteligencia, por lo cual resulta necesario fortalecer la colaboración y coordinación entre todos los actores involucrados para promover el desarrollo de ciudades inteligentes basadas en inteligencia artificial, con un manejo ético de la misma, cuidando en todo momento el derecho fundamental de la protección de los datos personales, prevaleciendo la dignidad humana, preservando la privacidad y utilizando a la tecnología como un método para consolidar una mejor sociedad.

Finalmente, tuvimos el honor de recibir el 1 de abril de 2022 la Ruta de la Privacidad en el estado de Michoacán con el tema «Inteligencia Artificial: perspectivas y prospectivas desde el derecho a la protección de datos personales y la privacidad». Se contó con la participación de numerosos sujetos obligados, representantes de la sociedad civil organizada, de la academia, funcionarios municipales y estatales, quienes tuvimos la oportunidad de escuchar a grandes panelistas sobre la materia que nos ocupa.

Asimismo, el 3 de junio tuve la oportunidad de participar en la Ruta de la Privacidad Querétaro, como moderador del panel «Mejores prácticas en el cuidado de Datos Personales en el Sector Público», en el cual se expuso en voz de expertos la importancia de la protección de los datos personales por parte de los servidores públicos, mediante casos prácticos que han sido exitosos y que resultan eficaces para prevenir la vulneración de este derecho humano.

Como se podrá observar, concluyo mi memoria reconociendo a todas y todos los actores que hicieron posible este importante ejercicio, desde su diseño como una idea hasta su implementación como un exitoso proyecto. Sigamos apoyando y llevando a todo nuestro país mecanismos como la Ruta de la Privacidad, que fortalecen a nuestras instituciones, pero, sobre todo, hacen mayormente efectivo con la ciudadanía y consolidan el derecho fundamental de la protección de datos personales que nos corresponde garantizar.

# LA RUTA DE LA PRIVACIDAD EN NUEVO LEÓN

MARÍA TERESA TREVIÑO FERNÁNDEZ

*Consejera Presidenta del Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales y Coordinadora de la Comisión de Gobierno Abierto y de Transparencia Proactiva del SNT*

Licenciada en Derecho por la UDEM. Ha desarrollado su experiencia laboral y profesional en el campo del Derecho, tanto en el Sector Público como en el Privado. Especialista en temas de Transparencia, Acceso a la Información y Protección de Datos Personales.

Especialista certificada en Protección de Datos Personales por la Universidad Complutense de Madrid. Experta en Delegado de Protección de Datos por la Universidad de Sevilla, España.

Cuenta con Diplomado en Gestión Documental por la Facultad de Derecho y Criminología de la UANL. Fue reconocida por el Archivo General de la Nación por su impulso y contribución al desarrollo archivístico del Estado de Nuevo León. Es Maestra en Ciencias Políticas por la Facultad de Ciencias Políticas y Relaciones Internacionales de la UANL. Es Consejera Presidenta del Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales y Coordinadora de la Comisión de Gobierno Abierto y de Transparencia Proactiva del SNT.

Durante la presente jornada, y con la participación de expertos en la materia, se desarrolló el tema de las implicaciones de la protección de datos personales en las ciudades inteligentes, donde se abordaron beneficios y riesgos que proceden del tratamiento de los datos personales dentro de la infraestructura de las ciudades inteligentes.

Bajo ese contexto, cada uno de los participantes brindó su punto de vista, así como opiniones y sugerencias, que buscan equilibrar el beneficio de la tecnología y la protección de la información de carácter personal que

se encuentra en posesión de las instituciones públicas y privadas.

Así, en el primer panel relativo a las Implicaciones de la protección de datos personales en una ciudad inteligente, el Comisionado Guerrero hace mención del estudio denominado *Nuestros Datos Nunca Duermen*. Ha mostrado que fluye por la red una gran cantidad de datos por minuto, como los mensajes difundidos a través de la plataforma de comunicación denominada WhatsApp, así como de imágenes de Instagram, lo que muestra el fenómeno de migración de nuestra vida en el mundo físico hacia el mundo digital.

Si bien existen ventajas de este flujo continuo de datos, también se encuentra la posibilidad de generarnos un riesgo en cuanto a la vulneración de nuestros datos personales, a través del uso de motores de búsqueda o activar la geolocalización en nuestros dispositivos inteligentes, ya que en ella se almacena información que es difundida a empresas sin autorización de nuestra parte. Por tal motivo, el Comisionado atinadamente hace un atento llamado a observar nuestra legislación en materia de Datos Personales. Entre ellas destaca la *Ley Federal de Protección de Datos Personales en Posesión de Particulares*, la cual refiere que debe de ser analizada para una reforma, con el fin de actualizarla, teniendo como referencia diversos estándares internacionales, como Canadá o la *Ley 3/2018* de España, mismas que contemplan la protección de datos personales en el entorno digital.

Por su parte, la Dra. Josefina Román Vergara, Comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, refiere el crecimiento acelerado de la urbanización, lo que genera desafíos como la construcción de ciudades inteligentes, mismas que se vislumbran como un símbolo del futuro y promesa del desarrollo para enfrentar los retos que las grandes ciudades afrontarán en el mundo. Del mismo modo, la Dra. Román hace referencia al concepto de ciudad inteligente, la cual es definida como «la integración efectiva de los sistemas físicos, digitales y humanos, en el entorno construido para ofrecer un futuro que sea sostenible, prospero e inclusivo para sus ciudadanos».

En dicha ponencia se destacan los beneficios y riesgos que implican las ciudades inteligentes, entre los que se encuentran mejorar la vida de las personas, medio ambiente, evitar costos excesivos a los ciudadanos, optimización de servicios públicos, así como transparencia en las administraciones públicas y la agilización de la comunicación con el ciudadano. Sin embargo, también involucra una mayor accesibilidad a la información de las personas por parte de las administraciones públicas o de otro sujeto implicado en la prestación de servicios públicos.

En ese sentido, destaca que el crecimiento y la complejidad de la in-

fraestructura que emplea el cómputo en la nube, internet, *big data* o las redes móviles generan también una vulnerabilidad en cuestión de seguridad y privacidad de los datos personales.

De manera que el reto de las ciudades inteligentes es crear mecanismos que impidan esa vulneración a la privacidad en los ciudadanos. Para llevar a cabo dicha tarea, la Doctora Josefina refiere el cumplimiento de diversas Normas, entre ellas la ISO 9,100 y la ISO/IEC TS 27570-2021.

Además, la Doctora Andrea Mendoza Enríquez**,** Investigadora en el Centro de Investigación y Docencia Económica, sostuvo que la inteligencia artificial es considerada como la toma de decisiones a partir del procesamiento masivo de datos. La Doctora Mendoza Enríquez destaca los semáforos inteligentes, donde verifican el tráfico y con ello se pueden tomar decisiones para mejorar el flujo vehicular.

En este sentido, hace hincapié en que la inteligencia artificial se encuentra presente en la mayoría de los rubros de la sociedad. Es considerada un potenciador, no únicamente en los mercados, también en la eficiencia del Estado y el cumplimiento de sus fines.

Asimismo, el uso de la tecnología no debe de estar sujeta a objetivos políticos, sino que debe de enfocarse —ya sea a corto, mediano o largo plazo— al beneficio de la sociedad.

En cuanto a la protección de datos personales, menciona que es necesario tomar en cuenta que cualquier implementación tecnológica debe estar enmarcada en los límites constitucionales, que atienda a las medidas y restricciones de los derechos humanos.

Abraham Montes Magaña, Comisionado del Instituto de Transparencia y Acceso a la Información Pública y Protección de Datos Personales (IMAIP), expuso que la inteligencia artificial se ha convertido en una de las herramientas más poderosas de la época moderna, cuenta con el potencial para mejorar la existencia de la humanidad. A su vez, menciona que amenaza con incrementar las brechas sociales, poner en peligro nuestra privacidad y nuestros datos personales, así como provocar la desaparición de millones de empleos alrededor del mundo. En ese sentido, el Maestro Montes Magaña enfatiza en la necesidad de conocer el impacto de la IA, en el entendido de que su desarrollo debe ser dentro de un marco ético y legal que se encamine al mejoramiento de la vida humana.

Del mismo modo, las ciudades inteligentes serán un mecanismo para lograr atender las necesidades de los habitantes, debido a que éstas buscan optimizar el manejo de los recursos para fomentar el bienestar social y calidad de vida. Para ello se lleva a cabo una relación entre los ciudadanos y los objetos que se encuentran interconectados con la IA. Esto optimiza

la toma de decisiones y la prestación de servicios, implicando un mayor flujo de datos para llevar a cabo estas acciones para la alimentación de la IA.

Esto involucra un riesgo en el tratamiento de datos en las ciudades inteligentes. Uno de ellos se refiere al acceso con el que cuentan los proveedores y empresas privadas que brindan sus servicios, así como asegurar que el tratamiento de la información no se encuentre vinculado a una persona física, que posteriormente permita identificar a su titular, poniendo en riesgo la privacidad y la protección de sus datos personales.

Como organismos garantes, abunda, es necesario fomentar el diseño de marcos de actuación donde se desarrolle la inteligencia artificial en un contexto de protección a la privacidad y protección de datos personales. Por ello propone a través de varios puntos para promover lo anterior, entre ellos establecer criterios de gobernanza de datos que especifiquen los posibles impactos negativos mediante el uso de IA; marco jurídico fortalecido, orientado hacia las predicciones algorítmicas; reglas de divulgación de datos generados por IA, obligatoriedad de las empresas privadas de IA a publicar criterios y estándares éticos relacionados con el tratamiento de datos personales, entre otros.

Asimismo, el Doctor Joel Gómez Treviño, de la Academia Mexicana de Derecho Informático, señaló que las ciudades inteligentes buscan el crecimiento económico, participación y mejor calidad de vida para el ciudadano. Para ello, se requiere de implementación de tecnologías que permitan a los ciudadanos contar con buenos servicios. Las ciudades inteligentes, refiere, deberían de enfocarse en crear ciudadanos inteligentes. No existe un concepto universal de las ciudades inteligentes: derivado de ello, hace alusión a ciertas características que las forman: Red de sensores conectados a objetos del mundo real; redes de comunicación digital que permite el flujo de datos que eventualmente podrán analizarse; y contar con una infraestructura que permita almacenar la información recabada anteriormente y dar paso a la interconexión de datos.

Derivado de ello, establece que es posible entender que las ciudades inteligentes permiten que las personas se comuniquen con datos, cosas, objetos y procesos de carácter global y dinámico, lo que favorecería el mejoramiento en los procesos y servicios. De esta manera, según lo explicado por el panelista, para el buen funcionamiento de las ciudades inteligentes es necesario contar con una infraestructura en telecomunicaciones que permita dichas comunicaciones.

En ese sentido, indica que, así como existen beneficios al contar con una ciudad inteligente, existen riesgos. Uno de ellos es la gran cantidad de flujo de datos con los que cuentan estas ciudades, ya que no queda

suficientemente claro quiénes manejan ese flujo de datos, lo que conduce a un sesgo en la información. Para un adecuado manejo del flujo de datos, se debe de prestar atención al desarrollo e implementación de la inteligencia artificial.

Por último, el Maestro Vitelio Ruiz, Director General de Investigación y Verificación del Sector Público del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, abordó los riesgos que existen en las ciudades inteligentes. Uno de ellos es saber qué sucede con las medidas de seguridad y los esquemas de colaboración entre entidades públicas y privadas, ya que se cuenta con dos dispositivos normativos, como la *Ley General de Protección de Datos en Posesión de Sujetos Obligados*, lo que atañe a la generación de dudas al momento de su aplicación, respecto del tratamiento de los datos personales, debido a la creación de asimetrías normativas.

Por otro lado, menciona que las ciudades inteligentes, debido al uso de tecnologías y de inteligencia artificial, con relación a la recolección de datos, va encaminada a mejorar la calidad de vida de sus habitantes, los procesos y servicios de la ciudad. Sin embargo, esto indica una serie de implicaciones respecto a la privacidad, derivado del constante monitoreo hacia las personas. Es decir, a través de éste es posible conocer los hábitos personales de los ciudadanos. Por lo tanto, es necesario contar con filtros que permitan regular la privacidad de las personas.

Para finalizar, el Maestro Ruiz llama a que tanto instituciones públicas como privadas colaboren para el desarrollo de tecnologías e inteligencia artificial que permita no únicamente el flujo de datos de manera continua para el beneficio de las personas, sino que, además, sea capaz de crear medidas de seguridad que garantice la protección de los datos personales de los ciudadanos y evitar el mal uso de éstos.

# FORTALECIMIENTO INSTITUCIONAL A TRAVÉS DE LA RUTA DE LA PRIVACIDAD

JULIO CÉSAR BONILLA GUTIÉRREZ

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

Fue Comisionado Presidente del INFO CDMX del 20 de diciembre de 2018 al 20 de diciembre de 2021, y Coordinador de los Organismos Garantes de las Entidades Federativas del Sistema Nacional de Transparencia 2020-2021.

Maestro en Derecho y Especialista en Derecho Electoral con mención honorífica por la División de Estudios de Posgrado de la Facultad de Derecho de la UNAM.

Es Profesor en el Posgrado en Derecho de la UNAM, donde ha impartido cátedra en la Especialización en Derecho Constitucional y Especialización Derecho a la Información, así como en la Maestría en Derecho.

Ha participado en diferentes foros, seminarios y diplomados en temas de Transparencia, Datos Personales, Acceso a la Información Pública, Rendición de Cuentas, Sistemas Anticorrupción, Derecho Electoral, Democracia, Elecciones, Derechos Humanos.

En la actualidad, la vigencia, el respeto y la efectiva garantía del derecho humano a la protección de los datos personales, la privacidad y la autodeterminación informativa de las personas son temas relevantes que cruzan por consideraciones necesarias relacionadas con el desarrollo tecnológico en el campo digital que, como humanidad, hemos experimentado en las últimas dos décadas y que previsiblemente continuarán siendo las normas en el futuro.

Tales avances y desarrollos, en forma de aplicaciones, redes y plataformas digitales en las que convivimos e interactuamos a diario y a cada instante, si bien facilitan las comunicaciones, el comercio, la democratización de la información, las capacidades educativas, colaborativas y las interacciones humanas de todo tipo a nivel global, en muchas ocasiones tales elementos tecnológicos aplicados al análisis de información a través de inteligencias artificiales, como con las que hoy contamos y convivimos en el ciberespacio, son potencialmente intrusivos respecto de los datos personales que compartimos en el espacio digital. Datos sobre los cuales perdemos control de forma casi instantánea al hacerlo.

Los avances del *Internet*, desde sus inicios y hasta hoy, han sido exponenciales. Pasamos de ser consumidores de datos a generarlos, editarlos, compartirlos, replicarlos y difundirlos activamente, con alcances mundiales, en tiempo real y en todo tipo de formatos.

En tal escenario, es preciso que tomemos en cuenta que nos acercamos vertiginosamente a un mundo interconectado en lo digital, pero no solamente entre personas. Una cantidad cada vez más grande de dispositivos que utilizamos en nuestra vida diaria no sólo interactúa con nosotros a través de las funciones que cumple de cara a las usuarias y usuarios que somos; sino que, de igual modo, esos dispositivos interactúan entre ellos y comparten información que incluye datos personales de los que somos titulares.

En virtud de lo anterior, y con miras a un fortalecimiento institucional que se torne en debida eficacia en el cumplimiento de sus funciones, la Ruta de la Privacidad implementada por el Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, representa una decidida política pública transversal y multinivel en materia de cultura de protección de datos personales, a efecto de que todas las personas, en condiciones de apertura, inclusión y equidad, se encuentren y convivan en ecosistemas digitales seguros y no intrusivos de su intimidad y privacidad. A tales esfuerzos debemos sumar intensivas y permanentes campañas de socialización de estas nuevas realidades derivadas de lo digital, con el fin de enfatizar la importancia fundamental que tienen los derechos ARCO como correlativos al derecho humano aludido y promover proactivamente su ejercicio para sentar a su vez las bases normativas e institucionales necesarias con miras a su efectiva garantía en el espacio digital.

En tal sentido, debemos comprender que realizar lo anterior se relaciona de modo directo con la necesidad de generar un equilibrio entre la más amplia apertura informativa posible y la protección de los datos

personales en lo digital. Esto en un mundo en el que las lógicas de mercado predominan y los datos de las personas se han convertido en un invaluable activo. Sin tal equilibrio, las personas estaremos expuestas y vulnerables en un sentido práctico, pero también profundo que se vincula con nuestra voluntad y dignidad.

Las inteligencias artificiales, insertas en los desarrollos digitales referidos, originalmente se encuentran alineadas con fines económicos, políticos e ideológicos para los que somos meramente usuarias o usuarios y que, consecuentemente, en poco son compatibles con la lógica de los derechos humanos, su dogmática, principios y/o con la debida consideración y aprehensión sustancial del concepto *persona*.

Debido a ello, el equilibrio al que me refiero no puede ser sino el resultado de un necesario, abierto y amplio diálogo que debemos continuar de modo incluyente y propositivo con todas y todos los actores sociales: instituciones, sociedad civil, academia, desarrolladores, reguladores, etcétera.

Claramente no lograremos un empalme absoluto entre los conceptos *usuario* y *persona*. Sin embargo, ello no debe frenar nuestros esfuerzos por sostener a la segunda de cara al primero y acercar ambas ideas a través de mecanismos que doten en todo momento de certeza a las personas, respecto del modo en el que se tratan sus datos en el espacio digital.

# LA RUTA DE LA PRIVACIDAD Y LA PORTABILIDAD

LUIS GUSTAVO PARRA NORIEGA

*Comisionado del Instituto de Transparencia y Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios*

Es Doctor en Derecho y Abogado por la Escuela Libre de Derecho; Maestro en Administración y Gerencia Pública por el Instituto Nacional de Administración Pública y la Universidad de Alcalá de Henares, España. Fue Secretario de Protección de Datos Personales en el INAI, de 2014 a 2018.

Desde 2018 se desempeña como Comisionado del INFOEM y como Coordinador de las Comisiones de Protección de Datos Personales y de la de Gobierno Abierto y Transparencia Proactiva del Pleno del INFOEM.

Coordinador Nacional de la Comisión de Vinculación, Promoción, Difusión y Comunicación Social del SNT 2022.

Es Coordinador de las Comisiones de Protección de Datos Personales y de la de Gobierno Abierto y Transparencia Proactiva del Pleno del INFOEM. Coordinador de la Comisión de Gobierno Digital del INCAM-Colegio de Abogados.

Articulista quincenal en *El Sol de Toluca*, con la columna Gobernanza Digital.

El SNT ha impulsado la implementación de la Ruta de la Privacidad 2022, con el objetivo de abordar el panorama general actual y hacia dónde se dirige el desarrollo de la inteligencia artificial y los retos que supone para la protección de los datos personales.

Temas de esta índole han salido a discusión debido al significativo avance de la inteligencia artificial en México y el resto del mundo. Por ello, actualmente se busca generar normativas que den plena seguridad y respaldo al usuario.

El uso del Internet, de las herramientas y las plataformas tecnológicas se ha vuelto parte de nuestras vivencias cotidianas. Concebidas inicialmente como auxiliares o facilitadoras de diversas prácticas, estas herramientas y plataformas se han convertido en una necesidad imperante. Niños, jóvenes y adultos por igual son presas fáciles de la tecnología: los videojuegos, las redes sociales, el comercio electrónico y la navegación por la red han ganado terreno rápidamente en la sociedad y la cultura.

Según un estudio realizado en 2021 por la Asociación Mexicana de Internet (AMI) sobre los hábitos de los usuarios en Internet, hasta 2020 existían 84.1 millones de internautas en nuestro país, lo que representa 72 por ciento de la población de 6 años o más. Durante ese año, debido a la pandemia por Covid-19, los usuarios de Internet tuvieron el mayor crecimiento observado en los últimos cinco años. Al cierre de 2020 se contabilizaron 115 millones de teléfonos móviles inteligentes y, en promedio, los usuarios accedieron a sus redes 6.8 días a la semana. Asimismo, siete de cada 10 internautas realizaron videollamadas durante el último año; dos de cada 10 usuarios compraron un producto publicitado en línea y 11 por ciento de la base total de internautas aumentaron su gasto en Internet durante dicho período.

Dentro de la Ruta de la Privacidad 2022, y como parte de las actividades para conmemorar el Día Internacional para la Protección de los Datos Personales, el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX), realizó varias mesas de diálogos con expertos que analizaron los temas de portabilidad, acciones preventivas y sistemas de gestión.

De la información presentada, cabe señalar a la portabilidad como un derecho que tienen los propietarios de datos personales para transferir su información personal, mientras que las buenas prácticas y la evaluación del impacto son herramientas que deben ser utilizadas para un mejor tratamiento de los datos personales en poder de los sujetos obligados o particulares.

Al participar en la mesa de diálogo uno, titulada «Portabilidad», me permití destacar esta facultad como parte del catálogo de derechos de la autodeterminación informativa que permite a cualquier persona obtener, transmitir y transferir su información bajo ciertos formatos electrónicos de manera segura, garantizando así en todo momento el resguardo y la eficacia de la protección de sus datos personales.

A su vez, resalté que en 2019, en el Estado de México se presentaron las primeras solicitudes de portabilidad y hasta enero de 2022 se han in-

terpuesto 42 solicitudes relacionadas con exámenes clínicos, expedientes médicos, así como altas y bajas en los institutos de seguridad social.

Es un hecho, pues, que nuestro escenario traspasa el plano físico y se adentra cada vez más en el espacio virtual, dentro del cual la privacidad y los datos personales, por las propias características del entorno digital, son cada vez más vulnerables. Tal parece que las herramientas tecnológicas generan una especie de falso blindaje, que hace que las personas proporcionen su información sin cuidado alguno.

Finalmente, es necesario destacar que la iniciativa denominada Ruta de la Privacidad 2022 fue puesta en marcha por el INAI, así como por diversos Organismos Garantes de las Entidades Federativas y la Comisión de Protección de Datos Personales del SNT, para ampliar el conocimiento y ejercicio del Derecho de la Protección de Datos Personales y analizar los desafíos que impone el uso amplio de las tecnologías, el creciente mercado digital, la expansión del *Big Data* y el Internet de las Cosas, así como la importancia del derecho a la privacidad en los entornos digitales.

# RUTA DE LA PRIVACIDAD EN QUINTANA ROO CIBERSEGURIDAD Y PROTECCIÓN DE DATOS PERSONALES EN EL TURISMO

ROBERTO AGUNDIS YERENA

*Comisionado del IDAIPQROO y Secretario de la Comisión de Protección de Datos Personales del SNT.*

Licenciado en Derecho por la Universidad Anáhuac; Maestro en Derecho Penal y Amparo por la Universidad Modelo. Se ha desempeñado en Quintana Roo como Abogado Postulante; fungió como Subcoordinador Operativo de Representación Estatal de la Secretaría de la Reforma Agraria y Delegado Estatal de la Representación de la Secretaría de la Reforma Agraria.

Se desempeñó como Director Jurídico del Despacho del Gobernador del Estado de Quintana Roo; posteriormente fue Director Jurídico de la Comisión para la Juventud y el Deporte.

En el Tribunal Electoral del Estado, fungió como Secretario de Estudio y Cuenta, y Secretario Auxiliar de Acuerdos.

Se desempeñó como Abogado Litigante especialista en materia electoral; fue Secretario Técnico de la Comisión Anticorrupción, Participación Ciudadana y Órganos Autónomos de la XVI Legislatura del Congreso de Quintana Roo.

Es claro: la simple referencia a Quintana Roo evoca irremediablemente la mar azul turquesa, el paraíso natural y lo exótico de nuestras ciudades convertidas en destinos turísticos de calidad mundial. Plantear la realización de la Ruta de la Privacidad en nuestro estado era la oportunidad perfecta para vincular dos temas de suma importancia: la protección de los datos personales y la industria turística, mismos

tópicos que tienen también una íntima relación con la ciberseguridad y las nuevas tecnologías.

Con el decidido apoyo y acompañamiento de Josefina Román Vergara, Norma Julieta del Río Venegas y Adrián Alcalá Méndez, Comisionados del INAI, y de Rodrigo Arístides Guerrero García, Coordinador de la Comisión de Protección de Datos Personales del SNT, desde tierras caribeñas logramos por primera vez dar un enfoque «tropicalizado» a los trabajos de la ya exitosa Ruta de la Privacidad.

La relevancia de la temática propuesta llamó la atención incluso del propio Gobernador del Estado, Carlos Joaquín González, quien acudió al llamado del SNT a plantear la postura del Poder Ejecutivo Quintanarroense en la materia pues, siendo este Estado el mayor motor de la industria turística en el país y contando con los destinos vacacionales de mayor envergadura en toda Latinoamérica, la Ruta de la Privacidad fue el foro ideal para la socialización de las políticas públicas adoptadas por el Gobierno Estatal en defensa de los vacacionistas, su ciberseguridad y la protección de sus datos personales.

La tarea era analizar los desafíos derivados del amplio uso de la tecnología en nuestros tiempos, platicar respecto del crecimiento de los mercados y el propio mundo digital y la aceleración en el surgimiento de las herramientas digitales, pero desde la visión del viajero, desde el análisis del prestador de servicios turísticos, y desde la óptica de las autoridades en cuya competencia se encuentra la salvaguarda de la seguridad del turista en todos los ámbitos.

Por ello se diseñaron paneles y mesas de análisis con la participación de la Secretaría de Turismo de Quintana Roo, a cargo de Bernardo Cueto Riestra, quien presentó las acciones implementadas desde el poder público estatal para proteger al turista, desde el momento de la compra de su paquete vacacional hasta durante su presencia en los destinos quintanarroenses.

Las cifras presentadas por la Comisionada Norma Julieta del Río Venegas fueron sustanciales para estos trabajos, pues del análisis a la Plataforma Nacional de Transparencia se obtuvo información precisa de los reclamos más comunes a las empresas prestadoras de servicios turísticos que han omitido o fallado en su labor de protección de los datos personales.

A su vez, el Comisionado Adrián Alcalá Méndez, realizó un interesante análisis normativo y legal de la protección de los datos personales en el ámbito turístico, presentando al auditorio muchos de los casos más emblemáticos resueltos desde el Pleno del INAI, y la evolución de los principales criterios en materia de protección de datos personales en ámbitos como el turístico.

Igualmente, participaron en dichos trabajos empresas de reconocimiento mundial como Grupo Xcaret, propietaria de los parques temáticos más importantes de América Latina y que por conducto de su dirección general de tecnologías explicó de manera concienzuda la forma en la que ejecutan la protección de sus sistemas de seguridad en favor del turista, mostrando la alta calidad y el desempeño de primer mundo que se realiza desde una empresa local.

No menos importante fue la participación a distancia del Maestro Pablo Corona Fraga, Vicepresidente para Ciberseguridad en la Asociación de Internet MX, quien, a través de la Conferencia Privacidad y Turismo, enfatizó el rol trascendental del turista en el cuidado de sus datos, haciendo una invitación a asumir su papel de manera responsable.

Los trabajos desarrollados generaron, sin duda, un amplio reconocimiento por parte de la Comisión de Protección de Datos Personales del SNT; la adecuación de la Ruta de la Privacidad a las condiciones específicas de un estado —en el caso, Quintana Roo— fue el ejemplo perfecto de que una gran idea como esta cruzada nacional sobre la conciencia del derecho humano a la protección de los datos personales ante el uso de la inteligencia artificial puede vincularse a los temas más sensibles y cotidianos de una comunidad.

Desde el IDAIPQROO seguiremos impulsando la Ruta de la Privacidad para dejar conciencia de la importancia de la protección de los datos personales en nuestra vida diaria.

Es nuestra labor y compromiso constitucional.

# FORTALECIMIENTO INSTITUCIONAL A TRAVÉS DE LA RUTA DE LA PRIVACIDAD CRÓNICAS DE LA CIUDAD DE MÉXICO

LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ

*Comisionada del Instituto de Transparencia y Protección de Datos Personales de la Ciudad de México*

Es Maestra en Gestión Pública Aplicada por el Tecnológico de Monterrey, politóloga por el Instituto Tecnológico Autónomo de México y especialista en partidos políticos y transparencia por la Universidad Autónoma Metropolitana.

Se ha desempeñado en cargos de dirección en los Poderes Ejecutivo y Legislativo, y en organismos autónomos, como el INE y el INAI, tanto a nivel local como federal. Cuenta con experiencia en el sector privado como directora en una Cámara Industrial Nacional y en sociedad civil como vicepresidenta de transparencia en la Asociación Mexicana de Integridad y Compliance.

Ha impartido cátedra ante diversas instituciones académicas como la Universidad Autónoma de Baja California, la Facultad de Derecho de la Universidad Nacional Autónoma de México, en Universidad Anáhuac y en la Escuela Libre de Derecho

Actualmente es Comisionada del Instituto de Transparencia y Protección de Datos Personales de la Ciudad de México, y Secretaria de la Comisión de Archivos y Gestión Documental del Sistema Nacional de Transparencia.

La Ruta de la Privacidad, recorrida este 2022, es un resultado más del federalismo cooperativo que desde el Sistema Nacional de Transparencia ponemos en práctica desde hace tiempo. Es fruto de la colaboración entre Comisionada Josefina Román Vergara, desde la coordinación de la protección de datos personales en el INAI; y de Arístides Rodrigo Guerrero en la coordinación de la Comisión de Protección de Datos Personales del SNT. Sin ellos, este proyecto no habría visto la luz.

Como coordinadora del área de protección de datos personales del INFO CDMX, fue un honor formar parte del arranque de la Ruta con el evento en el marco del Día Internacional de la Protección de Datos Personales que denominamos «Fortalecimiento institucional de la protección de los datos personales: de los estándares internacionales al ámbito local», en coordinación con el INAI y la Comisión de Protección de Datos Personales del SNT, en las instalaciones de la Facultad de Derecho de la UNAM. Además de que el mismo nos brindó mayor enriquecimiento a la experiencia local, con la participación de expertos nacionales e internacionales.

El contexto de este arranque de la Ruta fue simbólico, durante una fecha conmemorativa que tiene su origen en la firma del *Convenio 108* del Consejo de Europa en 1981, por lo que cada 28 de enero lo conmemoramos en cada rincón del planeta.

Si bien el tema general de esta primera Ruta de la Privacidad fue la Inteligencia Artificial, en este corte de listón desde la Ciudad de México, de manera específica nos enfocamos en temas prácticos de interés para las instituciones públicas que forman parte del padrón de sujetos obligados por la Ley local.

El gran recibimiento por parte de la audiencia lo respalda, pues hubo más de mil personas conectadas durante los dos días en los que se discutieron temas como la protección de datos personales por defecto y por diseño; el derecho a la Portabilidad; acciones preventivas: buenas prácticas y evaluaciones de impacto; Sistemas de gestión para la protección de datos personales: medidas y documentos de seguridad; Compliance como herramienta para un tratamiento efectivo de datos personales; Transparencia y documentación del tratamiento de datos personales en las instituciones públicas: Sistemas de Datos Personales y Registro de Sistema de Datos Personales.

Todo ello con el objetivo de generar y reforzar los conocimientos y capacidades necesarias respecto del fortalecimiento institucional en la materia para los sujetos obligados de la capital. Por lo que también se contó con la presentación de un Cumplímetro sobre la protección de datos personales, herramienta que permite realizar un autodiagnóstico no

vinculante y anónimo, que sirvió para conocer el grado de cumplimiento con la *Norma de Datos Personales en la Ciudad de México*.

La implementación de esta Ruta resulta más que pertinente pues, de conformidad con datos de Fortinet, durante el primer semestre de 2022 México fue blanco de 85 millones de intentos de ciberataques, lo que hace que la socialización de información respecto de la protección de la información personal, tanto por parte del sector público como privado, refuerce los conocimientos y medidas a implementar por parte de las instituciones responsables de su resguardo.

Temas como la generación de las tecnologías de la información y la comunicación, así como de la protección de datos desde el diseño de cada una de las herramientas mencionadas se enfocan a que desde el inicio de su concepción se tome en cuenta la privacidad de los usuarios, generando confianza hacia las empresas e instituciones, quienes a través de códigos de buenas prácticas y con el liderazgo de un experto en la materia cumplan con las obligaciones que por ley se confieren.

Estas acciones realizadas desde un inicio en los sistemas ya existentes y a implementar donde se contenga la información de las personas titulares es ideal para seguir avanzando hacia un futuro en el que tecnología como la inteligencia artificial, el internet de las cosas o la lectura de rostros sean cada vez menos invasivas y más respetuosas de nuestros derechos humanos. Sentar las bases para que esto sea posible es nuestra función y proyectos como la Ruta de la Privacidad resultan una gran oportunidad para materializarlo. Con ello, hagamos lo que nos corresponde.

# LA RUTA DE LA PRIVACIDAD EN ZACATECAS

FABIOLA GILDA TORRES RODRÍGUEZ

*Comisionada Presidenta del IZAI*

Es licenciada en Derecho por la Universidad Autónoma de Zacatecas y Notaria Pública del Estado de Zacatecas (con licencia) desde 2004 con sede en Guadalupe, Zacatecas, y donde actuó como presidenta del Colegio de Notarios de 2014 a 2017.

Se desempeñó en la H. Cámara de Senadores como Secretaria Técnica de la Comisión de Asuntos del Pacto Federal; y en la H. Cámara de Diputados como asesora de la vicecoordinación de trabajo en comisiones.

Fue directora del Servicio Estatal del Empleo de Gobierno del Estado, así como Secretaria General de Gobierno del Estado de Zacatecas de 2016 a 2018.

Desde mayo de 2019 se desempeña como Comisionada del IZAI. En noviembre de 2020 fue reelecta Secretaria Técnica de la Comisión de Rendición de Cuentas del SNT. El 26 de febrero de 2021 fue electa Comisionada Presidenta del IZAI. En noviembre de 2021 fue electa coordinadora de la Comisión de Rendición de Cuentas del SNT.

Zacatecas formó parte de esta iniciativa de socialización, con el fin de robustecer las prácticas y las normativas del derecho a la protección de datos personales, y la privacidad en América Latina y en México.

Siendo evidente la necesidad de analizar el panorama actual para plantear las nuevas políticas públicas en pro de la privacidad, veremos cuáles son los retos que existen en materia de protección de datos personales y los avances que como país y como nación hemos alcanzado en el cumplimiento de este mandato constitucional.

La protección de los datos personales debe considerarse un asunto

prioritario. Según datos del Banco de México, nuestro país ocupa el octavo lugar a nivel mundial en robo de datos personales, lo que refleja que la falta de una cultura de la protección de información de carácter personal continúa siendo un reto, así como el fortalecimiento de las legislaciones y normatividades nacionales e internacionales. Es importante concientizar a la población sobre el cuidado y la protección de sus datos personales.

Desde el IZAI, en conjunto con varias instituciones, hemos emprendido la tarea de plantar semillas para tener en Zacatecas una fuerte cultura de la protección de datos personales en varias escuelas que nos han hecho el favor de abrir sus puertas.

Esta experiencia, quiero compartirles, ha sido enriquecedora: nos ha dado la oportunidad de tener retroalimentación directa de nuestros niños y jóvenes. Con ello nos damos cuenta de los riesgos que enfrentan al convivir en la cotidianidad con varias pantallas. Tratamente comprobamos que hay que reforzar el conocimiento, pero que también muchos de ellos ya implementan acciones que les permiten cuidar su privacidad, en esta nueva realidad digitalizada.

Mucho es el trabajo en conjunto que tenemos que realizar para seguir impulsando la Protección de Datos Personales. Por eso agradezco a todos y cada uno de ustedes, grandes aliados y amigos del IZAI.

# PRINCIPALES RIESGOS PARA LA PRIVACIDAD Y PROTECCIÓN DE DATOS DEL INTERNET DE LAS COSAS

FRANCISCO REYNALDO GUAJARDO MARTÍNEZ

*Comisionado Vocal de COTAI*

Consejero del Instituto Estatal Transparencia, Acceso a la Información y Protección de Datos Personales desde diciembre de 2018. Inició laboralmente en el H. Congreso del Estado de Nuevo León, continuando en el Instituto Estatal Transparencia, Acceso a la Información y Protección de Datos Personales como Secretario de Acuerdos y Proyectos, Director de Asuntos Jurídicos, Secretario Técnico y Secretario Ejecutivo.

Su formación académica es en Maestría en Métodos Alternos de Solución de Conflictos y Licenciado en Derecho y Ciencias Sociales, en la Universidad Autónoma de Nuevo León. Diplomado en Delegado de Protección de Datos Personales, Derecho Procesal Constitucional, Seminario de Acceso a la Información y Transparencia Judicial, Protección de Datos Personales y Curso de Posgrado sobre Protección de Datos Personales, entre otros.

Catedrático, Expositor, Conferencista, Capacitador y Moderador. Realizó estudio y elaboración de proyecto de dictamen para la creación de la *Ley de Métodos Alternos para la Solución de Conflictos en Nuevo León*.

En el marco de la Ruta de la Privacidad, iniciado en enero de 2022, por el INAI y la Comisión de Protección de Datos Personales del SNT, con los Organismos Garantes integrantes del mismo Sistema, con la finalidad de llevar a cabo un evento conjunto en el estado de Nuevo León para sensibilizar y socializar sobre el tema de «Inteligencia Artificial: perspectivas y prospectivas desde el derecho a la protección de datos personales y la privacidad», tuve el honor de moderar la presentación del ponente, Doctor Eduardo Blasi Casagran.

Gracias a la exposición del Doctor Blasi, se abordaron diversos riesgos que existen en el manejo del internet de las cosas, esto en el marco de la protección de datos y la privacidad. Si bien, como indica el conferencista, el internet de las cosas es un concepto que es posible ubicarlo desde finales de los noventa, sin embargo, la transformación digital se aceleró en los últimos años, donde se considera que, dentro de los próximos años, todo estará conectado a internet. Un ejemplo de ello está en aparatos: desde computadoras hasta *smartphones*.

De manera tal, que el uso del internet de las cosas brinda a sus usuarios facilidades en su rutina diaria, lo que se traduce en un aumento en su bienestar y calidad de vida. Como muestra de ello, el Doctor Blasi refiere al sector médico, donde contamos con aparatos que miden nuestros signos vitales en tiempo real. Derivado de ello, se permite la observación y registro constante a personas con algún padecimiento grave, de manera que es posible prevenir alguna tragedia.

En ese mismo sentido, el internet de las cosas es implementado tanto en las ciudades inteligentes como en sectores empresariales u organismos públicos, donde uno de los retos más importantes para estas ciudades inteligentes es el tema de la protección de datos. Si bien al recabar datos es posible encontrar tratamientos que no tienen que ver con individuos como lo es en el tema del tráfico o seguridad, es necesario considerar llevar a cabo una evaluación de impacto, el cual es un análisis de aquellos elementos que conducen a un riesgo y anticiparse al mismo.

El ponente señala que es necesario considerar una serie de principios. Entre ellos menciona el principio de minimización, así como la privacidad por defecto, mismo que deberá ser un elemento fundamental: es decir, que las personas puedan elegir qué datos desean que sean públicos.

Además se señalan los riesgos que existen en la implementación del internet de las cosas en las ciudades inteligentes. Un ejemplo de ello fue la iniciativa que tuvo una localidad, donde se sugirió la comunicación de los ciudadanos a través de un grupo de WhatsApp. Si bien fueron notificados, la creación de dicho grupo no fue idónea, ya que los mismos participantes tenían acceso a datos de los demás participantes del grupo, generando así un riesgo en la información personal de los integrantes, al estar expuesto a terceros. Continuando con estas ideas, otro ejemplo en el que hace hincapié el conferenciante es el uso de datos biométricos como el reconocimiento facial, ya que éste puede generar riesgo en cuanto a nuestros datos personales clasificados como sensibles, donde es posible generar una vulneración en los ciudadanos, debido a un posible mal tratamiento.

De acuerdo con todo lo expuesto por el Doctor Blasi, es posible concluir

que, si bien el uso del internet de las cosas y el desarrollo de las ciudades inteligentes son importantes y nos llevan a una era digital, también es primordial que se implementen medidas de seguridad, así como normas que permitan la salvaguarda de nuestros datos personales.

Esto es necesario para corregir los males que puede provocar la disparidad entre el avance de la tecnología y la protección a los usuarios.

# RUTA de la PRIVACIDAD

## COMENTARIOS ADICIONALES

# LA RUTA DE LA PRIVACIDAD

EDUARDO BERTONI

*Representante de la Oficina Regional para América del Sur del Instituto Interamericano de Derechos Humanos*

*Ex director de la Agencia de Acceso a la Información Pública, Argentina*

Representante y Coordinador de la Oficina Regional para América del Sur del Instituto Interamericano de Derechos Humanos (IIDH). Ex Director de la Agencia de Acceso a la Información Pública y de la Dirección Nacional de Protección de Datos Personales, Argentina (2016-2020). Fundador del Centro de Estudios en Libertad de Expresión y Acceso a la Información (CELE) de la Facultad de Derecho de la Universidad de Palermo (2009-2016). Ex-Director Ejecutivo de Due Process of Law Foundation (DPLF), con sede en Washington D.C., hasta mayo de 2009. Entre 2002 y 2005, Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (CIDH) en la Organización de Estados Americanos (OEA).

Es una buena noticia que el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en coordinación y colaboración conjunta con los Organismos Garantes de las Entidades Federativas mexicanas y la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia, impulsen lo que dan en llamar la Ruta de la Privacidad.

Estamos en un mundo donde alguna vez nos hemos preguntado si «la privacidad ha muerto». O, sin ser tan catastróficos, dudamos sobre nuestro interés en proteger nuestra privacidad, dado que aceptamos los términos y condiciones que nos ponen e imponen los nuevos desarrollos tecnológicos, sin siquiera preguntarnos cómo esa aceptación nos afecta.

Creo que no se pueden dar respuestas simples a temas complejos. La privacidad como derecho fundamental no ha muerto, y deducir que no nos

importa ese derecho tan sólo por nuestras actitudes frente a situaciones específicas de uso de aplicaciones encierra un salto lógico inadecuado, como lo ha puesto de manifiesto el académico estadounidense Daniel Solove, en un artículo que tituló «El mito de la paradoja de la privacidad».

En otras palabras, la privacidad es un derecho humano que está muy vigente en la sociedad actual. Hecho que se refleja, por ejemplo, en el incremento de las regulaciones para proteger los datos personales en los años recientes. Pero frente al avance de tecnologías como las que nos pone a disposición lo que de manera genérica llamamos «inteligencia artificial», resulta necesario que se difundan esas regulaciones, que se difunda el contenido del derecho en todos los lugares posibles, y muy especialmente entre quienes tienen a su cargo justamente el desarrollo de esas nuevas tecnologías.

Por ello decía al comienzo que la Ruta de la Privacidad es una buena noticia, toda vez que justamente su objetivo es reflexionar sobre la protección de datos personales ante el uso de la inteligencia artificial, y concientizar a los desarrolladores de tecnologías de las implicancias que esos desarrollos puedan tener en la vulneración de derechos fundamentales.

# LA RUTA DE LA PRIVACIDAD EN AMÉRICA LATINA

PABLO PALAZZI

*Profesor de Derecho de la Universidad de San Andrés (UDESA)*
*Director Académico del Centro de Tecnología y Sociedad (CETyS)*
*de la Universidad de San Andrés*

Máster en Derecho (LL.M.) por la Fordham University School of Law (Nueva York). Socio a cargo del Departamento de Protección de Datos Personales y Ciberseguridad de Allende & Brea (Argentina). Profesor de Derecho y codirector del Centro de Estudios en Tecnología y Sociedad (CETyS), en la Universidad de San Andrés. Fue co-chair para Argentina de la IAPP, e integra el board de publicaciones de esta institución.

Ha participado en los siguientes libros: Protección de Datos. Doctrina y jurisprudencia (editor), CDYT, 2021; Fintech. Aspectos legales (coeditor, CDYT, 2019); Data Processing Agreements. Coordination, drafting & negotiation (Justin Weiss ed., IAPP, 2019); Delitos contra la intimidad informática (CDYT, 2019); Los delitos informáticos en el Código Penal (Abeledo Perrot, tercera edición, 2016); Défis du droit à la protection de la vie privée -Challenges of privacy and data protection law (coeditor, Bruylant, Bélgica, 2008); entre otros.

Ha sido destacado en los rankings de Legal 500, GDR, Who's Who Legal y Chambers and Partners en su área de experticia.

Agradezco la invitación de la agencia a cargo de protección de datos personales para colaborar en esta obra sobre la Ruta de la Privacidad. El Derecho a la Protección de los Datos Personales puede definirse como el área del Derecho que ampara los datos personales y que constituye un conjunto de reglas que guía a compañías y organizaciones estatales en el uso que se hace de la información personal; es decir, la que identifica individuos. También se ha dicho que se refiere a los estándares

a ser aplicados para el manejo de la información sobre personas, y las prácticas que deban seguirse para alcanzar y mantener esos estándares.

La Protección de Datos Personales es, entonces, la rama del Derecho que regula el uso de la información personal de individuos y empresas. Se trata de un derecho joven, con poco más de medio siglo de desarrollo, iniciándose en 1970 con la conocida ley alemana del Land de Hesse, unos meses después con la *Fair Credit Reporting Act* en los Estados Unidos y más adelante con leyes similares en el resto de Europa hasta cristalizarse en el Reglamento Europeo de Protección de Datos Personales (RGPD). Pero es un Derecho en constante desarrollo, como lo evidencian los pronunciamientos del Grupo de Trabajo sobre Protección de Datos de la Unión Europea (ahora Comité Europeo de Protección de Datos) o los congresos anuales de los comisionados de protección de datos europeos, o la cambiante regulación existente en EEUU, siempre en una lucha constante por lograr la anhelada ley federal que nunca llegará.

En América Latina, la protección de datos tuvo su desarrollo primero con el Habeas Data, instituto del Derecho Procesal Constitucional que desde una faz procesal otorga una protección al registrado al permitir un derecho de acceso y corrección de datos personales. Luego vinieron las leyes de protección de datos personales y la necesaria creación de agencias reguladoras de datos personales que tienen como cometido aplicar la ley, dictar regulaciones e imponer las sanciones del caso concreto, incluyendo también funciones educativas y de difusión de la privacidad. En este marco, la Ruta de la Privacidad es una original idea que lleva adelante las principales ideas en diferentes ámbitos y con distintos incumbentes fundamentales para el desarrollo del derecho fundamental a los datos personales.

En función del avance tecnológico actual, consideramos de relevancia institucionalizar una cruzada nacional para tomar conciencia sobre la protección de datos personales ante el uso de inteligencia artificial.

# REFLEXIÓN SOBRE EL SIGNIFICADO DE LA CAUSA DE LA RUTA DE LA PRIVACIDAD

CÉSAR MANUEL VALLARTA PAREDES

*Director General de Evaluación, Investigación y Verificación del Sector Público del INAI*

Es Licenciado y Maestro en Derecho por la Universidad Nacional Autónoma de México, con mención honorífica.

Ha sido profesor de diversas asignaturas en la Facultad de Derecho de la misma Casa de Estudios e invitado como Ponente a diversas instituciones académicas y públicas nacionales y de Buenos Aires, Argentina; Lima, Perú; y Río de Janeiro, Brasil; además de contar con diversos diplomados en materia de transparencia, acceso a la información, rendición de cuentas, ciberseguridad y protección de datos personales. Participó como autor en las obras colectivas: *Visiones contemporáneas del Derecho a la Información*, editado por la Tirant lo Blanch, la UNAM y el INAI; y *Procesos colectivos. Una visión de derecho comparado: Argentina, Colombia, Chile y México.*, de Editorial Porrúa; así como articulista en la Revista digital *México transparente*. Se ha desempeñado profesionalmente jurisdiccional, administrativo, electoral, fiscal, legislativo y de litigio; sí como en materia de transparencia, acceso a la información pública y protección de datos personales.

Desde 2014 colabora en el INAI, donde actualmente ocupa el cargo de Director General de Evaluación, Investigación y Verificación del Sector Público de la Secretaría de Protección de Datos Personales de dicho organismo garante; trinchera desde la cual ha conocido y participado en la sustanciación y resolución de diversos asuntos relevantes en materia de protección de datos personales en el sector público federal.

La Ruta de la Privacidad es una iniciativa que, liderada por los Comisionados coordinadores de la protección de datos personales en el Instituto, Dra. Josefina Román Vergara y Dr. Francisco Javier Acuña Llamas, ha logrado concientizar a un importante número de personas en todas las latitudes del país sobre la importancia del derecho fundamental a la protección de los datos personales. En esta ocasión, desde un enfoque de actualidad: el uso de la inteligencia artificial y el desarrollo de las nuevas tecnologías, con el objetivo de prospectar su impacto y su interrelación entre los desarrolladores de esos avances de la ciencia y de la técnica, los responsables del tratamiento de los datos personales (sujetos obligados) y las personas titulares que usan estos desarrollos tecnológicos y se encuentran inmersos en el dinamismo virtual (niñas, niños, adolescentes, personas adultas y de la tercera edad).

He advertido que, en el lanzamiento de estas acciones coordinadas, se han considerado para el diseño de los contenidos desarrollados durante las jornadas las diferentes asimetrías de acceso a la tecnología y la brecha digital en su uso. La realidad de los usos inadecuados y las malas prácticas e inclusive los hechos delictivos que se cometen alrededor del abuso de la información privada confiada por las personas.

La aspiración de lograr consolidar un compromiso de desarrollo seguro y justo de la inteligencia artificial y de las nuevas tecnologías, con un equilibrio interdisciplinario, considerando el marco normativo existente, potencializando el derecho fundamental a la protección de los datos personales; pero, sobre todo, poniendo como centro de atención al titular de los datos personales bajo los principios del humanismo digital es un gran aliciente para quienes defendemos los beneficios de la libre autodeterminación informativa y la adecuada seguridad de la información en posesión de sujetos obligados y regulados.

Finalmente, considero que este esfuerzo es un gran acierto que ha dejado una clara estela de conocimientos y nuevas habilidades en la ciudadanía que favorecen el debate público, además de la discusión al seno de quienes integran el Sistema Nacional de Transparencia para lograr homogeneizar las prioridades en que habrán de afrontarse los retos para garantizar el ejercicio pleno de la protección de datos personales en México. La visita a los diversos estados de la República por donde se ha encaminado esta Ruta de la Privacidad habrá de ser constante y cada vez más amplia.

# LA PROTECCIÓN DE DATOS PERSONALES: UN PROBLEMA CLÁSICO FRENTE A RETOS ACTUALES

GABRIEL SANTIAGO LÓPEZ

*Jefe de Ponencia de la Comisionada Presidenta del INAI, Blanca Lilia Ibarra Becerra*

Estudió la Licenciatura y la Maestría en Derecho, en la Facultad de Derecho de la Universidad Nacional Autónoma de México. Además, cursó un Máster en Derechos Humanos, Estado de Derecho y Democracia en Iberoamérica, en la Universidad de Alcalá de Henares.

Labora en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, como Jefe de Ponencia de la Comisionada Presidenta Blanca Lilia Ibarra Cadena, donde fue Secretario de Acuerdos y Ponencia de Acceso a la Información. Es autor de *La voz Legitimación activa*, en el *Diccionario de Derecho a la Información*; coautor del libro *Herramientas para el ejercicio periodístico* y del estudio *La Suprema Corte de Justicia de la Nación y la causa de pedir*. Además, autor del capítulo *Garantías del derecho humano de acceso a la información pública en México: los medios de defensa establecidos en la* LGTAIP, del libro *Reflexiones contemporáneas de los Derechos Humanos*.

La discusión sobre la protección de los datos personales da continuidad a uno de los problemas clásicos del pensamiento social: cómo proteger al individuo de las amenazas del entorno. Esta preocupación recurrente ha evolucionado a lo largo de la historia. Primero, en el Estado moderno, la noción de protección se limitaba a la responsabilidad de los soberanos de salvaguardar las tierras y personas de amenazas extranjeras. Luego, con la llegada del Estado liberal, la idea de protección aumentó para abarcar también la defensa respecto de las fuerzas estatales internas y de los conciudadanos. Con ello nacieron los

derechos individuales y los límites a la autoridad. Más tarde, el derecho a la protección volvió a ampliarse, pues se reconoció que, además de velar por los elementos materiales de las personas, debían considerarse sus posesiones inmateriales, como sus creencias, honor, intimidad y dignidad (Brandeis & Warren, 1890). Fue entonces que la privacidad e integridad humana se convirtieron en imperativos del mundo moderno, y comenzaron a emitirse normas para, por ejemplo, no ser sujetos de difamación o de exposición pública sin consentimiento.

La revolución digital impacta esta histórica búsqueda, pues nos enfrenta a desafíos como la inteligencia artificial, los metaversos o el *Big Data*, que no podrán sortearse sin discusiones con especialistas y mecanismos de colaboración con la sociedad. Estamos frente a un dilema clásico, pero ante los retos propios de un momento de innovación acelerada. Basta mencionar que el término «inteligencia artificial» surge en la década de los cincuenta (Mendoza, 2021, p.181) —hace 67 años— y que, actualmente, la inversión privada en ella oscila entre los 2,400 y los 3,200 millones de euros en Europa, y entre los 12,100 y los 18,600 millones de euros en América (Mendoza, 2021, p.183).

Nuestros datos personales fluyen con una velocidad inusitada en el entorno digital. Su apoderamiento y uso ilegal puede afectar nuestro patrimonio, por ejemplo, a través del robo de identidad; pero, incluso, puede dañar nuestra seguridad, pues facilita delitos como la extorsión o el secuestro.

En ese contexto, en aras de dimensionar las problemáticas que enfrenta nuestra intimidad y los retos en materia de protección de datos personales, se gestó la Ruta de la Privacidad, para que mayores sectores de la población conozcan las amenazas existentes, cómo afectan su vida cotidiana y para consolidar una cultura de la protección de los datos personales.

# LA PRIVACIDAD EN MÉXICO: UN DILEMA DE ORIGEN

ERIKA DANIELA MONTIEL MONSALVO

*Secretaria de Acuerdos y Ponencia de Acceso a la Información en la Ponencia de la Comisionada Presidenta del INAI, Blanca Lilia Ibarra Cadena*

Es egresada de la Escuela Libre de Derecho, con mención especial por su tesis en materia de protección de datos personales. Asimismo, es maestra en Constitucional y Derechos Humanos, por la Universidad Panamericana.

Actualmente es Secretaria de Acuerdos y Ponencia de Acceso a la Información en la Ponencia de la Comisionada Presidenta Blanca Lilia Ibarra Cadena y cuenta con más de 15 años de experiencia en las materias de derechos humanos, anticorrupción, transparencia, acceso a la información y protección de datos personales.

Asimismo, forma parte del cuerpo docente del Diplomado en Protección de Datos Personales impartido por la Escuela Libre de Derecho y el INAI.

Benjamin Constant ofrece una comparativa entre dos nociones de libertad: la de los antiguos y la de los modernos. En la primera, «todas las acciones privadas están sometidas a una vigilancia severa» y el individuo, «soberano casi habitual de los asuntos públicos», es «esclavo en todas sus relaciones privadas», pues mientras que como ciudadano decide «la paz y la guerra, como particular está circunscrito, observado, reprimido en todos sus movimientos».

En cambio, en la libertad de los modernos, el Estado no puede violentar al individuo, lo cual incluye no inmiscuirse en su vida particular, por lo que puede «ir y venir a cualquier parte sin necesidad de obtener permiso, ni de dar cuenta a nadie de sus motivos o sus pasos […] deliberar sobre sus intereses, sea para llenar los días o las horas de la manera más conforme a sus inclinaciones y caprichos».

Sin embargo, esta forma de concebir la libertad no impactó de igual forma en todas las democracias occidentales. Uno de los casos más ilustra-

tivos es México: primero, porque se construyó bajo una tendencia política centralista, y bajo las reminiscencias de un régimen de partido hegemónico y presidencialista, lo que devino en la concentración del poder, al grado de configurar lo que Jorge Carpizo llamó como *facultades metaconstitucionales;* segundo, y como herencia de las culturas prehispánicas, porque nuestra nación se caracteriza por poseer costumbres y tradiciones que vindican la vida comunitaria y acentúan la resolución comunal de los problemas públicos, cualidad que hace un guiño al Ágora y noción de libertad de los antiguos.

Esto ha impactado en la legislación mexicana, pues no contamos, como sucede en otros países, con un marco normativo ni robusto ni vetusto en la materia, pues fue hasta inicios del milenio que se emitieron legislaciones al respecto.

Aun más: en México, la privacidad ha evolucionado a partir de criterios judiciales, mismos que han estirado la interpretación del artículo 16 constitucional, donde se refiere que «Nadie puede ser molestado en su persona, familia, domicilio, papeles o posesiones».

En ese contexto, impulsar una Ruta de la Privacidad es una tarea relevante, pues debemos amalgamar en la conciencia social mexicana este derecho, sobre todo ante la inalcanzable innovación tecnológica global que nos plantea retos de avanzada como la inteligencia artificial y que nos demanda posicionar el valor de la privacidad para el desarrollo de una vida en libertad.

# LA INSTITUCIONALIZACIÓN DEL DERECHO HUMANO DE PROTECCIÓN DE DATOS PERSONALES

FELIPE DE JESÚS GUTIÉRREZ RINCÓN

*Jefe de Ponencia de la Comisionada del INAI, Josefina Román Vergara*

Licenciado en Derecho por el Instituto Tecnológico de Estudios Superiores de Monterrey, cuenta con una Maestría en Administración pública y política pública por el mismo instituto; además de diversos estudios en materia de acceso a la información pública y política pública.

Se ha desempeñado en diversos cargos dentro de la administración pública municipal, siendo los más relevantes Director General de Gobierno y Director General de Desarrollo Social. Dentro del ámbito estatal, ha sido Secretario Técnico de la Comisión de Asuntos Metropolitano de la Legislatura del Estado de México. También trabajó como asesor en la Subsecretaría General de Gobierno. Dentro del ámbito federal, fue asesor del Subsecretario de Planeación, Evaluación y Desarrollo Regional de la entonces Secretaría de Desarrollo Social, entre otros cargos.

Actualmente, ocupa el cargo de Jefe de Ponencia de la Comisionada Josefina Román Vergara, dentro del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Inteligencia Artificial: perspectivas y prospectivas desde el derecho a la protección de datos personales y la privacidad se constituyó el eje rector del Día Internacional de Protección de Datos Personales 2022 y, a su vez, como directriz para la realización de la Ruta de la Privacidad.

Así, a través de la colaboración conjunta de los organismos garantes de la Ciudad de México, Estado de México, Yucatán, Hidalgo, Chihuahua, Nuevo León, Veracruz, Michoacán, Guerrero, Quintana Roo, Tlaxcala, Querétaro, Oaxaca y Zacatecas, así como con el acompañamiento del Instituto Nacional de Transparencia, Acceso a la Información y Protec-

ción de Datos Personales (INAI), esta iniciativa ha buscado promover la importancia y trascendencia institucional del derecho humano de protección de datos personales a lo largo y ancho del país.

Mediante la inclusión de expertos de talla internacional, especialistas, académicos, autoridades y personalidades del sector público y privado, se ha buscado incorporar las voces de todas y todos los actores en la garantía de ese derecho humano, para que, de este modo, estemos en posibilidad de posicionarlo como un bien necesario e indispensable en este mundo interconectado. Desde el INAI, como organismo garante de la protección de datos personales a nivel nacional, resulta de la mayor relevancia generar y participar en espacios en los cuales sea posible impulsar el cumplimiento de las leyes en materia de datos personales, a través de acciones y estrategias puntuales que faciliten la socialización y difusión del derecho; en los que también se promueva el fortalecimiento institucional de los Organismos Garantes para la protección de los datos personales y que, además, se incorporen todos los sectores y áreas relevantes donde esta prerrogativa genere un beneficio y trascendencia pública y social.

En ello se ha configurado la Ruta de la Privacidad, bajo la Coordinación de la Comisionada del INAI Josefina Román Vergara y el Coordinador de la Comisión de Protección de Datos Personales, Arístides Rodrigo Guerrero García. Esta cruzada nacional ha puesto el acento en la importancia y la necesidad de crear sinergia para garantizar la protección de datos personales, de modo que nuestras comunidades sean resilientes y, eventualmente, sean capaces de enfrentar los retos que la era digital nos pone de frente, en materia de derechos humanos.

Los foros abiertos gracias a este movimiento de institucionalización, considero, han dado como resultado que los integrantes del Sistema Nacional de Transparencia y Protección de Datos Personales den voz a todas y todos los involucrados en el ejercicio y garantía del derecho a la privacidad, la intimidad y la protección de datos; y, además, ha propiciado crear espacios para la generación de propuestas y soluciones enfocadas a satisfacer las necesidades en este mundo digitalizado.

Por último, aprovecho estas líneas para reconocer la labor de las y los integrantes de la Comisión de Protección de Datos Personales, y de los organismos garantes que se han sumado a estos espacios de conocimiento y deliberación, pues gracias a ellos, a su trabajo, compromiso y colaboración, los 15 eventos y esta obra, hoy, se han materializado y son ya una realidad.

# RUTA DE LA PRIVACIDAD, HERRAMIENTA DE DIFUSIÓN DEL DERECHO A LA PROTECCIÓN DE LOS DATOS PERSONALES

NANCY PÉREZ GUZMÁN

*Directora General de Investigación y Verificación del Sector Privado del INAI*

Es licenciada en Derecho por el Instituto Tecnológico Autónomo de México, obteniendo el grado con Mención Especial. Comenzó su trayectoria laboral en el sector público, en el área de Apoyo a ex presidentes de la Presidencia de la República, con el Licenciado Miguel de la Madrid Hurtado, desarrollando actividades de investigación jurídica, principalmente. Muestra de ello fue su colaboración en el libro *Una mirada hacia el futuro*.

Asimismo, laboró en el sector privado, en SEARS y la Asociación Nacional de Tiendas de Autoservicio y Departamentales.

En 2007, ingresó al Instituto Federal de Acceso a la Información y Protección de Datos, desempeñando diversos cargos adscritos todos a Oficinas de Comisionados. Actualmente es Directora General de Investigación y Verificación del Sector Privado.

Entre otras actividades que ha realizado, destacan diversos cursos, seminarios y foros en materia tanto de acceso a la información como de protección de datos personales.

Planear, organizar y llevar a cabo eventos en los que concurran las autoridades en la materia, así como catedráticos e investigadores, con el objeto de compartir conocimientos y experiencias, como es la Ruta de la Privacidad, refleja el enorme compromiso institucional con la sociedad en la promoción del ejercicio del derecho humano a la protección de los datos personales.

Al respecto, cabe destacar que el pasado 26 de enero inició la Ruta de la Privacidad 2022, para conmemorar el día internacional de la protección de datos personales, y con el objeto de reflexionar entre generadores de tecnología, responsables y titulares que implementan el uso de la inteligencia artificial sobre la importancia en el cuidado de los datos personales, en todo el país.

Así, durante varios meses, la Ruta de la Privacidad tuvo presencia en el territorio nacional. En la Ciudad de México, Querétaro, Michoacán, Nuevo León, Tlaxcala, Veracruz, Yucatán y Zacatecas, por mencionar algunos.

Lo anterior permitió profundizar en diversos aspectos relacionados con el uso de la inteligencia artificial, que evoluciona a pasos acelerados y permea en todo el mundo, desde los menores de edad y hasta los adultos mayores, pero abordando el tema desde la perspectiva del cuidado de los datos personales. Esto es de suma relevancia, pues es necesario que todos los actores involucrados —esto es, autoridades, responsables y sociedad en general— tengamos conocimiento en materia de privacidad y protección de los datos personales.

Asimismo, con ello se promovió una vez más, en una ardua labor de los organizadores y participantes en las diversas mesas de diálogo, el ejercicio de los derechos de acceso, rectificación, cancelación y oposición al tratamiento de datos personales.

Por tanto, con este evento se materializó el compromiso de las autoridades que participaron para con la sociedad en general, incluyendo a los generadores de tecnología, responsables y titulares que implementan el uso de la inteligencia artificial, de reflexionar en el tema de la privacidad y la protección de los datos personales.

Lo anterior, toda vez que, a través de esta valiosa herramienta de difusión, se comparten conocimientos y experiencias, y se profundiza y promueve el pleno ejercicio del derecho humano a la protección de los datos personales.

# LA PROTECCIÓN DE DATOS PERSONALES, PRIORIDAD ANTE LOS NUEVOS DESAFÍOS: LA INTELIGENCIA ARTIFICIAL

MIREYA ARTEAGA DIRZO

*Directora General de Prevención y Autorregulación del INAI*

Doctora en Ciencias Políticas y Sociales por el Colegio de Morelos, cuenta con Maestría en Derecho con Orientación en Derecho Civil y Licenciatura en Derecho por la Universidad Autónoma del Estado de Morelos. Es especialista en Gobernabilidad, Derechos Humanos y Cultura de la Paz; Responsabilidad social Empresarial y Máster en Gobernanza global y Derechos Humanos por la Universidad de Castilla-La Mancha. Durante 15 años colaboró como asesora, secretaria técnica, directora, subdirectora y encargada de la Secretaría de Servicios Legislativos y Parlamentarios del Congreso del Estado de Morelos, para después incorporarse al Instituto Morelense de Información Pública y Estadística (IMIPE), donde ha sido presidenta del Instituto de 2015 a 2017 y nuevamente en 2019, cargo con el que concluyó su ciclo en esa institución.

Ha escrito para diversas publicaciones como *Monitor democrático*, de 2013 a 2021, editadas por COPUEX, y en revistas como *IUSTITIA*, *Ética e Inclusiones*, *revista de Humanidades y Ciencias Sociales de la UNAM*. Su más reciente participación editorial es como coautora en el libro *Delito de Feminicidio, Diálogo Polisémico y su emergencia en la política criminal sistémica*, editado en Colombia en este julio de 2020, así como recientemente coeditora y articulista del libro *Mirada social del feminicidio, a través de la política criminal sistémica*, publicado por Editorial Ibáñez, de Colombia.

Fungió hasta la primera mitad de julio como Directora de Facilitación del Sector Público y actualmente se desempeña como Directora General de Prevención y Autorregulación, ambos del INAI.

Estas jornadas de trabajo multidisciplinario, tanto en el sector público como privado, nos han permitido sentar las bases para afrontar el desafío que representa garantizar el derecho humano de protección de datos personales ante la inteligencia artificial (IA).

El eje rector abordado en la Ruta de la Privacidad cobra especial relevancia debido a que nuestra vida diaria está inmersa de la utilización de esta tecnología, poniendo al filo la protección de los datos personales. Por ello, a través de estos trabajos se han cimentado bases que permiten a todos los actores involucrados enfrentar estos nuevos retos para continuar garantizando el derecho humano de protección de datos personales y de privacidad, ahora en los entornos digitales.

En este contexto, tuve el privilegio de formar parte de las jornadas de Ruta de la Privacidad, donde se generó un espacio de diálogo, conocimiento y experiencia, y en el que también se tuvo la oportunidad de presentar el trabajo y resultados de la Dirección General de Prevención y Autorregulación, la cual tengo el honor de encabezar.

En primer lugar, en la Ruta de la Privacidad se expusieron las *Recomendaciones para el tratamiento de datos personales derivado del uso de la Inteligencia Artificial*, como una herramienta práctica que permita a los responsables de los sectores privado y público corroborar, durante el desarrollo o implementación de un producto o servicio que utilice IA, si se cumple con los principios y deberes de protección de datos personales establecidos en la normativa correspondiente. Por otro lado, reconociendo la diversidad cultural y a los habitantes de las comunidades indígenas de nuestro país, en la Ruta de la Privacidad Oaxaca se tuvo la oportunidad de presentar la Guía de Protección de Datos Personales en lenguas de los pueblos originarios de México traducidas a las lenguas más importantes y habladas de nuestro país (náhuatl, tzotzil, tzeltal, maya, mixteca y zapoteca).

En ese acto, se hizo hincapié en que dicho producto editorial permitirá a uno de los sectores más vulnerables de la población, orientar y dar a conocer los derechos de las leyes aplicables en la materia de protección de datos personales, así como los diversos principios y deberes que los responsables del tratamiento deben de cumplir.

Sin duda, la protección de los datos personales es un tema que continuará en la agenda. En este contexto, es una prioridad continuar fomentando estos espacios colaborativos que nos permitan alcanzar los objetivos planteados en la Ruta de la Privacidad y, por supuesto, es un honor haber formado parte de este espacio de institucionalización del derecho humano que tutelamos en el INAI.

# REFLEXIÓN SOBRE EL SIGNIFICADO DE LA CAUSA DE LA RUTA DE LA PRIVACIDAD

LUIS RICARDO SÁNCHEZ HERNÁNDEZ

*Director General de Normatividad y Consulta del INAI*

Es maestro en Derecho de las tecnologías de información y comunicación con estudios especializados en Protección de datos digitales por parte de INFOTEC de CONACYT. Además, Licenciado en Derecho por la Facultad de Derecho de la UAEMÉX. Es catedrático en la maestría en Derecho de las tecnologías de la información y comunicación del INFOTEC, así como de licenciatura y maestría en otras universidades.

Funge como Director General de Normatividad y Consulta de la Secretaría de Protección de Datos Personales del INAI, participando en diversos grupos e iniciativas internacionales. Antes laboró como Director de Facilitación del Sector Privado. Fue Jefe de la Unidad de Planeación y Transparencia de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de México; Director de Protección de Datos Personales en el Infoem; y Jefe del Departamento de lo Contencioso del OSFEM, fungiendo como auditor líder del Sistema de Gestión de Calidad.

Hoy en día, las tecnologías han evolucionado de forma exponencial, de manera que, al hablar de sus avances, también debemos incluir en nuestras reflexiones el impacto y sus efectos en los derechos de las personas. Por ello, la Ruta de la Privacidad se convirtió en el cauce para promover y socializar las perspectivas y prospectivas desde el derecho a la protección de datos y la privacidad en torno a la inteligencia artificial. Entre los tópicos abordados, se compartieron los principales retos que se tienen en el sector público para el aprovechamiento óptimo de las tecnologías y el tratamiento seguro de datos personales, ya que, a pesar de

constituir un concepto relativamente reciente, el Gobierno Electrónico se asociaba como la gestión gubernamental a través de las tecnologías. Sin embargo, actualmente, dada la gran evolución, es necesario transitar hacia el concepto de Gobierno Digital, el que supone tanto el manejo de información, como la creación y gestión de infraestructura, el fomento de una ciudadanía digital y el mejoramiento de productos y servicios.

Esto es así puesto que los gobiernos no sólo deben proteger a sus ciudadanos de los riesgos inminentes de las nuevas tecnologías, sino también promover su uso responsable a fin de que aplicativos como *big data*, blockchain, realidad virtual y tecnologías inmersivas, internet de todo e Z puedan extender sus beneficios para las personas.

En ese sentido, se señaló que, de conformidad por lo sugerido por la Organización para la Cooperación y el Desarrollo Económicos, un modelo integral de gobierno digital comprende las siguientes dimensiones:

- Digital por diseño
- Impulsado por datos
- Gobierno como plataforma
- Abierto por defecto
- Impulsado por el usuario
- Proactividad

A este respecto, podemos afirmar que la gobernanza digital está basada en una gobernanza de datos que, a su vez, supone principalmente dos aspectos: el uso ético de los datos, y el acceso y uso de éstos. De igual forma, es imprescindible colocar a los derechos humanos en el centro del gobierno digital y de las políticas de uso de datos, a través de las siguientes acciones:

- Gestionar datos con integridad.
- Conocer y observar los arreglos gubernamentales relevantes para el acceso, el intercambio y el uso de datos confiables.
- Supervisar y mantener el control sobre las entradas de datos.
- Ser específico sobre el propósito del uso de los datos.

Por ello es importante consignar que, en la transición del gobierno electrónico al gobierno digital, resulta elemental aumentar el acceso y uso de la información, reforzar la confianza sobre el ecosistema de datos, estimular la inversión en datos, incrementar para el acceso y uso, y fomentar un acceso y uso efectivo y responsable en la sociedad, y con ello, un gobierno digital que, a través de la protección de los datos, esté centrado en el humano.

# LA RUTA DE LA PRIVACIDAD

RUBÉN TRUJILLO MONTES DE OCA

*Secretario de Acuerdos y Ponencia de Datos Personales en la Ponencia del Comisionado del INAI, Francisco Javier Acuña Llamas*

Es Licenciado en Derecho por la Universidad Nacional Autónoma de México.Cursó Diplomado en Derecho Procesal Penal en el Colegio Universitario del Distrito Federal. Laboró en diversos cargos en la Procuraduría General de Justicia del Distrito Federal, hoy Fiscalía General de Justicia de la Ciudad de México. Se ha desempeñado con diversos puestos en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Desde 2019 se desempeña como Secretario de Acuerdos y Ponencia de Datos Personales en la Ponencia del Comisionado Francisco Javier Acuña Llamas.

El uso de aplicaciones gratuitas (redes sociales) se ha convertido en un atractivo para las nuevas generaciones, las que de manera indiscriminada difunden información relacionada con los aspectos más íntimos de su vida privada, la comida que consumen, los lugares que frecuentan, los amigos con los que conviven… Toda esa información forma parte de su vida privada y, en su conjunto o por separado, los hace identificables frente a otras personas. Sin embargo, están ante los avances tecnológicos de la inteligencia artificial, utilizada como herramienta para el procesamiento acelerado de las bases de datos y registros de la información, aquélla que identifica y hace identificable a los individuos, aumenta también la transferencia y manejo de datos personales sin que exista claridad en cuanto a su objeto, uso, destino, transferencia e incluso comercialización.

Pero la importancia radica no sólo en exigir a los responsables del almacenamiento, uso y difusión de la información el cumplimiento de las disposiciones normativas en materia de protección de datos personales, sino también en generar conciencia entre los titulares de la información,

a efecto de que éstos exijan conocer los alcances en el uso de sus datos personales a través del aviso de privacidad y con ello mantener un consentimiento informado sobre las implicaciones del uso de las tecnologías de la información.

Generacionalmente son los jóvenes, e incluso los menores de edad, quienes utilizan en mayor medida las redes sociales y las aplicaciones tecnológicas como medios de interacción con otros individuos. Sin embargo, éstos pierden de vista el valor de sus datos personales frente al valor que los responsables de su manejo les dan al momento de generar ganancias a expensa de éstos.

La importancia de la Ruta de la Privacidad radica en que su objetivo es generar conciencia en los titulares respecto al uso de la inteligencia artificial que engloba el manejo acelerado de la información; una colaboración institucional como política pública rectora a nivel nacional, así como el fortalecimiento en la comunicación entre los responsables del uso de los datos personales y sus titulares.

Si bien la inteligencia artificial sobrepasa las capacidades del Estado en cuanto a su regulación y protección de la información, generar conciencia en los titulares de la información permitirá mantener a una sociedad más informada respecto de la importancia de la protección de los datos personales.

# RUTA DE LA PRIVACIDAD

ULISES RAMÍREZ GALLARDO

*Jefe de Ponencia de la Oficina del Comisionado del INAI, Francisco Javier Acuña Llamas*

Licenciado en Sociología por la Universidad Nacional Autónoma de México. Cuenta con el Título del Máster del Reglamento General de Protección de Datos Personales de la Unión Europea de la Universidad Nacional de Educación a Distancia de España.

En el Instituto de Investigaciones Jurídicas de la UNAM colaboró en el área de acceso a la información, participando en diversos proyectos como la enciclopedia de acceso a la información en México, monitoreo de gasto en el sistema electrónico de información INFOMEX, y el diseño de cuestionamientos a la *Ley de Telecomunicaciones y Radiodifusión*, entre otros.

Desde 2014 es Jefe de Ponencia en la Ponencia del Comisionado Francisco Javier Acuña Llamas, en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

La privacidad se encuentra integrada por aquella información que se considera más preciada para cada uno de los individuos que conforman una sociedad, información que no sólo nos identifica, sino que además nos permite hacernos identificables ante otros individuos.

Los avances en el uso de las tecnologías de la información y, con ello, la creciente influencia de la inteligencia artificial ha facilitado un mayor manejo, almacenamiento y uso de la información que conforma la vida privada de sus titulares. Sin embargo, ante los avances en el uso de esas herramientas tecnológicas se ha generado, a la par, la necesidad de valorar y hacer más visible la problemática que deriva del uso de nuestra información, ya que no se trata sólo de su uso y almacenamiento, sino también incluso de su difusión y comercialización.

El valor intrínseco de dicha información pasa a segundo término cuando los responsables del manejo de ésta generan una necesidad mayor en

el uso de los servicios que prestan, frente a la conciencia de los titulares, permitiendo obtener su consentimiento —sea informado o no— para el almacenamiento, uso, distribución, y comercialización de la información. Con ello se genera una mayor vulneración y una menor eficacia de los mecanismos normativos que permitan su efectiva protección.

La labor del Estado ya no sólo se ciñe a cumplir con su deber protector dentro de los parámetros con los que legalmente cuenta, sino además a avanzar en la implementación de herramientas que permitan generar conciencia en los titulares respecto del valor en el manejo y obtención de su información por parte de los responsables.

La Ruta de la Privacidad refleja cómo, de manera conjunta, instituciones, titulares y responsables pueden elevar los niveles de conciencia en el valor de la información a la que permitimos su acceso a cambio del uso de las tecnologías de la información y los servicios que éstas prestan y con ello cubrir nuestras necesidades, sin perder de vista el valor que tiene cada dato, registro, e información que, aunque sea mínima, genera ganancias con su almacenamiento y distribución a los responsables que la poseen.

Concientizar a la población sobre el valor de la información será la única manera de proteger a cada individuo de posibles vulneraciones a su vida privada, lo cual, aun y cuando no sea tangible, se convierte en un ámbito que permite el libre desarrollo de cada persona dentro de una sociedad, ya que la hace única.

# APORTE SOCIAL Y JURÍDICO DE LA CAUSA DE LA RUTA DE LA PRIVACIDAD

MARTHA JUDITH SÁNCHEZ ÁLVAREZ

*Secretaria de Acuerdos y Ponencia de Acceso a la Información de la Ponencia de la Comisionada del INAI, Josefina Román Vergara*

Con 10 años de experiencia en la materia, se ha desempeñado en diversos cargos en el ámbito nacional dentro del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, como Secretaria de Acuerdos y Ponencia de Datos Personales y Subdirectora de Resoluciones de Protección de Datos.

En el ámbito local se desempeñó como Responsable de la Unidad de Protección de Datos Personales en el Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del estado de Colima. Es Licenciada en Derecho por la Universidad de Colima y cuenta con diversos cursos en materia de acceso a la información pública, archivos, gobierno abierto y protección de datos personales.

La dignidad humana, si bien no está definida textualmente en alguna norma jurídica, puede considerarse como aquélla que debe protegerse y reconocerse para todos los individuos por igual sin distinción alguna, por el solo hecho de ser personas.[71] Sobre esta base se originan el cúmulo de derechos y libertades que le permiten al individuo desenvolverse y desarrollarse como lo desea dentro de la sociedad. Por ello, las autoridades deben respetarla y garantizarla en todo momento.

Los derechos de privacidad y protección de datos personales entran

[71] Lefranc Weegan, Federico, *Holocausto y Dignidad Significado y fin de la invocación a la dignidad humana en el Preámbulo de la Declaración Universal de Derechos Humanos*, México, UBIJUS Editorial p. 101, http://movaprinting.com/HOLOCAUSTO_Y_DIGNIDAD.pdf, consultado el 22 de enero de 2022.

en la categoría de amplia defensa, al estar directamente vinculados con la dignidad humana y al ser sumamente necesarios para el desarrollo de la personalidad, pues le otorgan facultades para realizarse dentro de la sociedad porque la privacidad otorga la potestad a su titular de decidir qué información de su vida privada hace pública o comparte con la sociedad y cuál restringe. Incluso, desde la óptica de la intimidad, pueden contemplarse aspectos más personales y sensibles del individuo. Esto mientras que la protección de datos personales otorga a la persona la facultad de decidir sobre el control y flujo de su información personal, e impone a terceros deberes y obligaciones respecto de los datos que han sido confiados.

En ese sentido, el objetivo principal de este proyecto denominado Ruta de la Privacidad es difundir la importancia de la privacidad y la protección de datos personales dentro del ámbito digital. Por ello ha sido medular para incrementar el conocimiento que la población tiene sobre estos derechos y, a su vez, hacer efectivos estos elementos constitutivos de la personalidad. sAdicionalmente, dicha cruzada de institucionalización funge un papel fundamental para el desarrollo de la cultura de la protección de los datos personales en México; la cual, de acuerdo con Aristeo García González, es «[…] el conjunto de conocimientos, opiniones, prácticas o conductas que una persona tiene sobre el tratamiento y la protección de su información personal (datos personales)».[72]

Así pues, la Ruta de la Privacidad, tras su paso por 14 estados de la República Mexicana, ha sido, sin duda, un medio pertinente con el que se permite el aumento de conocimientos por parte de la sociedad en relación con los datos personales, su relevancia, los principios y deberes por los que se rige su tratamiento, el uso adecuado que puede darse sobre de ellos y los derechos vinculados que permiten garantizar el derecho humano, ante la inteligencia artificial o también conocida como Quinta Revolución Industrial. En suma, derivado de sus amplios alcances en los sectores públicos, privados y académicos, este espacio de conocimiento y diálogo brinda la oportunidad del incremento en los niveles de garantía de los derechos humanos que en el INAI tutelamos. Enhorabuena por este aporte a la cultura de la privacidad y la protección de datos personales.

[72] García González, Aristeo, «Hacia una cultura en materia de protección de datos personales», *Hechos y Derechos*, núm. 14, https://revistas.juridicas.unam.mx/index.php/hechos-y-derechos/article/view/6816/8752, consultado el 7 de abril de 2022.

# LA IMPORTANCIA DE LA RUTA DE LA PRIVACIDAD

LAURA PERLA GONZÁLEZ DÁVILA

*Jefa de Ponencia de la Oficina del Comisionado del INAI, Adrián Alcalá Méndez*

Es Abogada en Derecho y Politóloga por la Universidad Nacional Autónoma de México. Cuenta con estudios de Posgrado en Derecho Administrativo en la Facultad de Derecho de la misma Universidad y de Maestría en Transparencia y Protección de Datos Personales en la Universidad de Guadalajara.

Ha impartido diversos cursos especializados en materia de transparencia y acceso a la información, principalmente a los sujetos obligados del ámbito federal. Obtuvo la certificación de instructores que expide la Secretaría de Educación Pública.

Desde 2007 labora en el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (antes IFAI), ocupando diversos puestos. También ha formado parte de los grupos de trabajo de diversos comités, como el de Criterios del INAI.

Actualmente es normal que gran parte de la vida de una persona se desarrolle dentro del mundo virtual. A través de una pantalla, móvil o tableta, y con las tecnologías de la información, se realizan trámites, servicios, pagos, compras, se busca entretenimiento y se lleva a cabo la vida escolar y laboral. Sin embargo, toda la comodidad y practicidad que esto puede tener implica un costo, el necesario intercambio de nuestros datos. Ello nos coloca en un umbral de riesgos que es necesario conocer.

Recordemos que la protección de datos personales es un derecho humano consagrado en el artículo 16 de nuestra *Constitución Política*, y ello brinda a las personas el control sobre su información personal y nos faculta

para decidir quién, cómo, cuándo y hasta qué punto ésta se puede utilizar.

Pero ¿cuánto en realidad sabemos sobre la importancia de nuestra información para las empresas? ¿Cuánto valoramos el cuidado de nuestros datos? ¿Hasta dónde somos conscientes de que el primer paso para minimizar los riesgos está en nosotros? ¿Sabemos ante quién acudir cuando necesitamos ejercer alguno de nuestros derechos ARCO?

Para ello, el INAI, junto con los organismos garantes que integran el SNT, en ejercicio de sus atribuciones emprendieron una cruzada nacional denominada Ruta de la Privacidad, la cual tiene como fin el acercar la protección de los datos personales a todos y todas, de socializar y reflexionar sobre la privacidad y su protección, de llegar a más personas para que usen la tecnología de manera responsable al intercambiar su información.

Así, Comisionadas y Comisionados, especialistas, autoridades, sujetos obligados, responsables, academia y sociedad civil han unido sus voces para sumar esfuerzos y exponer, en un ejercicio de participación y desde diferentes perspectivas, mediante distintas actividades de promoción, la importancia de la protección de datos, hacer propuestas, definir rutas, acciones y exponer retos que impulsen una necesaria cultura de la protección de datos de la sociedad.

Así pues, la Ruta de la Privacidad se coloca como un ejercicio de colaboración innovador, que requiere constante actualización, a fin de que gradualmente se transmitan conocimientos, habilidades y herramientas como ruta clave que permita la construcción de capacidades humanas e institucionales, en pro del ejercicio de la protección de datos, para que se puedan fabricar, en nuestro país, mejores circunstancias en beneficio del derecho humano de los datos personales.

# REFLEXIÓN SOBRE EL SIGNIFICADO DE LA CAUSA DE LA RUTA DE LA PRIVACIDAD

NAYELI AGUAYO GARCÍA

*Secretaria de Acuerdos y Ponencia de Datos Personales*
*Oficina del Comisionado del INAI, Adrián Alcalá Méndez*

Es Licenciada en Derecho por la Universidad Americana. Maestra en Derecho por la Universidad Nacional Autónoma de México. Ha participado en Cursos, Seminarios y Talleres de Derecho Administrativo; Administración Pública; Argumentación Jurídica; entre otros. Ha impartido diversos cursos, talleres y seminarios en temas relacionados con los derechos de acceso a la información y protección de datos personales. Coautora en el libro *Visiones Contemporáneas del Derecho a la Información.*

Cuenta con 18 años de experiencia profesional en el INAI: Jefa de Departamento de Análisis, Ponencia del ex Comisionado Horacio Aguilar Álvarez de Alba; Subdirectora de Análisis y Directora de Análisis y Proyectos de Acceso a la Información, Ponencia de la ex Comisionada Jacqueline Peschard Mariscal; Secretaria de Acuerdos y Ponencia de Acceso a la Información, Ponencia de la ex Comisionada María Patricia Kurczyn Villalobos. Actualmente es Secretaria de Acuerdos y Ponencia de Datos Personales, en la Ponencia del Comisionado Adrián Alcalá Méndez.

La inteligencia artificial ha servido para remediar habilidades cognitivas, solucionar problemas mediante la aplicación de la lógica y la identificación de patrones: los sistemas informáticos que basan su funcionalidad en la implementación de algoritmos que ponen en marcha el *aprendizaje de máquinas* para llevar a cabo tareas que, normalmente, son realizadas por los humanos al requerir de inteligencia. Éstos han evolucionado con mayor rapidez que las normas que los regulan, sobre todo, porque su fuente primordial descansa en la utilización de *big data*,

al procesar una gran cantidad de datos a mayor velocidad, lo que conlleva el tratamiento de datos personales a gran escala.

Esto genera, en principio, la difusión de información en la era de las ideas y, por tanto, beneficia el derecho a la información en su expresión más amplia, piedra angular para la vida democrática, porque favorece el desarrollo de conciencias críticas. El uso de estas tecnologías hace necesario vislumbrar mecanismos de responsabilidad y control para la protección de datos personales y los *derechos de la personalidad* (privacidad, honor e intimidad).

La Ruta de la Privacidad impulsada por el INAI, en conjunto con los Organismos Garantes y el Sistema Nacional de Transparencia, dirige sus esfuerzos a difundir y socializar la necesidad de implementar un estándar de cuidado de los principios y deberes que rigen la protección de datos personales para ser aplicado por los sujetos inmersos en la ejecución de la inteligencia artificial; es decir, no sólo por los generadores de la tecnología, sino también por los responsables del tratamiento de los datos personales y de sus propios titulares al ejercer su derecho a la autodeterminación informativa.

Por lo anterior, deben difundirse los esfuerzos que los Organismos Garantes, y en específico el INAI, han realizado para tutelar la protección del derecho de las personas respecto al tratamiento automatizado de datos de carácter personal, en concordancia con el *Convenio 108* firmado y ratificado por México. Estas autoridades han percibido con claridad que no es viable descansar la obligación de proteger los datos personales de los usuarios en la ética de los desarrolladores de tecnología, ya que sería tanto como renunciar a la encomienda Constitucional que les fue asignada.

# REFLEXIONES SOBRE LA RUTA DE LA PRIVACIDAD

MIGUEL NOVOA GÓMEZ

*Director General de Protección de Derechos y Sanción del INAI*

Es Licenciado en Derecho por el Instituto Tecnológico Autónomo de México, y cuenta con una Maestría en Gobierno y Políticas Públicas por la Universidad Panamericana.

Obtuvo Diploma de Especialidad en Derecho Constitucional y Ciencias Políticas por el Centro de Estudios Políticos y Constitucionales, en Madrid España; así como el grado de Máster Universitario en Derecho de la Unión Europea, por la Universidad Complutense de Madrid.

Se ha desempeñado como Abogado General y Comisionado para la Transparencia de la Secretaría de Desarrollo Social; Titular del Órgano Interno de Control de la Secretaría de Turismo; y Subdirector General de Contratos y Servicios de la Suprema Corte de Justicia de la Nación, entre otros encargos.

Desde 2017 es servidor público del INAI, desempeñándose como Director General de Asuntos Jurídicos y Director General de Enlace con Partidos Políticos, Organismos Electorales y Descentralizados.

Actualmente es el Titular de la Dirección General de Protección de Derechos y Sanción.

Inmersos en la llamada era digital, somos los protagonistas del momento más tecnológico en la historia de la humanidad. Nuestra realidad gira en torno a las nuevas tecnologías y al internet, cuyo manejo ha transformado nuestra realidad en un mundo globalizado e interconectado. Estos cambios profundos suponen una verdadera revolución tecnológica que está formando nuevos hábitos, costumbres, e incluso el lenguaje en las personas. En este contexto, cabe hacer especial mención de la llamada inteligencia artificial como una nueva tecnología que genera grandes

expectativas sobre su impacto en el ámbito económico, científico y social.

Más o menos definida como el conjunto de técnicas computacionales y de procesos con el propósito de mejorar la capacidad de las máquinas para realizar un gran volumen de operaciones, la inteligencia artificial se vincula con el uso de algoritmos, y, sobre todo, de una gran cantidad de datos personales

En consecuencia, surge la preocupación de que el uso de información de carácter personal para el desarrollo de la inteligencia artificial sea respetuoso de los derechos humanos y de las leyes aplicables al tratamiento de datos personales. Debido a ello. los Gobiernos, la academia, la industria, las organizaciones de la sociedad civil y, por supuesto, las agencias o autoridades en materia de protección de datos personales, como es el caso del INAI, tienen en su agenda abordar de manera profunda este tema.

Una muestra visible de ello, en todo el territorio nacional, es la Ruta de la Privacidad. Es una iniciativa impulsada por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y el Sistema Nacional de Transparencia (SNT) para difundir entre la población la importancia del derecho a la protección de datos y la privacidad en el entorno digital.

Estoy seguro de que esta iniciativa, a la cual estamos llamados a fortalecer, en conjunto con los esfuerzos individuales de cada uno de nosotros, ya sea desde el ejercicio público en la materia, pero también desde nuestro ámbito personal, conseguirá generar consciencia en la población respecto de la importancia de cuidar nuestros datos personales en un complejo y retador entorno tecnológico.

# REFLEXIONES EN TORNO A LA RUTA DE LA PRIVACIDAD

VITELIO RUIZ BERNAL

*Director de Sustanciación de Protección de Derechos del INAI*

Licenciado en Derecho por la Universidad Panamericana, campus Ciudad de México. Cuenta con el Título del Máster del Reglamento General de Protección de Datos Personales de la Unión Europea de la Universidad Nacional de Educación a Distancia de España y cursó el Diplomado en Privacidad, Regulación y Gobernanza de Datos impartido por el Centro de Investigación y Docencia Económicas (2018).

Actualmente se desempeña como Director de Sustanciación de Protección de Derechos del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI).

Desde el reconocimiento constitucional del derecho a la protección de datos personales mediante la reforma del artículo 16 a la Carta Magna el 1 de junio de 2009, y la posterior aprobación y publicación de la *Ley Federal de Protección de Datos Personales en Posesión de los Particulares* en julio de 2010, deviene el mandato del Estado mexicano a promover y difundir este derecho humano, situación que recayó en la esfera de competencias del entonces Instituto Federal de Acceso a la Información (IFAI), ahora Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI). Finalmente, mediante la expedición de la *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados* en enero de 2017, se completa nuestro marco normativo de protección de datos personales, dotando de competencias a los órganos garantes locales respecto del tratamiento de datos personales que realizan los sujetos obligados de su jurisdicción.

El camino de la difusión y promoción del derecho a la protección de datos desde el órgano garante a nivel nacional no ha sido fácil por diversos

motivos, dentro de los que encontramos la brecha digital, el acceso inequitativo a tecnologías de la información, la falta de conocimiento sobre la existencia del derecho, entre otros. En ese sentido, se han creado desde el INAI, y ahora en conjunto con los órganos garante locales, iniciativas, materiales, herramientas y recursos que permiten tanto a particulares como a sujetos obligados implementar y dar cumplimiento a las normativas de los datos personales.

Dentro de estos esfuerzos nace la iniciativa de la Ruta de la Privacidad como el primer esfuerzo coordinado entre los órganos garantes locales y el garante nacional para difundir y promover este derecho a lo largo y ancho del territorio nacional, tanto para particulares como para sujetos obligados.

Los objetivos de esta iniciativa son posicionar y concientizar a la ciudadanía el tema de los datos personales en México. Este año se dio especial relevancia a la inteligencia artificial y las implicaciones que tiene su uso en la protección de datos personales. Sin duda, el advenimiento de estas nuevas tecnologías puede tener grandes beneficios para la humanidad, pero su uso desmedido también implica riesgos graves a la protección de datos personales, entre otros derechos humanos.

# RUTA DE LA PRIVACIDAD

ROGELIO ROBLES LÓPEZ

*Investigador de la Universidad Nacional Autónoma de México*

La Ruta de la Privacidad representa un esfuerzo interinstitucional —encabezado por el INAI— de los diversos organismos garantes y de sus homólogos en las entidades federativas, con la participación de la Comisión de Protección de Datos Personales del Sistema Nacional de Transparencia, a fin de visibilizar la importancia de la protección de los datos personales y la privacidad. Bajo este contexto, esta ruta representa un foro itinerante en el que participan ponentes especializados en la materia del sector público, académico y social, tanto internacionales como nacionales, con la finalidad de sensibilizar a la sociedad respecto de la relación que tienen los datos personales y la privacidad con otros derechos humanos fundamentales en una era tecnológica.

Entre los puntos que se ha abordado se encuentran los estándares internacionales en la materia, la ciberseguridad, la inteligencia artificial, o los derechos de las personas en situación vulnerable, lo anterior, desde su relación con la protección de los datos personales.

En este sentido, cabe recordar que ante el acelerado desarrollo de la tecnología las personas pueden verse beneficiadas por su uso, el cual facilita la vida diaria en diversos campos, por ejemplo: salud, seguridad, educación, entretenimiento. Sin embargo, también trae aparejada una serie de peligros, como lo es el robo de identidad, ciberacoso, mal tratamiento de los datos personales, virus, entre otros.

Por tal motivo, es indispensable celebrar estos foros de reflexión donde se brinde a la sociedad un espacio para conocer y debatir los beneficios y peligros que representa la era digital, así como los procedimientos e instituciones encargadas de garantizar su derecho a la protección de sus datos personales, logrando una sinergia entre el sector público, academia y sociedad para beneficio de todas y todos.

# CARTA DE DERECHOS DE LA PERSONA DIGITAL. CÓDIGO DE BUENAS PRÁCTICAS

ARÍSTIDES RODRIGO GUERRERO GARCÍA

*Coordinador de la Comisión de Protección de Datos Personales*

JOSEFINA ROMÁN VERGARA

*Comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales*

Las Tecnologías de la Información y la Comunicación (TIC), en tiempos recientes, se han constituido como un instrumento eficaz para el progreso humano, y a su vez, contribuyen en gran medida a la promoción y protección de los derechos humanos. Para lograr tales propósitos, es sabido que generan volumen de datos. Éstos son el insumo fundamental que les permite crear un entorno digital en el que sea posible realizar actividades de vigilancia, análisis y predicción, e incluso manipular el comportamiento de la población en una medida sin precedentes.

Es tal el auge del desarrollo de la tecnología y, en particular, el de inteligencia artificial, que éste cuenta en la actualidad con previsiones de crecimiento anual del 27 % entre 2020-2025, según datos manejados por la consultora especializada IDC.

Sin duda, estos avances tecnológicos plantean riesgos muy considerables para la dignidad humana, la autonomía y la vida privada. Por ello, la Comisión de Datos Personales del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, a través de sus integrantes, manifestó en reiteradas ocasiones su interés de generar acciones que reflejen la importancia creciente del ejercicio de los derechos humanos y fundamentales en la era digital, sobre todo de

aquéllos relacionados con la protección de datos personales, la libertad de expresión y otras libertades asociadas al entorno digital.

A través de la suma del talento y conocimiento de expertos y especialistas integrantes del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) y los organismos garantes de las entidades federativas, tuvieron lugar los trabajos de investigación y redacción de un documento con un lenguaje claro y cercano a la ciudadanía que vio la luz en noviembre de 2022, cuando la Comisión referida aprobó la «Carta de Derechos de la Persona Digital. Código de buenas prácticas».

Así, luego del esfuerzo conjunto de las y los integrantes de la Comisión, se generó un instrumento que tiene como objetivo central difundir los derechos que tiene cualquier persona usuaria de Internet, así como las obligaciones a cargo de diversas instituciones para garantizar el ejercicio de estos derechos y, de este modo, coadyuvar a que las personas usuarias de las TIC convivan de manera armónica y con pleno respeto a su dignidad e integridad dentro del mundo digital.

De modo paralelo, se espera que su contenido se retome durante la elaboración de políticas públicas y leyes que tengan por finalidad lograr la protección de los derechos en el mundo digital, y que, además, sea marco de referencia para la adecuación normativa que se espera México emprenda, de cara a la posible adhesión al convenio 108+.

La *Carta de Derechos de la Persona Digital*, disponible para el público, busca introducir a la persona lectora a la realidad actual del mundo digital y, a través de ocho capítulos (que se refieren de manera específica a los derechos de la persona digital más importantes, tomando en consideración al menos 28 principios que se describen de manera sucinta para fines de contexto), promover el respeto, la protección y la garantía de los derechos humanos en el entorno digital.

En cuanto a los derechos en específico, éstos se encuentran los asociados a la igualdad digital: el acceso universal a Internet, la no discriminación, la educación digital y el derecho a la neutralidad de Internet. Asimismo, se hace referencia a las libertades en el entorno digital (derecho a la identidad, a la pseudonimidad, a no ser localizada ni perfilada, libertad de expresión y acceso a la información, derecho a la herencia digital, al ocio en el ciberespacio y al uso de redes sociales).

En el mismo sentido, se hace alusión a los derechos relacionados con la seguridad de las personas usuarias (derecho a la privacidad y a la protección de datos personales, derecho a la transmisión, recepción y tratamiento seguro de información, derecho a la portabilidad y a la ciberseguridad),

con la participación, la democracia y el buen gobierno digital (derecho a recibir información veraz y a la participación ciudadana por medios digitales, derechos digitales frente a la Administración Pública y derecho de reunión, asociación y participación), y los derechos laborales (teletrabajo, desconexión digital y a la privacidad en el uso de cámaras de videovigilancia al interior de lugares de trabajo).

Un último bloque comprende aquellos derechos que tienen como titulares a personas en situación de vulnerabilidad y que requieren atención prioritaria (personas con discapacidad, niñas, niños y adolescentes, personas adultas mayores y personas pertenecientes a grupo originarios) y que buscan proteger la identidad personal, los datos neuronales y la voluntad personal (neuroderechos).

Finalmente, se presentan los medios de defensa y derechos de las víctimas del delito cibernético, la violencia digital y las violaciones a derechos humanos. En concreto, se considera que las personas usuarias de Internet y de las TIC tienen el derecho a contar con un recurso judicial adecuado y efectivo para su defensa y, en su caso, para la aplicación de la sanción correspondiente, cuando sus derechos humanos y libertades sean violados o restringidos en Internet.

Asimismo, se establece que las víctimas del delito cibernético, de la violencia digital y de violaciones a derechos humanos tendrán derecho a la asistencia y a la atención, considerando en todo momento un enfoque transversal de género y diferencial. De manera paralela, las autoridades deberán adoptar las medidas que sean necesarias para evitar que la víctima sufra alguna lesión o daño.

Como puede advertirse, la *Carta de Derechos de la Persona Digital. Código de buenas prácticas* ya es un instrumento que nos ayudará a tomar conciencia, por un lado, de los riesgos que afrontamos al hacer uso de las tecnologías y, por el otro, de que no estamos solos en la defensa de nuestros derechos.

# RUTA de la PRIVACIDAD

# COMISIONADOS COORDINADORES DE LA RUTA DE LA PRIVACIDAD

## ARÍSTIDES RODRIGO GUERRERO GARCÍA

*Coordinador de la Comisión de Protección de Datos Personales del SNT*

Doctor en Derecho por la Facultad de Derecho de la Universidad Nacional Autónoma de México, maestro en Derecho, Especialista en Derecho Constitucional y Licenciado en Derecho, grados obtenidos con mención honorífica.

Cuenta con un Máster en Derecho Parlamentario y Estudios Legislativos por la Universidad Complutense de Madrid y un curso avanzado sobre Protección de Datos Personales, impartido por la misma universidad y la Agencia Española de Protección de Datos, así como un curso de Metodología de la Comparación Jurídica por la Universidad de Bolonia, Italia.

En el ámbito docente ha destacado como profesor de la Facultad de Derecho de la UNAM, donde imparte diversas asignaturas, como Poder Judicial, Estructura Política del Estado Mexicano, Derecho Constitucional, Derecho Electoral y Derechos. Fue acreedor de la Medalla al Mérito Docente 2019 Profesor José Santos Valdés, otorgada por el Congreso de la Ciudad de México.

El 18 de diciembre de 2018 fue designado por el Pleno del Congreso de la Ciudad de México para desempeñar el cargo de Comisionado Ciudadano del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (INFO CDMX). El 15 de diciembre de 2021 fue electo como Comisionado Presidente del Instituto.

## JOSEFINA ROMÁN VERGARA

*Comisionada del INAI*

La Doctora en Derecho Josefina Román Vergara se desempeña actualmente como Comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para el período 2019-2026.

Con una carrera de más de 30 años en el servicio público, ha ocupado cargos, mando y dirección en diversas áreas del Gobierno del Estado de México y, a nivel federal, en el Servicio de Administración Tributaria.

En 2013 fue nombrada Comisionada del Instituto de Transparencia, Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios, donde un año después fue elegida, por sus pares, como Comisionada Presidenta.

Ante la Instalación del Sistema Nacional de Transparencia, Acceso a la Información Pública y Protección de Datos Personales, en 2015 fue electa como la Primera Coordinadora de Organismos Garantes de las Entidades Federativas del Sistema. Durante 2018, ocupó el cargo de Secretaria Técnica de la Secretaría Ejecutiva del Sistema Anticorrupción del Estado de México y Municipios. Ha sido docente en las materias de Derecho procesal fiscal y administrativo, Derecho fiscal y hacienda pública en diversas instituciones tanto públicas como privadas. Actualmente continúa como catedrática.

## FRANCISCO JAVIER ACUÑA LLAMAS

*Comisionado del INAI*

Es Licenciado en Derecho por la Universidad Regiomontana y Doctor en Ciencias Políticas y Sociología por la Universidad Complutense de Madrid. Es catedrático de Posgrado en la Especialidad de Derecho a la Información en la Universidad Nacional Autónoma de México.

Autor de diversos libros y publicaciones sobre temas relacionados con Derechos Humanos y Discriminación; Transparencia Electoral; Derecho a la Información; Transparencia y Corrupción; Datos Personales y Acceso a la Información, por citar algunos. Actualmente escribe de manera intermitente en *Excélsior*, *El Financiero*, *El Heraldo de México* y *El Universal*.

Fue Coordinador de Información, Documentación y Transparencia del Tribunal Electoral del Poder Judicial de la Federación, de 2011 a 2014. El 14 de mayo de 2014, rindió protesta como Comisionado del Instituto Federal de Acceso a la Información Pública y Protección de Datos, entonces IFAI. El 12 de mayo de 2017, el Pleno del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) eligió al Comisionado Francisco Javier Acuña Llamas como Presidente para el período 12 mayo de 2017 al 10 de diciembre de 2020.

# GALERÍA


RUTA de la PRIVACIDAD

## INTEGRANTES DEL PLENO

**BLANCA LILIA IBARRA CADENA**

Comisionada Presidenta del INAI

**ADRIÁN ALCALÁ MÉNDEZ**

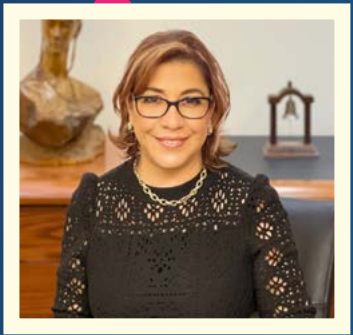
Comisionado del INAI

**NORMA JULIETA DEL RÍO VENEGAS**

Comisionada del INAI

**FRANCISCO JAVIER ACUÑA LLAMAS**

Comisionado del INAI



**JOSEFINA ROMÁN VERGARA**

Comisionada del INAI

# COORDINADORES DE LA RUTA DE LA PRIVACIDAD

**FRANCISCO JAVIER ACUÑA LLAMAS**

**Comisionado del INAI**


**JOSEFINA ROMÁN VERGARA**

**Comisionada del INAI**

**RODRIGO ARÍSTIDES GUERRERO GARCÍA**

**Coordinador de la Comisión de Protección de Datos Personales del SNT**

# EJE TEMÁTICO 1

**OSCAR R. PUCCINELLI**

Doctor en Derecho Constitucional
por la Facultad de Derecho de la Universidad
de Buenos Aires

**PABLO CORONA**

Director de desarrollo
de negocios en NYCE

**CARLA VÁZQUEZ WALLACH**

Abogada, consultora de política pública

**JOSÉ LUIS PIÑAR MAÑAS**

Doctor en Derecho
por la Universidad Complutense

**NELSON REMOLINA ANGARITA**

Profesor Asociado de la Facultad
de Derecho de la Universidad de los Andes

**HUGO ISAAK ZEPEDA**

Coordinador Internacional General
urbano de la Secretaría de Relaciones
Exteriores

**BRICEIDA CERVANTES**

**Experta en Seguridad Nacional**

**JORGE J. VEGA IRACELAY**

**Doctorando en Derecho, Universidad Carlos III, Madrid**

**JESSICA MATUS**

**Abogada experta en internet y privacidad**

**SAIPH SAVAGE**

**Colaboradora de Investigación en la UNAM y Directora del Laboratorio de Inteligencia Artificial Cívico en la Facultad de Ciencias de la Computación Khoury**

**LORENA NARANJO GODOY**

**Directora de la Maestría en Derecho Digital e Innovación y docente de la Universidad de las Américas en Ecuador**

**ZAHRA MOSAWI**

**Ex Comisionada de Comisión de Acceso a la Información de Afganistán**

# EJE TEMÁTICO 2

**HÉCTOR E. GUZMÁN RODRÍGUEZ**

Socio del área de protección
de datos personales y privacidad
en BGBG Abogados

**BERNARDO CUETO RIESTRA**

Secretario de Turismo del Gobierno
del Estado de Quintana Roo

**CARMEN QUIJANO DECANINI**

Socia fundadora de Bufete Quijano

**DIEGO GARCÍA RICCI**

**Universidad Iberoamericana**

**JONATHAN MENDOZA ISERTE**

**Secretario de Protección de Datos Personales del INAI**

**KARLA BELEM NEGRETE HUELGA**

**Profesora-Investigadora de la Facultad de Ciencias Políticas y Sociales de la Universidad Autónoma de Querétaro**

**ISABEL DAVARA F. DE MARCOS**

Doctora en Derecho y Licenciada en Derecho y en Ciencias Económicas y Empresariales por la Universidad Pontificia Comillas de Madrid

**JUAN CARLOS CARRILLO**

Director de Ciberseguridad y Privacidad de Datos, PwC México

**NUHAD PONCE KURI**

Consejera Presidenta del Consejo Consultivo del INAI

**MARCELA TRUJILLO**

**Socia Administradora de RVA Abogados, S.C.**

**PEDRO VICENTE VIVEROS REYES**

**Integrante del Comité de Participación Social (CPS) del Sistema Anticorrupción del Estado de Jalisco**

**OLIVIA ANDREA MENDOZA ENRÍQUEZ**

**Profesora de la División de Estudios Jurídicos del Centro de Investigación y Docencia Económicas, CIDE**

# EJE TEMÁTICO 3

**NORMA JULIETA DEL RÍO VENEGAS**

**Comisionada del INAI**

**ADRIÁN ALCALÁ MÉNDEZ**

**Comisionado del INAI**


**ROBERTO AGUNDIS YERENA**

**Comisionado del IDAIPQROO y Secretario de la Comisión de Protección de Datos Personales del SNT**

**LUIS GUSTAVO PARRA NORIEGA**

**Comisionado Instituto de Transparencia y Acceso a la Información Pública y Protección de Datos Personales del Estado de México y Municipios**

**MARÍA TERESA TREVIÑO FERNÁNDEZ**

**Consejera Presidenta del Instituto Estatal de Transparencia, Acceso a la Información y Protección de Datos Personales y Coordinadora de la Comisión de Gobierno Abierto y de Transparencia Proactiva del SNT**

**JULIO CÉSAR BONILLA GUTIÉRREZ**

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

**FRANCISCO REYNALDO GUAJARDO MARTÍNEZ**

**Comisionado Vocal de la COTAI**

**FABIOLA GILDA TORRES RODRÍGUEZ**

**Comisionada Presidenta del IZAI**

**LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ**

**Comisionada del Instituto de Transparencia y Protección de Datos Personales de la Ciudad de México**

# COMENTARIOS

**LAURA PERLA GONZÁLEZ DÁVILA**

Jefa de Ponencia de la Oficina
del Comisionado del INAI,
Adrián Alcalá Méndez

**EDUARDO BERTONI**

Representante de la Oficina Regional
para América del Sur del Instituto
Interamericano de Derechos Humanos.
Ex-Director de la Agencia de Acceso
a la Información Pública, Argentina

**NANCY PÉREZ GUZMÁN**

Directora General de Investigación
y Verificación del Sector Privado del INAI

**MIREYA ARTEAGA DIRZO**

**Directora General de Prevención y Autorregulación del INAI**

**LUIS RICARDO SÁNCHEZ HERNÁNDEZ**

**Director General de Normatividad y Consulta del INAI**

**RUBÉN TRUJILLO MONTES DE OCA**

**Secretario de Acuerdos y Ponencia de Datos Personales en la Ponencia del Comisionado del INAI, Francisco Javier Acuña Llamas**

**ULISES RAMIREZ GALLARDO**

Jefe de Ponencia de la Oficina del Comisionado del INAI, Francisco Javier Acuña Llamas

**MARTHA JUDITH SÁNCHEZ ÁLVAREZ**

Secretaria de Acuerdos y Ponencia de Acceso a la Información de la Ponencia de la Comisionada del INAI, Josefina Román Vergara

**PABLO PALAZZI**

Máster en Derecho (LL.M.) por la Fordham University School of Law (Nueva York)

**NAYELI AGUAYO GARCÍA**

**Secretaria de Acuerdos y Ponencia de Datos Personales.**
**Oficina del Comisionado del INAI, Adrián Alcalá Méndez**

**MIGUEL NOVOA GÓMEZ**

**Director General de Protección de Derechos y Sanción del INAI**

**VITELIO RUIZ BERNAL**

**Director de Sustanciación de Protección de Derechos**

**CÉSAR MANUEL VALLARTA PAREDES**

**Director General de Evaluación, Investigación y Verificación del Sector Público del INAI**

**GABRIEL SANTIAGO LÓPEZ**

**Jefe de Ponencia de la Comisionada Presidenta del INAI, Blanca Lilia Ibarra Cadena**

**FELIPE DE JESÚS GUTIÉRREZ RINCÓN**

**Jefe de Ponencia de la Comisionada del INAI, Josefina Román Vergara**

# RUTA de la PRIVACIDAD

EN LA REPÚBLICA MEXICANA

## CHIHUAHUA


inai
Josefina Román Vergara
Comisionada del INAI


VIVO
136
inai
RUTA de la PRIVACIDAD
DIPDP 2022
Chihuahua, Chihuahua
PANEL: "Gobierno electrónico, tecnologías y la Protección de Datos Personales"


GUERRERO


nteligencia Artificial:
Perspectivas y prospectivas desde el derecho
a la protección de datos personales y la privacidad


COTAI


Universidad Autónoma de Nuevo León
COTAI


Universidad Autónoma de Nuevo León
RUTA

NUEVO LEÓN

# OAXACA


Com. Josué Solana OSAIPO
Edgar Estrada
Blanca Lilia Ibarra
Francisco Acuña
Arístides Rodrigo Guerrero García
José Méndez Spindola

## QUERÉTARO




QUINTANA ROO

SONORA


FORO ESTATAL
DE TRANSPARENCIA


7 DE OCTUBRE 2022
FORO ESTATAL
DE TRANSPARENCIA


TLAXCALA

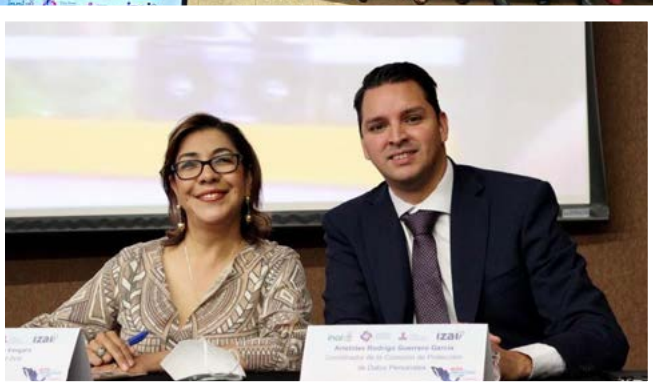

inaip
yucatán
Av. Colón N° 185 por 10 y 12 Col. García Ginerés, C.P. 97070, Mérida, Yucatán.
Tel. (999) 926 86 31, 926 87 44 y al 800 00 46 24
SÍGUENOS
www.inaipyucatan.org.mx

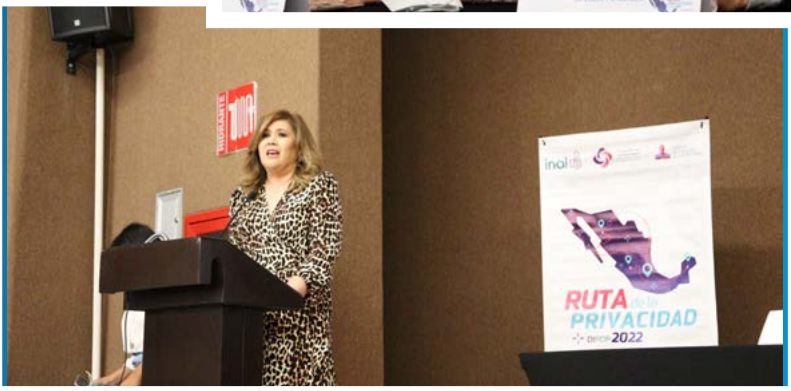

Av. Colón N° 185 por 10 y 12 Col. García Ginerés, C.P. 97070, Mérida, Yucatán.
Tel. (999) 926 86 31, 926 87 44 y al 800 00 46 24
SÍGUENOS
www.inaipyucatan.org.mx

**YUCATÁN**

## ZACATECAS


RUTA de la PRIVACIDAD
2022
ZACATECAS




RUTA de la PRIVACIDAD
2022

Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales

Sistema Nacional de Transparencia
Acceso a la Información Pública y Protección de Datos Personales

# RUTA de la PRIVACIDAD

*Memorias de la Ruta de la Privacidad.*
*Inteligencia artificial: perspectivas y prospectivas*
*desde el derecho a la protección de datos personales y la privacidad*

se terminó de imprimir en noviembre de 2022
en los talleres de Litográfica Ingramex, S.A. de C.V.
Calle Centeno 162-1, Col. Granjas Esmeralda, CP 09810, CDMX.
Libro editado por Editorial Didáctica M.R., por encargo del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Hecho en México.

Se tiraron 2,000 ejemplares.

inai.org.mx

A la luz del Día Internacional de Protección de Datos Personales, que se celebra el 28 de enero de cada año, en 2022, el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, en coordinación y colaboración conjunta con los Organismos Garantes de las Entidades Federativas participantes y la Comisión de Protección de Datos del Sistema Nacional de Transparencia, decidió promover e impulsar la *Ruta de la Privacidad* como una cruzada nacional de socialización para reflexionar sobre la protección de datos personales ante el uso de la inteligencia artificial (IA), y crear conciencia entre los desarrolladores de esa tecnología, los responsables y titulares que la implementan.

A través de este libro, y con la inclusión de las voces de autoridades, sector privado y social, se busca que de modo corresponsable se asuma el compromiso de desarrollo de una IA segura y respetuosa del derecho a la privacidad y a la protección de datos personales; así como difundir el conocimiento generado con estas acciones realizadas a lo largo y ancho de México, para la promoción, socialización y difusión de los derechos que se tutelan desde el SNT y sus organismos garantes.


INAImx inai_mx INAImexico

inaimexico inai.org.mx 800 835 43 24

Avenida Insurgentes Sur 3211, Colonia Insurgentes Cuicuilco,
Alcaldía Coyoacán, Código Postal 04530, Ciudad de México.



editorial

ISBN: 978-607-99443-9-1

9 786079 944391