

DESAFÍOS DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES EN LA ERA DIGITAL

Una mirada desde América Latina

LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ
OLIVIA ANDREA MENDOZA ENRÍQUEZ

COORDINADORAS



tirant
lo blanch

**DESAFÍOS DEL DERECHO A
LA PROTECCIÓN DE DATOS
PERSONALES EN LA ERA DIGITAL:
UNA MIRADA DESDE AMÉRICA LATINA**

COMITÉ CIENTÍFICO DE LA EDITORIAL TIRANT LO BLANCH

MARÍA JOSÉ AÑÓN ROIG

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

ANA CAÑIZARES LASO

*Catedrática de Derecho Civil
de la Universidad de Málaga*

JORGE A. CERDIO HERRÁN

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

JOSÉ RAMÓN COSSÍO DÍAZ

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

MARÍA LUISA CUERDA ARNAU

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

MANUEL DÍAZ MARTÍNEZ

Catedrático de Derecho Procesal de la UNED

CARMEN DOMÍNGUEZ HIDALGO

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

EDUARDO FERRER MAC-GREGOR POISOT

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

OWEN FISS

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

JOSÉ ANTONIO GARCÍA-CRUCES GONZÁLEZ

Catedrático de Derecho Mercantil de la UNED

JOSÉ LUIS GONZÁLEZ CUSSAC

*Catedrático de Derecho Penal
de la Universidad de Valencia*

LUIS LÓPEZ GUERRA

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

ÁNGEL M. LÓPEZ Y LÓPEZ

*Catedrático de Derecho Civil
de la Universidad de Sevilla*

MARTA LORENTE SARIÑENA

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

JAVIER DE LUCAS MARTÍN

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

VÍCTOR MORENO CATENA

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

FRANCISCO MUÑOZ CONDE

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

ANGELIKA NUSSBERGER

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

HÉCTOR OLASOLO ALONSO

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

LUCIANO PAREJO ALFONSO

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

CONSUELO RAMÓN CHORNET

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

TOMÁS SALA FRANCO

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

IGNACIO SANCHO GARGALLO

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

ELISA SPECKMAN GUERRA

*Directora del Instituto de Investigaciones
Históricas de la UNAM*

RUTH ZIMMERLING

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

Fueron miembros de este Comité:

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

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

**DESAFÍOS DEL
DERECHO A LA
PROTECCIÓN DE
DATOS PERSONALES
EN LA ERA DIGITAL:
UNA MIRADA DESDE
AMÉRICA LATINA**

**OLIVIA ANDREA MENDOZA ENRÍQUEZ
LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ**
Coordinadoras

tirant lo blanch
Ciudad de México, 2024

Copyright © 2024

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

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

Este libro será publicado y distribuido internacionalmente en todos los países donde la Editorial Tirant lo Blanch esté presente.

© Colectivo de Autores

© EDITA: TIRANT LO BLANCH
DISTRIBUYE: TIRANT LO BLANCH MÉXICO
Av. Tamaulipas 150, Oficina 502
Hipódromo, Cuauhtémoc
CP 06100, Ciudad de México
Telf: +52 1 55 65502317
infomex@tirant.com
www.tirant.com/mex/
www.tirant.es
ISBN: 978-84-1071-774-9
MAQUETA: Disset Ediciones

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

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

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

DR. JULIO CÉSAR BONILLA GUTIÉRREZ

Comisionado Ciudadano del INFO CDMX

MTRA. LAURA LIZETTE

ENRÍQUEZ RODRÍGUEZ

Comisionada Ciudadana del INFO CDMX

DRA. SONIA VENEGAS ÁLVAREZ

Especialista externa

DRA. JULIETA MORALES SÁNCHEZ

Especialista externa

MTRO. JUAN GÓMEZ PÉREZ

Especialista externo

Coordinador del Comité

ESP. HÉCTOR JAVIER MAYA IBARRA

*Director de Vinculación y Proyección Estratégica del
INFO CDMX*

Secretario Técnico del Comité

LIC. RAÚL LLANOS SAMANIEGO

Director de Comunicación Social del INFO CDMX

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

ARÍSTIDES RODRIGO GUERRERO GARCÍA

Comisionado Presidente del Info CDMX

JULIO CÉSAR BONILLA GUTIÉRREZ

Comisionado Ciudadano del INFO CDMX

LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ

Comisionada Ciudadana del INFO CDMX

MARÍA DEL CARMEN NAVA POLINA

Comisionada Ciudadana del INFO CDMX

Índice

<i>Prólogo</i>	13
JOSEFINA ROMÁN VERGARA	
<i>Introducción</i>	17
<i>Transformación Digital e Inteligencia Artificial</i>	21
YARINA AMOROSO FERNÁNDEZ	
<i>Privacidad y protección de datos personales: Pilares de la ciberseguridad moderna</i>	43
MIRIAM JOSEFINA PADILLA ESPINOSA	
<i>Barreras y nuevas perspectivas sobre la violencia de género facilitada por las TIC</i>	59
JESSICA MATUS ARENAS	
<i>Privacidad y protección de datos en niños, niñas y adolescentes: Desafíos y futuro en la Era Digital</i>	75
MÓNICA VILLALAZ CHIAL	
<i>Privacidad en la era de la computación cuántica</i>	89
OLIVIA ANDREA MENDOZA ENRÍQUEZ	
<i>Panorama de la regulación del derecho a la protección de datos personales en México ante la era digital</i>	107
LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ	

Prólogo

En la última década, la protección de datos personales ha emergido como uno de los temas más cruciales y debatidos en el ámbito global. Este nuevo paradigma no es una excepción en América Latina, una región que, si bien comparte una rica diversidad cultural y socioeconómica, también enfrenta desafíos comunes en la adaptación y aplicación de normativas que resguarden los derechos humanos en un entorno digital cada vez más complejo. *Desafíos del derecho a la protección de datos personales en la era digital: una mirada desde América Latina* no sólo se adentra en esta problemática, sino que lo hace a través de la perspectiva de un grupo de mujeres especialistas, cuyas contribuciones ofrecen una visión comprensiva y multidisciplinaria del tema.

El surgimiento de la era digital ha transformado la manera en que vivimos, trabajamos y nos relacionamos. Por supuesto, la digitalización y el intercambio constante de información han traído consigo grandes beneficios para la convivencia humana, desde la facilidad de acceso a la información hasta la capacidad de conectarnos globalmente en tiempo real.

Sin embargo, este avance tecnológico también ha planteado serias preocupaciones sobre los riesgos inherentes a la privacidad y a la protección de nuestros datos personales. En América Latina, donde las legislaciones aún están en proceso de consolidación y adecuación a los estándares internacionales, la necesidad de abordar estos desafíos se vuelve aún más urgente.

Este libro reúne el conocimiento y la experiencia de destacadas mujeres en el campo del derecho, la ciberseguridad, la tecnología, la privacidad y la protección de datos personales. Ellas, desde diversas disciplinas, abordan las complejidades inherentes a la protección de datos personales. Sus análisis no sólo consideran las perspectivas legales, sino también los aspectos

tecnológicos, sociales y económicos que interactúan en este ámbito.

Uno de los temas más relevantes en las contribuciones de las autoras es la necesidad de armonizar las legislaciones nacionales con los marcos internacionales, como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea. Si bien en varios países de la región, se han adoptado leyes de protección de datos personales inspiradas en el citado GDPR, lo cierto es que la implementación efectiva y la adaptación a las realidades locales sigue constituyendo un reto significativo.

A partir de ello, las autoras subrayan la importancia de una legislación robusta que proteja los derechos de los individuos, pero reconocen la necesidad de fomentar una cultura de protección de datos que trascienda la mera normativa.

Además, la obra explora cómo la educación y la concienciación desempeñan un papel fundamental en la protección de datos personales. En una región donde la brecha digital aún es palpable, y donde muchas personas carecen de un conocimiento adecuado sobre sus derechos digitales, la educación y la sensibilización se convierten en una herramienta esencial. Las autoras proponen estrategias para empoderar a las personas, a través de la formación y la sensibilización, permitiendo que se conviertan en actores activos en la defensa de su privacidad.

Otro aspecto crucial que se aborda en este libro es el papel de la tecnología en la protección de datos. En la era digital, las innovaciones tecnológicas, como la Inteligencia artificial, representan tanto oportunidades como riesgos. Las especialistas discuten cómo estas tecnologías pueden ser utilizadas para fortalecer la protección de datos, mediante sistemas de seguridad avanzados y mecanismos de control más eficientes.

No obstante, también alertan sobre los peligros de un mal uso o abuso de estas tecnologías, que podrían llevar a violaciones significativas de la privacidad y a la seguridad de los grupos en situación de vulnerabilidad; más aún, si consideramos que, de acuerdo

con la Universidad Nacional Autónoma de México,¹ ha quedado demostrado que la IA tiene un rasgo machista, perpetuándose así con sesgos de género y discriminación.

Sin duda, la diversidad de perspectivas nacionales dentro de América Latina es asimismo un punto destacado en este libro. Cada país enfrenta sus propios desafíos y oportunidades en materia de protección de datos, y las autoras reflejan esta variedad, ofreciendo estudios de caso y análisis específicos que enriquecen la comprensión de la persona lectora.

Cada capítulo ofrece una visión detallada de cómo se están abordando estos problemas en diferentes contextos. En definitiva, *Desafíos del derecho a la protección de datos personales en la era digital: una mirada desde América Latina* es una obra que no sólo informa sino que también inspira y motiva a la acción. Las contribuciones de estas mujeres nos invitan a reflexionar sobre el futuro de la protección de datos en nuestra región y a considerar qué medidas podemos tomar para garantizar que el avance tecnológico no se traduzca en una vulneración de nuestros derechos fundamentales.

Este libro es una lectura esencial para cualquier persona interesada en la intersección entre tecnología y derecho, y particularmente valioso para aquellos que buscan entender los desafíos y oportunidades que enfrenta América Latina en este campo.

A través de las líneas de esta obra, y de la mano de mujeres estudiosas de su campo, exploraremos los complejos retos y oportunidades que enfrentamos en la protección de datos personales en la era digital. Este libro ofrece una comprensión profunda y diversa de la realidad latinoamericana en este ámbito crucial,

¹ Vid. Universidad Nacional Autónoma de México. La inteligencia artificial no es feminista. *Gaceta UNAM*. <https://www.gaceta.unam.mx/la-inteligencia-artificial-no-es-feminista/>. Recuperado el 21 de junio de 2024.

constituyéndose en una guía para entender y navegar los retos contemporáneos de la privacidad y la protección de datos.

JOSEFINA ROMÁN VERGARA²

² Comisionada del Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales.

Introducción

El derecho a la protección de datos personales se ha consolidado como un derecho fundamental de cara a la era digital que atravesamos, caracterizada por intensos intercambios de información, particularmente a través de las vías digitales. En este contexto, la protección de datos personales y la privacidad se han convertido en pilares esenciales para garantizar los derechos humanos en una sociedad cada vez más interconectada.

El derecho a la protección de datos personales comienza a cobrar relevancia a partir de la segunda mitad del siglo xx, principalmente en Europa, donde varios países comenzaron a desarrollar leyes que buscaban proteger la privacidad y los datos personales. Esto se puede ver como resultado de una de las primeras iniciativas en la materia, la Declaración Universal de los Derechos Humanos, la cual, a pesar de no reconocer explícitamente la protección de datos personales, reconoce el derecho a la privacidad, sentando así las bases para futuras legislaciones.¹

El Convenio 108 del Consejo de Europa, adoptado el 28 de enero de 1981, es el primer tratado internacional que reconoce principios y normas dirigidas específicamente a la protección de datos personales, marcando un hito en la protección de las personas con respecto del tratamiento de datos de carácter personal.²

Desde entonces, la materia ha evolucionado constantemente, buscando así abordar complejos desafíos que surgen con el

¹ Vid. Protección Data. (sf). *Orígenes del actual marco normativo*. <https://protecciondata.es/historia-normativa-proteccion-datos/>. Recuperado el 13 de junio de 2024

² Vid. Organización de los Estados Americanos. (sf). *Protección de datos personales*. https://www.oas.org/es/sla/ddi/proteccion_datos_personales_otros_documentos.asp. Recuperado el 13 de junio de 2024.

avance de las tecnologías y, sobre todo, con la penetración de la era digital en todos los ámbitos de nuestra vida. En ese contexto, surge esta obra, centrada en la participación y visión de mujeres especialistas en la materia en América Latina, abordando estos desafíos de una manera integral, considerando distintas perspectivas que añaden conocimiento y analizan problemáticas que no son percibidas o abordadas con tanta frecuencia desde los enfoques tradicionales y mayoritarios.

Yarina Amoroso, de Cuba, nos ofrece una mirada integradora de la relación entre Transformación Digital e Inteligencia Artificial, así como su intersección con el Derecho. Con base en claves hermenéuticas, Amoroso hace una exploración de las soluciones jurídicas que son necesarias para abordar las implicaciones éticas, sociales, económicas y políticas de esta herramienta.

A su vez, Miriam Padilla, de México, profundiza sobre el tema de la ciberseguridad, destacando la importancia de la protección de datos personales en un mundo interconectado y en el que el Internet de las Cosas se encuentra en constante expansión, subrayando los desafíos asociados y el camino a tomar desde distintos ámbitos, ya sea personal, corporativo e incluso gubernamental.

Por su parte, Jessica Matus, de Chile, en “Barreras y nuevas perspectivas sobre la violencia de género facilitada por las TIC”, nos ofrece valiosas reflexiones en torno a una problemática compleja que se ha intensificado con el uso de las tecnologías de la información, la violencia de género digital. Además de poner elementos necesarios para el entendimiento de este problema, la autora nos ofrece algunas líneas de acción a seguir hacia su erradicación.

Por otro lado, Mónica Villalaz, de Panamá, realiza un importante análisis en la protección de los datos personales de las niñas, niños y adolescentes, población en posición de mayor vulnerabilidad ante los riesgos que plantea la esfera digital, anotando la necesidad de crear políticas y marcos regulatorios

que se enfoquen en la protección de los menores, dada su mayor posición de vulnerabilidad.

Andrea Mendoza, de México, en su capítulo sobre computación cuántica, explora cómo esta tecnología emergente podría transformar la seguridad de los datos personales, examinando los retos y las oportunidades presentes en la protección de la privacidad.

Finalmente, Laura Enríquez, de México, presenta una perspectiva nacional desde el contexto mexicano, en la que se aborda el panorama respecto de temas específicos relacionados con la protección de datos personales y la privacidad.

En conjunto, este libro ofrece una visión comprensiva y multidisciplinaria que nos permite conocer a profundidad tanto los desafíos como las oportunidades existentes alrededor de la protección de datos personales en una era caracterizada por la digitalización y el intercambio de información, al tiempo que se destaca la invaluable contribución de mujeres especialistas en Iberoamérica, que nos comparten una visión que permite comprender esta materia con un enfoque no solamente distinto, sino más completo.

Las nuevas herramientas tecnológicas han venido no sólo para quedarse, sino que habrán de continuar expandiéndose; por ello, nos encontramos obligados a su estudio continuo, por medio del cual podamos determinar las áreas de oportunidad, y la forma de atenderlas. Solamente de esta manera podremos prepararnos para un futuro incierto en el que cada vez debemos proteger más nuestra privacidad frente a la mayor exposición existente por los distintos medios digitales. Esta obra es una herramienta que permite continuar con este estudio y prepararnos para lo que está emergiendo y lo que está por venir.

Transformación Digital e Inteligencia Artificial

YARINA AMOROSO FERNÁNDEZ¹

Resumen

Se aporta una mirada integradora de la imbricación entre Transformación Digital e Inteligencia Artificial, y de esta relación con el Derecho, con base en lo que se entiende que son algunas de las claves hermenéuticas que permiten comprender y avanzar por la ruta de soluciones jurídicas a esta relación con implicaciones éticas, sociales, económicas y políticas. Se afirma que la Inteligencia Artificial (IA) ha revolucionado numerosos aspectos de la sociedad, incluido el ámbito legal. Se reconoce también que en el contexto de la privacidad y la protección de datos, la IA plantea desafíos y oportunidades significativas.

Palabras claves: Transformación digital, Inteligencia Artificial, Ética Digital, Legal-Tech, Sociocibernética

INTRODUCCIÓN

Asistimos a la transformación digital imbricada en la trama de la llamada Revolución 4.0. (Reyes, 2023) en cuyo contexto se pueden aprovechar las sinergias entre diversas tecnologías, los grandes volúmenes de datos que se acumulan (*BigData*), el Internet de las Cosas (IoT), la Robótica, pero ninguna relación es tan

¹ Profesora Auxiliar del Centro de Estudios de Gestión de Proyectos y Toma de Decisiones de la Universidad de las Ciencias Informáticas de Cuba, y presidenta de la Sociedad Cubana de Derecho e Informática de la Unión Nacional de Juristas de Cuba.

transcendental como la que le aporta la Inteligencia Artificial (IA) (Piñero, 2024).

El término “Inteligencia Artificial” (IA) se formuló en 1956 (Moor, 2006) y durante muchos años se enmarcó en el trabajo científico o académico, o en la ciencia ficción. Hoy la realidad es totalmente diferente; ha salido de los laboratorios y las aulas para estar presente en toda la actividad de la sociedad moderna. Convivimos con la IA aun cuando no seamos consciente de ello.

Este cambio ha sido producto de la combinación de los avances en los métodos de aprendizaje automático, la creciente cantidad de datos y el incremento de la potencia computacional. A la misma vez, las aplicaciones de la IA se han vuelto más compactas, efectivas, baratas, y, por eso, más frecuentemente usadas. Crear sistemas inteligentes y complejos requiere una sustancial potencia de cómputo, pero usarlos generalmente no.

La IA no es sólo una tecnología habilitadora de la transformación digital, sino que la misma transformación digital habilita el desarrollo y las nuevas aplicaciones de la IA. Igual que no hay desarrollo socioeconómico sin transformación digital, no hay transformación digital sin el desarrollo de la IA (Hidalgo, 2024).

Según la CEPAL (2023) los reportes de tendencia señalan a la IA como la tecnología de mayor impacto estratégico, especialmente la de tipo generativa, de manera que la Transformación Digital está habilitada, en buena medida, por la Inteligencia Artificial (IA) y existe entre ellas una estrecha relación.

Estas relaciones implican personas de diferentes profesiones con disímiles competencias e incorpora a la ciudadanía, por lo que se requiere ajustar todo el mecanismo sociocibernético en función de preservar valores y aprovechar las ventajas para impulsar desarrollo sostenible. También con el objetivo de proteger la dignidad humana como valor supremo hay que establecer las bases normativas para ordenar los procesos y soportar la gestión de riesgos, porque la IA es portadora de implicaciones éticas, sociales, económicas y políticas (Herrera, 2023).

Por ello, afirmamos que se abre una nueva ventana en todas las áreas funcionales y especializadas del Derecho, pues el carácter disruptivo de la IA desafía conceptos y categorías largamente consolidados. Esto exige repensar profundamente las instituciones jurídicas y adaptarlas al contexto de una sociedad en transformación digital que impacta el propio desempeño de las organizaciones jurídicas, que pueden ser asistidas, a su vez, por soluciones de IA.

Por ello es necesario reflexionar sobre el Derecho que estos tiempos reclaman para asegurar los cauces legítimos para el uso de las tecnologías de la IA de forma ética, transparente y explicable, y favorecer la realización de las líneas de desarrollo de la IA como disciplina.

A continuación se comparten reflexiones que pretenden sistematizar en apretada síntesis diferentes aspectos que hacen parte de la realidad que trae aparejada el proceso de transformación digital al que asistimos y en el que, como se ha expresado, la IA se manifiesta cada vez más cotidianamente, lo que trae aparejado muchos retos para los empleos, la seguridad, la privacidad y la toma de decisiones basado en datos, que es también tendencia en la evolución y la generación de soluciones inteligentes con base en herramientas de IA. Ello evidencia, a su vez, las necesidades de capacitación en los desarrolladores y los usuarios, así como la evaluación sistemática de las aplicaciones. Cada una de estas cuestiones, entre otras, constituyen puntos de atención para el Derecho.

PENSAR EL DERECHO PARA LA TRANSFORMACIÓN DIGITAL ASISTIDO POR LA IA

El uso de la inteligencia artificial (IA) en los procesos de Transformación Digital presenta varios riesgos que deben ser considerados y regulados por el Derecho. Como ya se ha expresado, la IA maneja grandes cantidades de datos, incluyendo información personal. Una filtración de estos datos puede comprometer el bienestar de las personas. Por eso es tan importante prever desde el diseño de las aplicaciones el cumplimiento de

los principios básicos de tratamiento y protección de datos reconocidos por la legislación para evitar tensiones y violaciones de derechos ante estas realidades.

Si bien en la implementación de procesos de transformación digital es dable que las organizaciones usen herramientas de IA para evaluar el comportamiento de las personas e identificar tendencias de consumo, lo cierto es que la finalidad de vigilar y potencialmente manipular a las personas, plantea serias preocupaciones éticas y legales (Cotino, 2019).

Por otra parte, si los algoritmos de aprendizaje de la IA no se configuran adecuadamente, pueden acabar reproduciendo sesgos propios de los humanos y, por ende, el sesgo algorítmico constituye un elemento de atención para gestionar el riesgo y delimitar las responsabilidades.

También los errores de programación informática pueden afectar a los algoritmos, de forma que ofrezcan resultados engañosos. De ahí se desprende la necesidad de dejar claro en los contratos laborales la responsabilidad social de los desarrolladores, entre otros elementos, por errores programáticos. Para cumplir con el principio de Trazabilidad y Explicabilidad, el equipo de desarrollo o servicio de la IA debe preservar y presentar, si es requerido, la documentación completa de los datos de formación, contexto, finalidad y efectos colaterales.

Los sistemas de IA pueden ser vulnerables a ciberataques que pueden resultar en el robo de datos personales o información confidencial de cualquier organización. Gestionar el riesgo de los ciberataques constituye una máxima de prevención y de que la organización diseñe el plan de contingencia. A su vez, se conoce que muchos de esos ataques se realizan con éxito en buena medida porque aprovechan las vulnerabilidades que muchas veces se generan por imprudencia humana o la violación de reglas de ciberseguridad.

Ello pone en relieve el riesgo de cumplimiento normativo, lo que debe gestionarse con estrictos programas de auditoría y

expresas cláusulas de responsabilidad para operadores de las infraestructuras críticas.

Las decisiones tomadas por los sistemas de IA pueden causar problemas a los individuos, lo que puede resultar en daño e incidir en la pérdida de confianza al interactuar con la organización.

Por eso es importante que los implicados en el desarrollo y uso de estas tecnologías cumplan protocolos claros para cada etapa de su ciclo de vida. Además, es fundamental que el profesional de la Gestión de Riesgos identifique y evalúe las vulnerabilidades inherentes a la Inteligencia Artificial. Aun así, dada la escasa legislación que existe en la actualidad sobre la implantación de la IA, el uso de esta tecnología puede generar situaciones de incumplimiento normativo. Por tanto, cobra importancia el principio de transparencia y la exigencia de la participación humana en la toma de decisiones finales y en los procesos de aprobación de diseños que se reconoce también como un principio.

Al ocuparse de la Transformación Digital (TD) el Derecho tiene que aceptar modificar su dinámica de brindar respuesta jurídica a la realidad que se impone como fruto de las tecnologías emergentes y la convergencia tecnológica, además de que tiene que aportar elementos para la concreción del Gobierno de la Información (Amoroso, Chacón, García, Guerrero, Reyes, 2019), porque es necesario poner más el énfasis en las libertades, derechos, deberes y responsabilidades, así como en las garantías jurídicas en el entorno digital y en la nueva forma de gestionar el interés público y las relaciones de poder con los ciudadanos, lo cual comprende al propio Derecho como sistema de información y como ciencia social.

En las sedes de la administración del Estado y sus organismos públicos, las estrategias para el uso de las tecnologías de la información y las comunicaciones (TIC) constituyen el marco estratégico universal para avanzar en la Transformación Digital de la Administración Pública, estableciendo sus principios rectores,

los objetivos y las acciones para alcanzarlos, así como los hitos para el desarrollo gradual de la Administración Digital, cuyo horizonte hoy debe apuntar a los Objetivos de Desarrollo Sostenible de las Naciones Unidas ods2030.

La estrategia TIC es un documento programático que incorpora las recomendaciones y buenas prácticas para la elaboración de políticas públicas de Administración Digital y se alimenta de la estrecha relación con los documentos de consenso referencial, servicios y oportunidades de cooperación de organismos internacionales para alinearla con la agenda digital nacional y la estrategia regional o global.

Asimismo, es un claro instrumento para la interpretación de normas jurídicas y la elaboración de nuevas Leyes que se integran al ordenamiento jurídico del sector público. Pero este escenario se ha complejizado más con la presencia de la IA que viene acompañada de la exigencia de elaborar su propia estrategia que, lejos de suplantar a la anterior, se suma a los instrumentos programáticos que los hacen parte del orden ético y normativo a seguir.

Así, la Sociedad Digital y en red se enfrenta a las amenazas propias de la naturaleza de la infraestructura tecnológica que la sostiene, a la impronta de las tecnologías emergentes, especialmente las derivadas de la Inteligencia Artificial y a la necesaria optimización de los recursos para lograr combatirlas sin invadir los derechos de quienes son, al fin y al cabo, los destinatarios de protección, los ciudadanos.

Desde la Organización de las Naciones Unidas (ONU, 2020) se insiste en que es preciso continuar impulsando el aspecto de la seguridad en el desarrollo tecnológico, porque la sociedad depende en gran medida de ello. Un mal uso de la IA puede derivar en vigilancia masiva o permitir el acceso y el uso indebido de datos personales o sensibles sin el consentimiento o desconociendo los derechos de las personas afectadas.

La automatización de tareas ha transformado los sistemas de producción y gestión, y ha rebajado mucho los costes aso-

ciados. Como también lo ha hecho en la elaboración, el almacenamiento, el acceso y la difusión de archivos de datos con informaciones de todo tipo, razón por la cual, entre las medidas necesarias de formación o desarrollo seguro de la tecnología, es importante fomentar que se incorporen aspectos de seguridad desde su concepción, además de mitigar las vulnerabilidades existentes y de asegurar sistemas protegidos, bien configurados y gestionados.

Conviene resaltar que esta seguridad no sólo es de tipo tecnológica, sino que también implica la capacidad para crear y mantener información de calidad, veraz y confiable.

En otros términos, lejos de asegurar la solución o servicio digital, de lo que se trata es de hacer las cosas en un entorno de seguridad y disponibilidad confiable, lo que debe gestionarse como un buen hacer *continuum*, asumirse como una cultura, y, por ende, enseñarse en las aulas de ingeniería y gestión de *software* y diseño de sistemas. Otro tanto corresponde a los encargados de velar por la calidad del proceso de desarrollo tecnológico, cuyo producto debe ser validado por el usuario final.

Otro aspecto a tener en cuenta es la gobernanza de las tecnologías emergentes, ya sea relacionada con la revolución de los datos, con los ingentes volúmenes que se generan, o con su susceptibilidad a ser explotados por la Inteligencia Artificial, la robotización, la computarización o la biogenética, por sólo mencionar algunos ejemplos.

Sea como fuere, el Estado debe preservar la capacidad tecnológica de la comunidad y proporcionar herramientas útiles a las estrategias de seguridad pública, aspirando incluso al perfeccionamiento de sus propios desarrollos especializados de las industrias tecnológicas para evitar la dependencia y disminuir los riesgos asociados al consumo de soluciones de seguridad tecnológica.

Hasta ese punto es necesaria la intervención de los poderes públicos, para ofrecer a los ciudadanos las máximas garantías de

seguridad y de protección de sus derechos y libertades en el contexto tecnológico y digital.

Por la complejidad de los retos y amenazas a los que se está enfrentando el ciudadano es importante que las políticas de seguridad pública estén provistas de una capacidad de respuesta adecuada que permita la máxima eficacia en la obtención de resultados con los recursos disponibles.

La Constitución, ley de leyes, confía la garantía de la seguridad ciudadana a las entidades de orden interior y protección de la seguridad nacional, siendo éstos los órganos responsables principalmente, sin ser excluyente, de acometer estas tareas, con un conjunto muy plural y diversificado de actuaciones configuradas al amparo del libre ejercicio de los derechos y libertades de las personas.

En este contexto, la seguridad pública debe ser entendida como la actividad dirigida a proteger valores fundamentales en lo que se fundan la salvaguarda de personas y bienes, a mantener la tranquilidad de los ciudadanos en todas las dimensiones, y, por ellos, igualmente en el Ciberespacio.

En el contexto digital y en red, las amenazas más evidentes se traducen en ataques informáticos a infraestructuras y servicios esenciales, el espionaje, la manipulación de información, los delitos económicos *online*, los daños informáticos, la interceptación de comunicaciones, la video-vigilancia y cualesquiera otros sistemas de control de movimientos de las personas, entre otras conductas indebidas que deben ser objeto de revisión permanente acorde a la propia evolución tecnológica que siempre trae aparejada nuevas vulnerabilidades que hay que gestionar adecuadamente.

Otras amenazas menos visibles, igualmente peligrosas, lo son la extrapolación de la discriminación —dígase racial, de género, origen étnico o cualquier otra—, producto, por ejemplo, de los sistemas evaluadores de riesgo utilizados por la policía; muy a tono con el movimiento social *Las vidas negras importan*

(#BlackLivesMatters), aunque está presente en el otorgamiento de créditos bancarios, las pólizas de las aseguradoras, así como la admisión y facturación en hospitales públicos u otros servicios automatizados.

A mediados de 2019, la Universidad de Stanford publicó los resultados preliminares de un proyecto que, según el rostro, determina la inclinación sexual de las personas. Sin embargo, éste es el *case* que sirvió para entrenar y validar al algoritmo. El objetivo detrás del proyecto es determinar la inclinación política del votante con un sistema de reconocimiento facial en los colegios electorales y que en el futuro permita hacer campañas electorales a la medida, de acuerdo a dónde viven las personas.

La algoritmización puede, en algunos contextos, tener un alcance más propio de la seguridad nacional, porque está muy vinculado al ejercicio soberano en el contexto digital.

Las ciudades inteligentes, la Inteligencia Artificial y el Internet de las Cosas pueden aportar más riesgos sobre el escenario descrito (ITU-T L.1603 (2016)). Pero, si bien es lógico que se vayan actualizando las legislaciones conforme a los retos de seguridad y los exijan, es importante señalar que dejarse llevar por la inmediatez como criterio principal de actuación no va a garantizar un resultado menos lesivo.

En coincidencia con Mena (2018), otros tipos de peligros se originan en el descuido de los mecanismos garantes de la calidad de la información. Por ejemplo, las modificaciones que se producen en la información que está sujeta necesariamente a procesos de actualización y migración. Estos procesos, si se hacen sin cumplirse los requisitos establecidos y con el rigor requerido, generan las condiciones propicias para que existan grandes posibilidades de utilizar datos e información sin calidad, por lo que dejarían de ser información veraz y confiable; por consiguiente, se compromete el valor legal de la evidencia.

En muchas ocasiones el uso de información fallida en la toma de decisiones tiene este origen (Varona, 2020), fruto de

una actitud negligente y sin mala intención, pero que produce efectos que, si bien son imprevisibles, resultan ser igualmente dañinos, como el actuar intencional y culposos, por lo que deriva en ser sujeto responsable del hecho y sus consecuencias.

Las fórmulas para atajar el problema no pueden basarse sin más en el hecho de que exista tecnología que permita repeler las acciones delictivas, sino que se debe ponderar si es tanta la utilidad que proporcionará a efectos de seguridad pública cuando se conculquen derechos fundamentales de forma irreversible o de muy difícil reparación.

En tal sentido, se considera que hay que establecer claramente y dar a conocer a los operadores de sistemas de información sus deberes y responsabilidades sociales, así como las consecuencias jurídicas de sus actos en el proceso de gestión. Igualmente se estima que el ejercicio consciente de asumir y compartir valores éticos en el desempeño profesional es otra garantía para el cumplimiento de las normas en tanto se asumen por convicción ética y responsabilidad conciudadana. Por eso, cada vez más se asume como paradigmas de programación la seguridad por diseño, la privacidad por diseño, y la ética por diseño. Todo lo cual se expresa en lo que ya se empieza a reconocer como componentes prácticos que sostienen el principio de Responsabilidad Social Tecnológica para los desarrolladores de soluciones digitales (Varona, 2018).

Ante este complejo escenario, en los días 19 y 20 de octubre de 2017 el Consejo Europeo planteó la necesidad de una estrategia común de la ciberseguridad en la Unión Europea (UE).

En las conclusiones del debate (Consejo Europeo, 2017) se señalaba que “el mundo digital se basa en la confianza, y que ésta sólo puede lograrse si en todas las políticas digitales se garantiza proactivamente la seguridad desde su concepción, se proporciona una certificación adecuada de seguridad de los productos y servicios, y se incrementa la capacidad para prevenir, disuadir, detectar y responder a los ciberataques”.

Un artículo de referencia del debate del Consejo Europeo en el periódico español *El País* (2017) reconoce que en los debates se examinó la necesidad de “concienciar sobre la urgencia de hacer frente a las nuevas tendencias”, en clara alusión a lo que se comprende como *Trustworthy AI*, que sin ser literal, en español puede asumirse como “IA confiable” e incluye a las tecnologías de cadena de bloques, la que se presentan como solución para garantizar un elevado nivel de protección de los datos, así como la vigilancia sobre los derechos digitales y el comportamiento acorde a las normas éticas.

Pero existen otros problemas más difíciles de resolver —que actualmente se intentan enfrentar para preservar los derechos fundamentales— que tienen su raíz en que se asume que la discriminación resultante de la IA no es intencionada y depende en gran medida del punto de referencia.

Para mejor comprensión, nos acercamos a tres ejemplos:

- Los vehículos autónomos, que ya son una realidad en países como Estados Unidos y Canadá, donde el principal problema ético reside en que en caso de accidente hay que decidir a quién se debe proteger: al dueño del carro, al pasajero, o al peatón al que se dañó, y por ende, determinar quién debe ser juzgado como responsable: al fabricante, el equipo de desarrolladores, o, de manera general, a todos los que con algún grado de participación o condición los vincula el hecho. Respecto del primer problema, en algunas regiones se inclinan por uno o por otro considerando que el núcleo IA del vehículo autónomo debe considerar elementos como la edad, sexo, incluso el estatus social percibido, en su toma de decisiones. Todavía no existe un debate marcado sobre la responsabilidad de los segundos.
- Los sistemas automáticos utilizados para la admisión en las escuelas, donde el algoritmo, en su afán de ser menos discriminatorio, favorece lo que entiende por minorías: emigrantes, raciales, sexuales, entre otros atributos. Y termina discriminando a la inversa. Cuando se escala

el problema se tiene, por ejemplo, que la escuela está compuesta en su mayoría por individuos que pertenecen a comunidades de minorías, y discriminó a gran parte de la población aplicable. Esta realidad se conoce como “discriminación blanca”.

- El caso Amazon y la discriminación laboral por cuestión de género, en el cual se pudo constatar que dicha empresa utilizó un algoritmo de aprendizaje profundo o *deep learning* en los procesos de selección de personal. El algoritmo detectó que el porcentaje de mujeres que habían llegado a la fase final de entrevista en los procesos de contratación de la empresa era muy escaso, motivo por el cual comenzó a rechazar sistemáticamente los currículums presentados por éstas (Vallejo, 2020).

Por eso, el enfoque actual sobre los problemas sociales enraizados en el uso de la tecnología se enfoca principalmente a este último tipo de problemas. Los anteriores, pueden ser considerados como problemas de oficio, que están, y estarán, como resultado de los problemas raíces de la sociedad global y comportamientos indebidos que hoy se reproducen en ese entorno, pero se dan en el entorno de lo conocido y han ido mutando con la evolución tecnológica.

Pero también es correcto señalar que conceptos, como el *overfitting* (sobreajuste) en modelos de aprendizaje automático, tiene que ser exigido. En coincidencia con Varona (2020), muchos de los problemas de sesgo se deben a que los modelos no se reentrenan para evitar el *overfitting*. Lo que, por un lado, dificulta que el sistema pueda llegar a una conclusión, y por otro lado, siguen reproduciendo sesgos preexistentes fruto de los datos originales con que fueron entrenados.

Ante esta realidad, todos los países miembros que integran la ONU están implicados, por su condición de garantes y por su responsabilidad, en actuar para consolidar sus propias estrategias de seguridad en el ciberespacio y de responder a los ataques con los recursos necesarios para prevenir, detectar y

responder ante las crisis, y siempre respetar los derechos de los ciudadanos.

Por eso cada vez más, desde las organizaciones de la propia Naciones Unidas, se les conmina a que no sólo deben preocuparse, sino esencialmente ocuparse de los problemas derivados y previsibles de la IA confiable en la medida que ésta se hace presente en la cotidianidad social y como extensión del ejercicio ciudadano.

Inspirado en esta realidad, el 25 junio de 2019 la Organización para la Educación, Cultura y la Ciencia de las Naciones Unidas (UNESCO) publicó el Consenso de Beijing sobre la Inteligencia Artificial y la Educación, siendo el primer documento multilateral e intergubernamental que propone consejos y convoca a construir un código ético para la IA (UNESCO, 2019).

Este decisivo paso dado en 2019 se corresponde con el compromiso de apoyar a los Estados miembros para que puedan sacar provecho del potencial de las tecnologías de la IA con miras a reconocerla como una oportunidad para alcanzar los Objetivos de Desarrollo Sostenible de las Naciones Unidas ods 2030.

La Recomendación fue aprobada por aclamación por los 193 Estados miembros el 23 de noviembre de 2021. Este instrumento normativo fue elaborado con un enfoque mundial basado en el derecho internacional y centrado en la dignidad humana y en los derechos humanos como valores. Sirve a su vez como base para poner los sistemas de IA al servicio de la humanidad, las personas, las sociedades, así como el medio ambiente y los ecosistemas. También se aprobó con la vocación de estimular la utilización de los sistemas de IA con fines pacíficos.

Este instrumento multilateral reconoce los principios siguientes (UNESCO, 2021):

- Proporcionalidad e inocuidad
- Seguridad y protección
- Equidad y no discriminación
- Sostenibilidad

- Derecho a la intimidad y protección de datos
- Gobernanza y colaboración adaptativas y de múltiples partes interesadas
- Supervisión y decisión humanas
- Transparencia y explicabilidad
- Responsabilidad y rendición de cuentas
- Sensibilización y educación

Al ser una Recomendación, se incluye un mecanismo de evaluación periódica y, con el objetivo de acompañar a los Estados a desarrollar sus propias estrategias, se elaboró una Metodología de Evaluación de Preparación (RAM), herramienta clave para la implementación de la Recomendación sobre la Ética de la IA, porque permite a los países a entender cuán preparados están para aplicar la IA ética y responsablemente para todos sus ciudadanos. La RAM ayuda a resaltar cualquier brecha institucional y regulatoria, y apoya a los gobiernos a llenar esas lagunas, con el fin de asegurar un ecosistema ético de IA de acuerdo con la Recomendación.

La Unión Europea aprobó el 8 de diciembre de 2023 la Ley que regula la IA, el que constituye un marco normativo de implementación gradual hasta 2027, con fases bien delimitadas en el tiempo y que comprenden acciones específicas para que las entidades comiencen a crear las condiciones para cumplir lo normado. Tiene la vocación de convertirse en un estándar legislativo.

La Ley prohíbe la manipulación subliminal y el uso indebido de vulnerabilidades a grupos específicos; reconoce las reglas para la creación de códigos de práctica y gobernanza que orienten a las entidades cómo implementar de manera ética y responsable el desarrollo y uso de sistemas de IA. La Ley acoge asimismo un modelo de regulación basado en riesgos y por ello distingue sistemas de alto riesgo y establece obligaciones específicas. Esta norma propugna por una IA Fiable, porque

se desarrolle y use conforme a la ley, que respete principios éticos y que sea robusta, aquella en que los sistemas de IA siempre ofrecen un correcto funcionamiento y existe el mecanismo para prever medidas de protección que prevean cualquier efecto adverso imprevisto (EUR-Lex, 2023).

EL CIUDADANO DE LA SOCIEDAD DIGITAL Y EN RED. ÉTICA Y DERECHOS HUMANOS

La IA debe basarse en el respeto a los derechos humanos. Preocupa cómo la IA puede afectar la privacidad y la libertad de expresión, de modo que la regulación de la IA debe garantizar que los beneficios superen los riesgos y establecer límites para proteger los derechos humanos.

Hoy los procesos de digitalización y datificación de la sociedad ponen en evidencia cómo el tratamiento de datos desempeña un papel central en el desarrollo de la ciudadanía digital y cómo la presente sociedad algorítmica insta a vincular la dimensión individual y colectiva del uso de los datos.

Desde esta perspectiva, la ciudadanía digital puede hacerse efectiva en términos de participación en la vida democrática sólo si las personas, como individuos y grupos, ejercen su derecho a su propio desarrollo y a su relación, sin restricciones injustificadas por entidades públicas o privadas.

Esto destaca la dimensión sociopolítica de los datos, ya que la información se utiliza para analizar, organizar y dar forma a la sociedad. En este sentido, la relevancia de la protección de datos va más allá de la dimensión individual y se convierte en un elemento constitutivo de la ciudadanía (Consejo Europeo Directiva 2014/60/UE, 2014).

La ausencia de cualquier estigma social y control generalizado es la condición previa para cualquier forma de ciudadanía digital y esto es aún más cierto en la sociedad actual, donde

existe el riesgo de que la “verdad algorítmica” prevalezca sobre las decisiones democráticas (Varona, 2018). Desde esta perspectiva, las cuestiones colectivas relacionadas con el impacto ético y social del uso de datos deben abordarse adecuadamente para desarrollar modelos de gobernanza de datos que los tengan en cuenta.

Los algoritmos tienden a evaluar a individuos y predecir determinados comportamientos basándose en inferencias extraídas sobre la información disponible sobre el grupo con el cual los atributos del individuo exhiben mayor afinidad (Varona y Suarez, 2020). Sin embargo, la decisión final debe siempre abordarse desde la singularidad del individuo y recaer la responsabilidad de la decisión sobre el decisor.

La evaluación de estos impactos sociales —a través de un debate abierto y participativo sobre la dirección que debe tomarse para equilibrar la eficiencia, los derechos y los intereses sociales— es necesariamente parte de una idea de democracia y fundamental para una ciudadanía digital efectiva.

Estamos en una realidad del Derecho frente a la IA y de una zona de gestación del derecho a la IA. En tal sentido, se necesita de una regulación adecuada y justa, aunque la hiperregulación puede tener un efecto contrario al objetivo que se está deseando. Se requiere, por lo mismo, una regulación sólida que equilibre la innovación tecnológica con la protección de los derechos fundamentales de las personas. En este sentido, es fundamental que los juristas estén al tanto de las implicaciones legales y éticas de la IA en relación con la privacidad y la protección de datos.

Si bien la Inteligencia Artificial plantea desafíos complejos en el ámbito legal, especialmente en lo que respecta al derecho a la privacidad y a la protección de datos, los juristas deben estar preparados para abordar estas cuestiones de manera proactiva y garantizar que la IA se utilice de manera ética y respetuosa con los derechos individuales (Fernández, 2020).

A continuación, se detallan algunos de los principales aspectos de este impacto:

1. *Recopilación y procesamiento de datos*: la IA permite recopilar y procesar grandes cantidades de datos de manera rápida y eficiente. Esto plantea desafíos en términos de privacidad, ya que la recopilación masiva de datos puede exponer información personal sensible y generar riesgos de violación de este derecho fundamental.
2. *Análisis predictivo*: los algoritmos de IA pueden realizar análisis predictivos basados en datos históricos, lo que puede llevar a la identificación de patrones y perfiles de comportamiento. Esto plantea preocupaciones sobre la posibilidad de discriminación algorítmica y la toma de decisiones automatizadas que pueden afectar los derechos humanos. La opacidad y los posibles sesgos de estos algoritmos generan preocupaciones sobre la equidad y el respeto a la dignidad de las personas afectadas por estas decisiones.
3. *Transparencia y explicabilidad*: uno de los desafíos clave en el uso de la IA en el ámbito legal es la falta de transparencia y explicabilidad de los algoritmos. Esto dificulta que las personas comprendan cómo se toman las decisiones basadas en IA y cómo se utilizan sus datos personales, lo que puede socavar el derecho a la privacidad y a la protección de datos.
4. *Responsabilidad y transparencia*: la asignación de responsabilidad por las decisiones tomadas por sistemas de IA plantea el reto de garantizar que las personas afectadas mantengan su dignidad y puedan impugnar decisiones que consideren injustas o discriminatorias.
5. *Consentimiento informado*: la recopilación y el procesamiento de datos por parte de sistemas de IA formulan interrogantes sobre la obtención del consentimiento informado de los individuos. Es fundamental garantizar que las personas sean

conscientes de cómo se utilizan sus datos y otorguen su consentimiento de manera informada.

6. *Seguridad de los datos*: la IA también plantea desafíos en términos de seguridad de los datos. Dado que los sistemas de IA suelen depender de grandes cantidades de información, es crucial que los datos se protejan adecuadamente para prevenir violaciones de seguridad y a la privacidad de las personas. La ciberseguridad comienza a asumirse como derecho para el ciudadano y es responsabilidad del Estado establecer los mecanismos para asegurar la protección de los datos y la privacidad.
7. *Interacción humana vs. automatización*: la introducción de sistemas automatizados en el ámbito legal y la administración pública plantea preguntas sobre el papel de los profesionales legales y su capacidad para mantener una relación significativa con los ciudadanos, lo que puede tener implicaciones para la dignidad humana en términos de recibir un trato justo y respetuoso.

Sin lugar a dudas, la recopilación y el procesamiento masivo de datos personales en el contexto de la IA implica desafíos para la protección de la privacidad y la dignidad de las personas, especialmente si no se garantiza un adecuado control sobre el uso de dichos datos. Por otra parte, es fundamental abordar estos retos de manera proactiva para asegurar que se respete el principio de dignidad humana en todas las etapas del desarrollo e implementación y en el uso de estas tecnologías.

CONCLUSIONES

La Inteligencia Artificial (IA) ha revolucionado numerosos aspectos de la sociedad, incluido el ámbito legal. Su utilización plantea desafíos éticos y de responsabilidad, especialmente en lo que respecta a la toma de decisiones automatizadas, la privacidad y protección de los datos y la equidad en el acceso a la justicia.

Es fundamental garantizar la fiabilidad y transparencia de los algoritmos de IA, especialmente cuando se utilizan para tomar decisiones con significativas implicaciones legales.

La IA ha revolucionado la forma en que se realizan tareas rutinarias y repetitivas en el ámbito legal, como la revisión de documentos legales, la gestión de contratos, la investigación jurídica y la redacción de informes. Esto ha permitido una mayor eficiencia y productividad en el trabajo legal. Si embargo, plantea desafíos en términos de privacidad y seguridad de los datos, especialmente cuando se trata de información confidencial y sensible.

Los algoritmos de IA han mejorado la capacidad de realizar análisis predictivos en el ámbito legal, lo que ha facilitado la identificación de patrones, tendencias y riesgos potenciales. Además, la IA ha sido utilizada para apoyar la toma de decisiones legales, como en la predicción de resultados judiciales o en la evaluación de riesgos legales.

Los profesionales legales deben adquirir nuevas habilidades y conocimientos para aprovechar al máximo las capacidades de la IA, lo que puede requerir un proceso de capacitación y adaptación significativo.

Existe el riesgo de que la integración de la IA en el ámbito legal pueda exacerbar las desigualdades existentes si no se garantiza un acceso equitativo a esta tecnología para todos los profesionales legales y ciudadanos.

La integración de la IA en el ámbito legal presenta numerosas oportunidades para mejorar la eficiencia, el acceso a la justicia y la calidad de los servicios legales, pero también desafíos importantes relacionados con la ética, la fiabilidad, la capacitación, la privacidad y la equidad. Abordar estos desafíos de manera efectiva será fundamental para maximizar los beneficios de la IA en el ámbito legal y mitigar sus posibles riesgos que pueden colisionar con el principio de dignidad humana. Se reconoce la importancia de que el operador de justicia retenga en todo momento su

responsabilidad sobre una decisión dada independientemente de la sugerida por los algoritmos.

La Informática Jurídica, también inserta entre las prácticas de uso y desarrollo de la IA, hoy se integra reconociéndose como las humanidades digitales y el humanismo digital en evolución al *LegalTech*; es una herramienta importante para la Transformación Digital y el soporte funcional del Derecho que demanda este proceso, porque conducen a ubicar al ciudadano al centro del proceso y a participar en la decisión.

REFERENCIAS BIBLIOGRÁFICAS

- Amoroso, Y., Chacón, N., García, M., Guerrero, J., Reyes, P. (2019) *Gobierno de la información. Realidades contemporáneas*. Editorial Universidad de las Américas, Quito, Ecuador.
- CEPAL, (2023). *La transformación digital puede contribuir a la transformación de los modelos de desarrollo en América Latina y el Caribe para hacerlos más productivos, inclusivos y sostenibles*. www.cepal.org. Recuperado el 7 de enero de 2024.
- Consejo Europeo (2014). *Directiva 2014/60/UE del 15 de mayo de 2014 relativa a la restitución de bienes culturales que hayan salido de forma ilegal del territorio de un Estado miembro, y por la que se modifica el Reglamento (UE) no. 1024/2012 (refundición)* (DO L 159, 28 de mayo de 2014).
- Consejo Europeo (2017). *Informe EUR-Lex-52013JC0001, 2017/Estrategia Común para la Ciberseguridad*.
- Consejo Europeo (2017). *Informe EUR-Lex-52013JC0001, 2017/Estrategia Común para la Ciberseguridad*.
- Cotino Hueso, Lorenzo (2019). *Derecho y garantías ante el uso público y privado de Inteligencia Artificial, Robótica y Big Data. El Derecho de las TIC en Iberoamérica*. La Ley, Uruguay.
- El País* (2017) *La robótica también sustituye a los empleados de cuello blanco*. <https://books.google.com.cu>. Recuperado el 7 de enero del 2024.
- EUR-Lex (2023) *Reglamento de la IA*. <https://eur-lex.europa.eu>. Recuperado 7 de enero de 2024.
- Fernández Arienza, Alberto, (2020) Comentario a la sentencia de la Corte de Apelaciones en el caso State of Wisconsin Vs Eric L. Loomis del Tribu-

- nal Supremo del Estado de Wisconsin. *Revista Derecho Digital e Innovación*, no. 5. abril-junio.
- Ferry, L. (2017). *La revolución transhumanista. Cómo la tecnomedicina y la uberización del mundo van a transformar nuestras vidas*. Alianza Editorial, pp. 113 y ss. <https://www.amazon.es/revolución-transhumanista>. Recuperado de 7 de enero de 2024.
- Herrera, Triguero Francisco (2023). *Conferencia Magistral, La inteligencia artificial silenciosa ha entrado en nuestras vidas*. Academia de Ciencias de Cuba, La Habana.
- Hidalgo, Delgado Yusniel (2024). *La Inteligencia Artificial en la Transformación Digital de la Sociedad: Casos de estudio en Datalissoft*. X Encuentro Internacional Ciudades MIL de la UNESCO, La Habana.
- Martino, A. (1987). *Manuscrito del Curso de Informática Jurídica impartido en 1897 en La Habana*, Ministerio de Justicia de Cuba, IDG Florencia, Italia.
- Mena, M. y Castillo, J. (2018) Integración de los enfoques de gestión documental y gestión de riesgos para el tratamiento de la información como evidencia de actos y transacciones organizacionales. *Revista Cubana de Información en Ciencias de la Salud*. La Habana.
- Moor, James (2006). *The Dartmouth College Artificial Intelligence Conference: The Next Fifty Years*. AI Magazine, Volume 27, Number 4, pp. 87-91.
- ONU (2020). <https://www.un.org/disarmament/es/los-avances-en-la-informaticizacion-y-las-telecomunicaciones-en-el-contexto-de-la-seguridad-internacional/>. Recuperado 7 de enero de 2024.
- Piñero Pérez, Pedro (2024). *Tendencias de la Inteligencia Artificial. Impacto en el desarrollo*. X Encuentro Internacional Ciudades MIL de la UNESCO, La Habana.
- Proyecto Inocencia. <https://www.innocenceproject.org/>. Recuperado 7 de enero del 2024.
- Recomendación ITU-T L.1603, (2016). *Key Performance Indicators for Smart Sustainable Cities to Assess the Achievement of Sustainable Development Goals*. www.itu.int Recuperado 7 de enero de 2024.
- Reyes, Olmedo Patricia (2023). *Ética de las tecnologías. Desafíos y oportunidades en el mundo digital*. Actas del XXIV Congreso Iberoamericano de Derecho e Informática, Universidad de Villavicencio. Colombia.
- Rifkin, J. (2019). *La sociedad de coste marginal cero: el Internet de las Cosas, los bienes comunes y el eclipse del capitalismo*, Sociedad y Derecho. Paidós, Ibérica, Tribunal de Justicia de la Unión Europea, (2014). (C-131/12), Sentencia pronunciada en 2014. Derecho al olvido.

- UNESCO, (2021). *Recomendación sobre la Ética de la IA*. <https://on.unesco.org/48XkvEO>
- Vallejo, Rivas Pilar (coord.). (2020). *Discriminación algorítmica en el ámbito laboral: perspectiva de género e intervención*. Editorial Aranzadi.
- Varona, D. (2018). La responsabilidad ética del diseñador de sistemas en Inteligencia Artificial. *Revista de Occidente* (446-447), pp. 104-114.
- Varona, D. (2020). *AI Systems Are Not Racists Just Because. T-13 hours: Building Community Online in CSDH/SCHN2020*. London, Ontario: Canadian Society of Digital Humanities.
- Varona, D., Lizama-Mue, Y. y Suarez, J. L. (2020). *Machine Learning's Limitations in Avoiding Automation of Bias*.

Privacidad y protección de datos personales: Pilares de la ciberseguridad moderna

MIRIAM JOSEFINA PADILLA ESPINOSA¹

Resumen

Este capítulo aborda la importancia de la ciberseguridad en un mundo cada vez más interconectado, destacando la prevalencia de internet y la expansión del Internet de las Cosas. Subraya los desafíos asociados a la protección de datos personales y la privacidad, así como la necesidad de adoptar medidas de protección a nivel personal, el desarrollo y ejecución de estrategias corporativas de seguridad de la información en entidades privadas y políticas gubernamentales robustas en materia de ciberseguridad en entidades públicas y gobiernos. Además, reflexiona sobre las consecuencias de un mundo sin ciberseguridad y la importancia de proteger los derechos fundamentales a la privacidad y la protección de datos personales.

Palabras clave: ciberseguridad, privacidad, protección de datos personales, derechos humanos, seguridad de la información.

¹ Especialista en seguridad de datos personales, maestra en Administración de la Tecnología e ingeniera en computación por la Universidad Nacional Autónoma de México. Actualmente es directora de Seguridad de Datos Personales del Sector Privado en el Instituto Nacional de Transparencia, Acceso a la información y Protección de Datos personales (INAI).

INTRODUCCIÓN

En el mundo hiperconectado, donde, según datos de la International Telecommunications Union (ITU) para 2023, el 67 por ciento de la población mundial estaba en línea, es decir, unos 5,400 millones de personas son usuarias de Internet (ITU, 2023), en México, según datos de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTITH), 93.1 millones de personas eran usuarias de internet (INEGI, 2024). Esta información nos brinda datos relevantes sobre la importancia que esta red de redes ha cobrado en nuestra vida cotidiana. Nuestro mundo depende cada vez más de la conexión a internet de nuestros dispositivos y ésta es una de las razones del gran crecimiento del denominado “Internet de las Cosas”,² lo cual, sin duda, facilita nuestra vida cotidiana, pero, a su vez, impone retos en materia de ciberseguridad, privacidad y protección de datos personales.

Todos estos dispositivos conectados, aplicaciones y servicios digitales que utilizamos en nuestro día a día recolectan grandes cantidades de datos, incluidos, por supuesto, datos personales de nosotros. De ahí la importancia de contar a nivel personal con medidas de ciberhigiene digital, a nivel organizacional con una estrategia de seguridad de la información corporativa con un enfoque basado en la gestión de riesgos, y a nivel gubernamental es indispensable desarrollar e implementar estrategias nacionales en materia de ciberseguridad que mediante políticas públicas serán las directrices que permitirán fortalecer la seguridad en los niveles personal y organizacional.

² El término “Internet de las cosas” o *Internet of Things* (IoT) hace referencia a la digitalización de todo tipo de dispositivos comunes, como vehículos, cámaras de grabación, implantes médicos, ropa, etcétera. Los dispositivos IoT permiten enviar y recibir información a través de una red, generalmente Internet, aunque pueden utilizar otras tecnologías. Instituto Nacional de Ciberseguridad (INCIBE) (sf). Temáticas IoT <https://www.incibe.es/empresas/tematicas/iot>. Recuperado el 27 de mayo de 2024.

Hoy estamos cada vez más familiarizados con escuchar o leer noticias sobre vulneraciones a la seguridad de los datos personales³ ocurridas en diferentes entidades del sector privado y el público, en el orden nacional e internacional. Sin embargo, debemos reflexionar sobre lo que realmente nos están diciendo todos estos casos, que muestran la importancia de la ciberseguridad para proteger los derechos a la privacidad y a la protección de nuestros datos personales, evidencian la necesidad de actualizar y fortalecer las medidas de seguridad en curso para proteger la información, reflejan las afectaciones que estos incidentes han generado en las personas usuarias, de dispositivos, plataformas y servicios digitales; muestran cómo han evolucionado las técnicas de ataques conforme a los grandes cambios tecnológicos desde la llegada de la inteligencia artificial. Justo estos puntos trata este capítulo.

¿UN MUNDO SIN CIBERSEGURIDAD?

Imagina que sería de nosotros en un mundo sin ciberseguridad. Para entender la magnitud primero es importante conocer este concepto.

El estándar *ISO/IEC TS 27100:2020 Information Technology-Cybersecurity-Overview and Concepts* (ISO, 2020) define a la ciberseguridad como la protección de las personas, la sociedad, las

³ *Vulneración a la seguridad de datos personales*: es un tipo particular de incidente de seguridad ocurrido en cualquier fase del tratamiento que se caracteriza por afectar a los sistemas de tratamiento de datos personales. Una vulneración a la seguridad de los datos personales considera situaciones como la pérdida o destrucción no autorizada, el robo, extravío o copia no autorizada, el uso, acceso o tratamiento no autorizado y el daño, alteración o modificación no autorizada. Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) (sf). *Recomendaciones para el manejo de la seguridad de la información y protección de datos personales*. https://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf. Recuperado el 27 de mayo de 2024.

organizaciones y las naciones frente a los ciberriesgos, siendo estos últimos definidos como la posibilidad de que las amenazas exploten las vulnerabilidades del ciberespacio y, por tanto, dañen a las entidades que se encuentran en éste.

El ciberespacio se define como el entorno digital interconectado de redes, servicios, sistemas, personas, procesos, organizaciones y aquello que reside en él o lo atraviesa.

De tal forma, imaginar un mundo sin ciberseguridad implicaría la existencia sin control de vulneraciones a la seguridad de los datos personales. Dicho de otro modo, al no contar con medidas de seguridad adecuadas para proteger la información personal, estaríamos expuestos a que nuestros datos personales⁴ y datos personales sensibles⁵ quedaran fácilmente accesibles y explotables por actores malintencionados, lo cual aumentaría los casos de fraudes, extorsiones y usurpación de identidad.

Adicionalmente en este mundo carente de ciberseguridad, no cabría el respeto a la privacidad de las personas, de las organizaciones y de los gobiernos. Por ello, los atacantes podrían sin control interceptar comunicaciones privadas, acceder a dispositivos personales u organizaciones, de tal forma que podrían comprometer y exponer detalles íntimos o confidenciales de sus víctimas.

⁴ *Datos personales*: cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es “identificable” cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información.

⁵ *Datos personales sensibles*: aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual.

Sin mecanismos de defensa, los dispositivos conectados podrían ser infectados fácilmente con *software* malicioso, lo que resultaría en la pérdida de datos, el secuestro de dispositivos —con la finalidad de, por ejemplo, solicitar a la víctima un rescate— o incluso a través del uso de redes de *bots*⁶ llevar a cabo ataques a gran escala.

Los gobiernos podrían verse afectados por ataques que desestabilicen las infraestructuras críticas, considerando que, ante la falta de protección, sistemas, como la energía eléctrica, el agua potable y los sistemas de transporte, entre otros, pueden ser víctima de sabotajes que interrumpan su operación, impidiendo así el funcionamiento de servicios esenciales, lo que afectaría a millones de personas con un impacto que podría ser catastrófico.

Los ejemplos presentados son sólo una pequeña muestra de lo que puede suceder en un mundo sin ciberseguridad, lo que provocaría una desconfianza generalizada en la tecnología, en las empresas y en las instituciones, y afectaría el desarrollo tecnológico y la innovación.

⁶ *Redes bots (botnet)*: es un conjunto de computadoras, denominados *bots*, infectadas con un tipo de programa malicioso, que son controlados remotamente por un atacante y pueden ser utilizados de manera conjunta para realizar actividades maliciosas. Instituto Nacional de Ciberseguridad (INCIBE) (sf). Botnet. <https://www.incibe.es/aprendeciberseguridad/botnet>. Recuperado el 27 de mayo de 2024.

LA PRIVACIDAD Y LA PROTECCIÓN DE DATOS PERSONALES, DERECHOS FUNDAMENTALES PARA LA CIBERSEGURIDAD.

Cuando imaginamos un mundo sin ciberseguridad, podemos formular que dos derechos fundamentales se podrían ver fuertemente impactados.

Uno de ellos es el *derecho a la privacidad* —reconocido en el artículo 12 de la Declaración Universal de Derechos Humanos (ONU, 1948), en el artículo V de la Declaración Americana de los Derechos y Deberes del Hombre (OEA, 1948), en el 11 de la Convención Americana sobre Derechos Humanos (OEA, 1969), en el 17 de Pacto Internacional de los Derechos Civiles y Políticos (Gobierno de México, 1981), y en el caso de México, en el primer párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos (Cámara de Diputados, 1917), instrumentos jurídicos que reconocen el derecho a la no injerencia en la vida privada de las personas, permitiéndoles ejercer el control de la información personal que comparten y sus usos.

Por ejemplo, imagina que una persona prefiere mantener en secreto su orientación sexual, debido a sus convicciones personales o por temor a sufrir cualquier tipo de discriminación, su derecho a la privacidad implica que esta persona tiene la libertad de decidir cuándo y a quién revelará detalles íntimos de su vida privada, de tal forma que se proteja su autonomía y su dignidad.

Por otro lado, está el *derecho a la protección de los datos personales*, el cual brinda a las personas el poder para controlar su información personal, a fin de que pueda decidir quién, cuándo, cómo y hasta qué punto puede ser tratada su información personal (INAI, 2019).

Con el objetivo de garantizar la protección de la privacidad y el flujo transfronterizo de datos personales la Organisation for Economic Co-operation and Development (OECD), publicó en 1980 unas directrices (OECD, 1980) que establecieron los princi-

pios básicos de protección de datos personales, incluyendo la limitación de uso, la seguridad de datos y el derecho a obtenerlos.

Posteriormente, para salvaguardar el derecho fundamental de protección de datos personales, el 28 de enero de 1981 el Consejo de Europa adoptó el Convenio 108 (Consejo de Europa, 1981), oficialmente conocido como la “Convención para la Protección de las Personas con Respecto al Tratamiento Automatizado de Datos de Carácter Personal”, el cual se convierte en el primer instrumento internacional vinculante en el campo de la protección de datos personales, que establece un marco legal para asegurar la protección de la privacidad y los datos personales en el ámbito internacional. Este convenio exige a los países que lo firman implementar medidas en su legislación nacional para aplicar los principios de protección de datos personales, de tal forma que se garantice con ello el respeto a los derechos humanos y a las libertades fundamentales cuando se realiza un tratamiento automatizado de datos.

Cabe señalar que para adaptar la protección de datos personales a las necesidades actuales y futuras en un mundo cada vez más digitalizado y globalizado, el convenio ha sido modernizado dando origen al Convenio 108+ (EDRi, 2019).

En el caso de México, el derecho a la protección de datos personales fue reconocido en 2009, en el segundo párrafo del artículo 16 de la Constitución Política de los Estados Unidos Mexicanos, que establece que toda persona tiene derecho a la protección de sus datos personales, al acceso, la rectificación y cancelación de éstos, así como a manifestar su oposición.

Para que la aplicación de las leyes de protección de datos sea efectiva, existen las autoridades de protección de datos, las cuales tienen el poder de investigar, detectar y sancionar violaciones cometidas por las entidades públicas y privadas. Adicionalmente tienen la responsabilidad de crear conciencia sobre los derechos y obligaciones en los titulares, responsables y encargados.

Retomando el ejemplo del derecho a la privacidad —en este caso cuando hablamos del derecho a la protección de datos personales—, la persona puede decidir compartir con una empresa o institución el dato de su orientación sexual —siempre que la información compartida sea de su conocimiento y consienta en cómo será manejada—, sobre la base de que dicha entidad privada o pública está obligada a garantizar —en cumplimiento con el marco legal aplicable en materia de protección de datos personales— la integridad, confidencialidad y disponibilidad de la información. Adicionalmente, la persona sabe que tiene el derecho a controlar su información y a su acceso, rectificación, cancelación y oposición.

Una vez presentados y ejemplificados los conceptos del derecho a la privacidad y a la protección de datos personales, puede verse cómo éstos están íntimamente vinculados a la ciberseguridad, y esta relación permite entender cómo debe protegerse la información en la Era Digital a través de estos aspectos:

- *Marcos regulatorios*: es indispensable establecer un marco legal sólido y actualizado para la protección de datos personales, la privacidad y la ciberseguridad. En el caso de esta última, es de suma importancia contar con una estrategia nacional que, mediante políticas públicas, leyes y demás normativa que sea necesaria, establezcan estrictos deberes y obligaciones a las entidades privadas y públicas que manejan datos personales. Por ejemplo, en México, el artículo 19 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) (Cámara de Diputados, 2010), que regula el tratamiento de datos personales en el sector privado, y en el artículo 31 de la Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados (LGPDPSO) (Cámara de Diputados, 2017) en el sector público, señalan la obligación de establecer y mantener medidas de seguridad administrativas, técnicas y físicas para proteger los datos personales contra daño, pérdida, alteración, destrucción o el uso, acceso o tratamiento no autorizado.

En el caso de la Unión Europea, el artículo 32 del Reglamento General de Protección de Datos (RGDP) (*Diario Oficial de la Unión Europea*, 2016) impone a los responsables del tratamiento de datos personales la obligación de determinar las medidas de seguridad técnicas y organizativas apropiadas para garantizar el nivel de seguridad adecuado al riesgo, teniendo en cuenta el estado de la técnica, los costes de aplicación, la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas.

De tal forma, todos los tratamientos de datos personales en el ciberespacio, por entidades privadas o públicas, deben contar con medidas de seguridad que reduzcan el riesgo de cualquier vulneración.

- *Educación y concienciación*: la educación sobre ciberseguridad, privacidad y protección de datos personales debe ser una prioridad, a nivel personal, organizacional y de gobiernos. Un ejemplo de esto pueden ser las campañas de concientización que los gobiernos realizan con el objetivo de brindar a la ciudadanía información sobre los riesgos de compartir información personal y, a su vez, presentar recomendaciones para que puedan protegerse contra ataques, además de los programas de capacitación que las organizaciones implementan para fortalecer al interior la cultura en materia de ciberseguridad y protección de datos personales.

Una sociedad que conoce y ejerce sus derechos, que recibe educación en materia de ciberseguridad y protección de datos, es más segura y resiliente frente a los crecientes riesgos y amenazas del entorno digital.

- *Seguridad y privacidad desde el diseño*: actualmente existe la tendencia —y, en algunos casos, la obligación legal— a la incorporación de medidas de seguridad y privacidad desde el diseño de sistemas y aplicaciones. Con ello se bus-

ca que el desarrollo de las tecnologías no sólo sea eficaz desde el ámbito técnico, sino que se incorporen protecciones a la privacidad y datos desde el inicio, cumpliendo con el principio de “privacidad desde el diseño” definido por el estándar ISO 31700-1 *Consumer Protection-Privacy by Design for Consumer Goods and Services-Part 1: High-Level Requirements*, como las metodologías de diseño en las que la privacidad se tiene en cuenta, que son integradas desde la fase inicial de diseño y a lo largo de todo el ciclo de vida de los productos, procesos o servicios que implican un tratamiento de información personal, incluida la retirada del producto y la eventual eliminación de cualquier información personal asociada.

Esto proporciona que las tecnologías y aplicaciones disponibles en el ciberespacio sean respetuosas con los derechos de privacidad y protección de datos.

- *Respuesta a incidentes*: es indispensable desarrollar, adoptar y mantener protocolos efectivos de respuesta ante incidentes de ciberseguridad, sobre todo aquellos relacionados con vulneraciones a la seguridad de los datos personales. Esto implica que las entidades privadas y públicas deben contar con procedimientos internos que les permitan reaccionar rápidamente para contener y mitigar los posibles daños ocasionados por la vulneración y, a su vez, cumplir con las obligaciones que establezca el marco normativo en materia de protección de datos personales, ya sea la notificación a titular y/o a las autoridades competentes.
- *Colaboración internacional*: la protección de datos personales y la ciberseguridad son desafíos globales que requieren la cooperación internacional. Esto puede incluir acciones como el intercambio de mejores prácticas, realizar ejercicios conjuntos de ciberseguridad y la armonización de leyes de protección de datos. Estas acciones facilitan la cooperación y el intercambio seguro de información entre países.

Ejemplo de esta colaboración internacional en materia de protección de datos personales es la Global Privacy Assembly (GPA), la cual tiene como objetivo general lograr la convergencia normativa hacia el establecimiento de estándares internacionales que garanticen la tutela efectiva de un derecho humano a la privacidad y a la protección de datos personales. Para lograrlo la asamblea realiza reuniones anuales, cuenta con grupos de trabajo y publica resoluciones con el fin de promover el intercambio de experiencias y buenas prácticas entre las autoridades de protección de datos y privacidad del mundo.

Del mismo modo, la Red Iberoamericana de Protección de Datos (RIPD), integrada por veinte autoridades de protección de datos de doce países y veintiún entidades observadoras de América Latina, Europa y África, es un foro integrador cuyo objetivo es impulsar la elaboración y adopción de leyes que garanticen el derecho a la protección de datos y privacidad en los países de la región.

- *Tecnología innovadora*: el uso de tecnologías avanzadas como el cifrado, la autenticación multifactor (NIST, 2022),⁷ las tecnologías que mejoran la privacidad (OECD,

⁷ La *autenticación multifactor* es una importante mejora de la seguridad que requiere que el usuario verifique su identidad proporcionando algo más que su nombre de usuario y una contraseña. Requiere que el usuario proporcione una combinación de dos o más de los siguientes elementos: algo que se sabe, algo que se tiene y algo que es. National Institute of Standards and Technology (NIST) (2022). *Multi-Factor Authentication*. <https://www.nist.gov/itl/smallbusiness-cyber/guidance-topic/multi-factor-authentication>. Recuperado el 27 de mayo de 2024.

2023)⁸ y las soluciones basadas en *blockchain* (NIST, 2021),⁹ pueden mejorar de forma significativa la ciberseguridad y la protección de los datos personales, considerando que estas tecnologías ayudan a asegurar que los datos personales en el ciberespacio estén protegidos en tránsito y en reposo.

Trabajar en éstos y otros aspectos es indispensable para lograr un ciberespacio seguro, donde se proteja la información de las personas y se respeten sus derechos.

Un llamado a la acción

⁸ Las *tecnologías que mejoran la privacidad* comprenden una variedad de herramientas diseñadas para salvaguardar la privacidad personal. Estas tecnologías varían desde aquellas que proporcionan anonimato hasta las que permiten a los usuarios controlar la divulgación de su información personal, especificando cuándo y bajo qué circunstancias se puede revelar dicha información. Mediante el uso de las PET, los individuos pueden hacer elecciones conscientes e informadas respecto a la gestión y protección de su privacidad. OECD (2023), *Emerging privacy-enhancing technologies: Current regulatory and policy approaches*, OECD *Digital Economy Papers*, no. 351. OECD Publishing, Paris. <https://doi.org/10.1787/bf121be4-en>. Recuperado el 27 de mayo de 2024.

⁹ El *blockchain* (cadena de bloques) representa un nuevo paradigma para las interacciones digitales y es fundamental en el funcionamiento de la mayoría de las criptomonedas. Funciona como un libro de contabilidad colaborativo e inalterable que registra transacciones en bloques vinculados entre sí. Cada bloque se conecta al anterior mediante un identificador único que cambia si los datos del bloque se alteran, lo que afecta a todos los bloques siguientes. Esto garantiza que cualquier manipulación sea evidente para todos los usuarios de la cadena, ofreciendo un método robusto y seguro para el mantenimiento colaborativo de registros. Esta tecnología ofrece gran resistencia contra alteraciones o destrucciones, fortaleciendo la seguridad y la transparencia en las transacciones digitales. National Institute of Standards and Technology (NIST) (2021). *Blockchain*. <https://www.nist.gov/blockchain>. Recuperado el 27 de mayo de 2024.

En este apartado y una vez que hemos revisado los elementos necesarios para la protección de los datos personales en el entorno digital, y que nos muestra cómo la privacidad y la protección de datos personales son pilares de la ciberseguridad, se listarán algunas acciones indispensables para garantizar que los tratamientos de datos personales en el entorno digital por personas físicas, entidades privadas y públicas y gobiernos cumplan con los principios, deberes y obligaciones establecidas en el marco normativo en materia de protección de datos personales y de ciberseguridad.

Para las personas usuarias:

- Mantenerse informado sobre las prácticas seguras en internet y las herramientas que le permitan proteger su información personal.
- Usar contraseñas robustas y únicas para cada cuenta, para lo cual puede considerarse el uso de un gestor de contraseñas.
- Revisar y ajustar de forma regular las configuraciones de seguridad y privacidad de los dispositivos y de las plataformas digitales utilizadas.

Para entidades privadas:

- Desarrollar e implementar políticas de protección de datos y privacidad que cumplan con el marco normativo vigente.
- Crear y poner en práctica un programa de formación continua acerca de la protección de datos y la ciberseguridad para todos las empleadas y empleados.
- Realizar auditorías internas y externas de forma regular para asegurar la conformidad y la eficacia de las medidas de seguridad.

Para entidades públicas:

- Asegurar la transparencia en el tratamiento de datos personales.
- Establecer mecanismos claros de rendición de cuentas.

- Promover la colaboración con otras entidades para mejorar la protección de datos y conocer las mejores prácticas de seguridad adoptadas a nivel internacional.
- Invertir en tecnologías avanzadas para la protección de infraestructuras críticas y los datos sensibles.

Para gobiernos:

- Desarrollar y actualizar regulaciones que como tema principal consideren la ciberseguridad y la protección de datos personales.
- Llevar a cabo campañas nacionales para educar y concientizar a la sociedad sobre la importancia de la ciberseguridad y cómo deben proteger su información personal.
- Implementar tecnologías de punta y protocolos de seguridad robustos para asegurar que las infraestructuras críticas del gobierno se encuentren protegidas contra ciberataques.
- Participar en foros y acuerdos internacionales para mejorar la cooperación en la protección de datos personales y la ciberseguridad a nivel global.

Estas acciones son fundamentales para que las personas, las entidades privadas y públicas, y los gobiernos aseguren un ambiente digital seguro y respetuoso de los derechos a la privacidad y la protección de datos personales.

REFERENCIAS BIBLIOGRÁFICAS

- Cámara de Diputados del H. Congreso de la Unión (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>. Recuperado el 27 de mayo de 2024.
- Cámara de Diputados del H. Congreso de la Unión (sf). *Constitución Política de los Estados Unidos Mexicanos*. <https://www.diputados.gob.mx/LeyesBiblio/pdf/CPEUM.pdf>. Recuperado el 27 de mayo de 2024.

- Consejo de Europa (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*. <https://rm.coe.int/1680078b37>. Recuperado el 27 de mayo de 2024.
- Diario Oficial de la Unión Europea (2016). *Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos)*. <https://www.boe.es/doue/2016/119/L00001-00088.pdf>. Recuperado el 27 de mayo de 2024.
- European Digital Rights (EDRi) (2019). *Protecting Personal Data World-Wide: Convention 108*. <https://edri.org/our-work/protecting-personal-data-world-wide-convention-108/>. Recuperado el 27 de mayo de 2024.
- Global Privacy Assembly (sf). *Página principal*. <https://globalprivacyassembly.org/>. Recuperado el 27 de mayo de 2024.
- Gobierno de México (1981). *Pacto internacional de Derechos Civiles y Políticos*. <http://www.ordenjuridico.gob.mx/TratInt/Derechos%20Humanos/D47.pdf>. Recuperado el 27 de mayo de 2024.
- Instituto Nacional de Acceso a la Información (INAI) (2019). *Diccionario de protección de datos personales*. https://home.inai.org.mx/wp-content/documentos/Publicaciones/Documentos/DICCIONARIO_PDP_digital.pdf. Recuperado el 27 de mayo de 2024.
- Instituto Nacional de Ciberseguridad (INCIBE) (sf). *Botnet*. <https://www.incibe.es/aprendeciberseguridad/botnet>. Recuperado el 27 de mayo de 2024.
- Instituto Nacional de Ciberseguridad (INCIBE) (sf). *Temáticas IoT*. <https://www.incibe.es/empresas/tematicas/iot>. Recuperado el 27 de mayo de 2024.
- Instituto Nacional de Estadística y Geografía (INEGI) (2024). *Estadísticas a propósito del Día Mundial del Internet*. https://inegi.org.mx/contenidos/saladeprensa/aproposito/2024/EAP_DMInternet.pdf. Recuperado el 27 de mayo de 2024.
- Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI) (sf). *Recomendaciones para el manejo de la seguridad de la información y protección de datos personales*. https://inicio.inai.org.mx/DocumentosdeInteres/Recomendaciones_Manejo_IS_DP.pdf. Recuperado el 27 de mayo de 2024.
- International Organization for Standardization (2020). *ISO/IEC TS 27100:2020 Information Technology-Cybersecurity-Overview and Concepts*. <https://www.iso.org/obp/ui/en/#iso:std:iso-iec:ts:27100:ed-1:v1:en>. Recuperado el 27 de mayo de 2024.

- International Organization for Standardization (2023). *ISO 31700-1:2023 Consumer Protection — Privacy by Design for Consumer Goods and Services Part 1: High-Level Requirements*. <https://www.iso.org/standard/84977.html>. Recuperado el 27 de mayo de 2024.
- Naciones Unidas (1948). Declaración Universal de los Derechos Humanos. <https://www.un.org/es/about-us/universal-declaration-of-human-rights>. Recuperado el 27 de mayo de 2024.
- National Institute of Standards and Technology (NIST). (2021). *Blockchain*. <https://www.nist.gov/blockchain>. Recuperado el 27 de mayo de 2024.
- National Institute of Standards and Technology (NIST) (2022). *Multi-Factor Authentication*. <https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication>. Recuperado el 27 de mayo de 2024.
- OECD (2023). Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches. *OECD Digital Economy Papers*, no. 351, OECD Publishing, Paris, <https://doi.org/10.1787/bf121be4-en>. Recuperado el 27 de mayo de 2024.
- Organización de los Estados Americanos (OEA). (1948). *Declaración Americana de los Derechos y Deberes del Hombre*. <https://www.oas.org/es/cidh/mandato/basicos/declaracion.asp>. Recuperado el 27 de mayo de 2024.
- Organización de los Estados Americanos (1969). *Convención Americana sobre Derechos Humanos*. https://www.oas.org/dil/esp/1969_Convención_Americana_sobre_Derechos_Humanos.pdf. Recuperado el 27 de mayo de 2024.
- Organization for Economic Co-operation and Development (OECD) (1980). *Directrices de la OCDE sobre la privacidad*. https://www.oas.org/es/sla/ddi/docs/directrices_ocde_privacidad.pdf. Recuperado el 27 de mayo de 2024.
- Red Iberoamericana de Protección de Datos (sf). *Inicio*. <https://www.redipd.org/es>. Recuperado el 27 de mayo de 2024.
- Unión Internacional de Telecomunicaciones (2023). *Conectividad universal y significativa para 2030*. <https://www.itu.int/es/mediacentre/Pages/PR-2023-09-12-universal-and-meaningful-connectivity-by-2030.aspx>. Recuperado el 27 de mayo de 2024.

Barreras y nuevas perspectivas sobre la violencia de género facilitada por las TIC

JESSICA MATUS ARENAS¹

Para el progreso de los Derechos Humanos de las mujeres es necesario adoptar medidas integrales y multidimensionales para evitar el uso indebido de la tecnología como herramienta de sometimiento y violencia. El derecho y el acceso a la justicia desempeñan roles vitales en este esfuerzo, para proporcionar la protección requerida y asegurar que las víctimas puedan buscar y obtener reparación de manera efectiva.

¹ Graduada en Derecho por la Universidad de Chile, es una especialista en protección de datos personales, privacidad y ciberseguridad con más de 17 años de experiencia en sectores público, privado y sociedad civil. Es coautora de *La cesión de datos personales* (2006) y autora de ensayos sobre violencias digitales. Con formación en Derecho Informático y estudios de Magíster en Derecho y Tecnologías, imparte clases en diversos diplomados de la Universidad de Chile y Pontificia Universidad Católica de Valparaíso. Es fundadora de Fundación Datos Protegidos (2015), ex presidenta de Internet Society Capítulo Chile (2020-2022), y conductora del podcast “La comunidad de los datos”. En la actualidad, ejerce como consultora nacional e internacional en Matus Legal, consolidando su influencia en este campo.

La violencia de género digital se refiere a actos de violencia facilitados por el uso de tecnologías, donde las víctimas, en su mayoría mujeres, son acosadas, controladas o humilladas a través de medios digitales. Este tipo de violencia se sitúa dentro de una cultura de impunidad, caracterizada por la falta de aplicación efectiva de procesos legales.

La tecnología permite que los abusadores lleguen de manera más rápida a sus víctimas y a una escala mucho mayor. El ciberacoso, la difusión no consentida de imágenes íntimas, la creación y difusión de información falsa, la distorsión de contenido con *deepfake* y otras formas de violencia de género en línea pueden acarrear consecuencias devastadoras para las mujeres, a nivel psicológico y social. La ampliación del alcance del abuso basado en imágenes dificulta que sus víctimas puedan escapar de él, aparte de que las diversas tecnologías de seguimiento, monitoreo y vigilancia para controlar y acosar eliminan la capacidad de encontrar seguridad y refugio.

También supone un impacto profundo en la vida diaria de una mujer, desde su salud mental hasta sus relaciones personales y oportunidades profesionales, lo que perpetúa ciclos de dependencia, pobreza y exclusión social. Cuando la tecnología se utiliza para perpetuar la violencia de género, contribuye a la normalización de esta conducta. Por ello si las plataformas digitales y redes sociales no se regulan de manera adecuada, pueden convertirse en espacios donde la misoginia y la violencia se toleran o incluso de promueven.

En 2018, las Naciones Unidas, en su Resolución sobre “Promoción, protección y disfrute de los derechos humanos en Internet” (Organización de las Naciones Unidas, 2018), expresó su preocupación por “*que persistan muchas formas de brecha digital entre los países y dentro de éstos, así como entre hombres y mujeres y niños y niñas, [...] reconociendo la necesidad de cerrarlas, en particular mediante la cooperación internacional*”. Reconoció que la brecha digital entre los géneros, que incluye disparidades en el acceso

a las TIC y la utilización de esa tecnología, menoscaba el pleno disfrute por la mujer de sus derechos humanos, y que *“las violaciones de los derechos de las mujeres en línea son una preocupación mundial cada vez mayor que entorpece el ejercicio y el disfrute por los géneros de los derechos humanos y las libertades fundamentales en pie de igualdad, y puede disuadir a las mujeres de utilizar las TICs, lo que puede exacerbar la brecha digital entre los géneros y aumentar las desigualdades de género en la sociedad”*.

En la actualidad, no existe país en el mundo que escape a este fenómeno. El desconocimiento sobre los mecanismos de protección —y el temor de las víctimas de ser doblemente victimizadas por denunciar sus casos ante instituciones que no cuentan con protocolos adecuados de atención— supone una importante subestimación de la violencia de género digital.

Un ejercicio integrador de las diversas áreas de investigación y práctica son esenciales para la generación del conocimiento que permita abordar este problema y su erradicación. La información y la visibilización serán entonces determinantes para la toma de decisiones y para el diseño e implementación de políticas públicas. La combinación de éstas con políticas legislativas podría ser la opción de mayor impacto para la prevención, sanción, erradicación y reparación a las víctimas.

PRINCIPALES BARRERAS IDENTIFICADAS Y PERSPECTIVAS EN LATINOAMÉRICA

Disparidad entre las regulaciones

En la región existe un estado dispar en las regulaciones en torno a Internet y las TIC y la prevención y combate de la violencia de género. Escasos países poseen una institucionalidad adecuada contra la violencia de género, y, en muchos casos, las

únicas disposiciones legales aplicables a la violencia digital son ciertos tipos penales que se adaptan a las conductas ejecutadas en el entorno *online*, como en los casos de las amenazas o extorsión. Ante la carencia de normativas apropiadas, las conductas de ciberviolencia quedan en muchos casos sin sanción, o se aplican sanciones inadecuadas, por tipos penales que protegen bienes jurídicos percibidos como de menor importancia por el legislador, que los relega a delitos contra el honor o la intimidad, los que, en muchos casos, son sólo perseguibles por acción penal privada, y sancionados con multa (Herramientas Eurosocial N° 103).

Hoy casi todos los países de la región cuentan con leyes integrales de prevención de la violencia contra las mujeres, pero únicamente en dos países existe un reconocimiento expreso de la violencia digital como una modalidad de la violencia de género, sin perjuicio de que, en general, podrían aplicarse los procedimientos judiciales o administrativos que contemplan este tipo de leyes de manera indirecta, a través de cláusulas abiertas o de remisiones a la modalidad de violencia psicológica.

Este tipo de leyes, definidas por el Observatorio de Igualdad de Género de América Latina y el Caribe de la CEPAL, se caracterizan por poseer:

Un enfoque integral que incluya la actuación de diversas áreas del Estado, con un abordaje capaz de articular la contención, investigación, sanción y reparación de las distintas situaciones que se presentan ante los diversos tipos de violencia. Los mandatos que surgen de las obligaciones internacionales permiten la flexibilidad necesaria para que los Estados den respuestas eficaces frente a todas las formas de violencia a partir de abordajes diversos. Así es como normas de naturaleza penal, civil, administrativa y laboral se combinan estableciendo procedimientos particulares para las distintas problemáticas, con el desafío de articularse dentro de una perspectiva integral ordenadora (Comisión Económica para América Latina y el Caribe, 2015).

Si bien la mayoría de las normativas se ha referido a la difusión de imágenes sin consentimiento, comienza paulatinamente la discusión para incluir otras conductas tan graves como el acoso cibernético, que prácticamente no se denuncia ni mucho menos se sanciona. Es interesante, en este contexto, el trabajo que se está desarrollando en México, donde el Estado de Coahuila lo ha legislado como un delito autónomo, adicionándolo a su Ley de Acceso de las Mujeres a una Vida Libre de Violencia y al Código Penal estatal. A esta tarea se dedica también los estados de México, Aguascalientes, Yucatán, Jalisco y Tamaulipas, entre otros.

En cualquier caso, las sanciones efectivas, proporcionales y disuasorias, incluyendo la privación de libertad y sanciones monetarias según sea apropiado, deberían ser el estándar aplicable a los procesos de ciberviolencia cuando constituya un delito, como lo ha establecido el artículo 13 del Convenio de Budapest sobre cibercrimen.²

Falta de estadísticas oficiales

La ausencia de información estadística actualizada de las personas enfrentadas a diversos actos de violencia *online* en razón de su género es una importante barrera, porque sin ella es imposible dar cuenta de la verdadera magnitud de este fenómeno que permite atender a las necesidades de las personas afectadas. No existen encuestas nacionales sobre violencia de género digital, salvo en México el trabajo que desarrolla el INEGI, con un módulo sobre ciberacoso (MOCIBA)³ que genera información estadística para conocer la prevalencia de ciberacoso entre las personas

² A mayo de 2024, los Estados siguientes de la región han ratificado el Convenio: Argentina, Brasil, Chile, Colombia, Costa Rica, Panamá, Paraguay y República Dominicana.

³ La información más reciente puede consultarse en <https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/MOCIBA/MOCIBA2022.pdf>

de doce años y más que usan internet en cualquier dispositivo, e identificar el tipo y la caracterización del ciberacoso, y en Uruguay las encuestas del Observatorio sobre la Violencia Basada en Género hacia las Mujeres.

Este cometido puede recaer en los órganos de estadísticas u organismos o servicios con competencia en la promoción de derechos de la mujer o igualdad, o mediante el registro de situaciones de violencia facilitada por las tecnologías en centros de atención a mujeres. Es asimismo necesario, con el fin de contar con datos actuales de judicialización en sede civil por responsabilidad extracontractual en estos contextos, obtener información pública, de manera desagregada, de los tribunales con competencia penal y de los órganos de investigación, así como por parte del sistema judicial civil. En variados casos las víctimas han recurrido a la justicia buscando reparación a través de una indemnización por daño moral (Fundación Datos Protegidos, 2019).

Entre las cifras que más preocupan, según un informe elaborado por ONU Mujeres Chile, tenemos que las niñas y adolescentes se encuentran tres veces más expuestas a vivir experiencias de violencia digital y un 41 por ciento reconoció haber sido víctima de acoso digital, Casi la mitad de las adolescentes entre los 15 y 18 años ha recibido una petición de tipo sexual o le han pedido una fotografía íntima contra su voluntad, y la mitad de las adolescentes entre 12 y 14 años ha señalado que alguien las ha “ciberacosado” en el último año (ONU Mujeres Chile, Fundación Datos Protegidos y ONG Amaranta, 2021).

Ausencia de protocolos y preparación técnica (institucionalidad inadecuada)

Se necesita urgentemente la formación y preparación en el conocimiento y tratamiento de los casos de violencia digital por parte de los funcionarios de la administración del Estado, en particular los actores del sistema judicial criminal (jueces,

fiscales, defensores, y policías). Ello requiere la comprensión de los alcances y consecuencias del uso de tecnologías, así como de sus limitaciones, desde la recepción de las denuncias (primera acogida), los protocolos de denuncia, de actuación y otros que sean adecuados y que aseguren la reserva de la identidad e imagen de las víctimas para evitar su revictimización. En tal sentido, la dignidad y la privacidad deben ser los principales elementos.

Resulta de especial relevancia la especialización y el fortalecimiento de las capacidades en materia de cibercrimen y violencia de género. Ello supone un salto de competencias, además de contar con los recursos necesarios para la educación de las víctimas y el público en general en relación con sus derechos y las herramientas legales con las que cuentan para obtener reparación integral, junto con sanciones.

Falta de visibilización del fenómeno de la violencia digital y deficiencias en la educación digital y alfabetización mediática

Muchas personas no están plenamente conscientes de la existencia o la gravedad de la violencia digital, esto incluye no sólo las formas más conocidas, como el ciberacoso, sino otras, como la manipulación digital o el *doxing* (publicación de información privada sin consentimiento). La falta de conciencia puede llevar a que no se den cuenta del abuso o no sepan que están sufriendo una acción criminal.

Los sistemas educativos no han integrado de manera efectiva la educación digital y la alfabetización mediática en sus currículos, lo que deja a jóvenes sin las herramientas necesarias para navegar de manera segura, así como reconocer y manejar situaciones de violencia digital, además de que perpetúan estereotipos y culpan a la víctima, minimizando la gravedad de la agresión.

No visibilizar el problema afecta la disponibilidad de los recursos para las víctimas. La falta de información, o el escaso

apoyo de las autoridades, impide, desincentiva u obstaculiza a las mujeres a interponer una denuncia y recibir apoyo legal, psicológico y de servicios de asistencia.

Instituciones como las autoridades de protección de datos personales podrían cumplir un rol importante, por su carácter técnico y conocimientos especializados en TIC. Es posible hallar variados proyectos e iniciativas en materia de violencia de género digital de parte de este tipo de organismos. Un caso a destacar es el denominado “Canal Prioritario” de la Agencia Española de Protección de Datos, para solicitar la retirada urgente de contenidos sexuales o violentos publicados sin consentimiento en internet, o la Mesa de Trabajo Sobre Violencia Digital y Salud Mental que se ha constituido recientemente en el marco de la Red Iberoamericana de Protección de Datos.

Por otra parte, es importante la organización de redes, mesas de trabajo y discusión, la celebración de convenios y otras formas de colaboración en el ámbito público, y eventualmente la colaboración público-privada —dentro de sus competencias—, tanto internamente como a niveles regional e internacional.

Fallas en la aplicación de procesos legales

Una de las barreras más significativas es la falta de implementación efectiva de los procesos legales. La percepción de impunidad prevalece, gracias a los muchos actos de violencia digital que quedan sin sanción. Esta situación se debe a múltiples factores, como la falta de leyes específicas, la escasa preparación de los funcionarios encargados de aplicar la ley, y la complejidad inherente a la identificación y persecución de delitos en el entorno digital.

De acuerdo con un estudio de 2020, en México en los últimos tres años en 18 estados del país se han abierto 2,143 carpetas de investigación por el delito de difusión de imágenes

íntimas sin consentimiento, y sólo el 17 por ciento de las carpetas iniciadas han encontrado alguna forma de conclusión a través de alternativas de justicia sin llegar a juicio, tales como la suspensión condicional del proceso, el acuerdo reparatorio o el juicio oral abreviado. Dicho informe refiere hallazgos clave, como la ejecución de las reformas a nivel local de la Ley Olimpia (difusión no consentida), y los obstáculos que han enfrentado las víctimas al iniciar procesos penales: el 84.46 por ciento de las víctimas fueron mujeres y el 83 por ciento de las carpetas de investigación siguen en trámite (Luchadoras, 2020).

En definitiva, la escasa formalidad en el tratamiento de denuncias de violencia digital dificultan la evaluación del problema y la formulación de políticas efectivas.

Acceso a la justicia y necesidad de reparación

Para lograr reparaciones transformativas efectivas en casos de violencia de género se deben implementar medidas que operen a niveles individual, institucional y estructural. Esta aproximación integral garantiza que las reparaciones no sólo aborden el daño inmediato sufrido por las víctimas, sino que también modifiquen las condiciones que permitieron que ocurriera la violencia. Involucrar a mujeres de diversas etnias, niveles socioeconómicos y ubicaciones geográficas en las discusiones sobre reparaciones, permitirán asegurar que las políticas y medidas adoptadas reflejen fielmente sus experiencias, preocupaciones y necesidades específicas. Este enfoque inclusivo y representativo ayuda a desarrollar iniciativas más efectivas y pertinentes que verdaderamente abordan las raíces y las consecuencias de la violencia de género.

Igualmente, es importante reconocer que las medidas de reparación deben ir más allá de la mera compensación económica: deben incluir un espectro más amplio de respuestas, como la restitución, la rehabilitación, la satisfacción y las garantías de

no repetición, que abarquen soluciones materiales y simbólicas. Estas medidas deben ser adaptadas a las circunstancias individuales y las preferencias de las víctimas, pudiendo variar desde compensaciones en dinero hasta iniciativas que promuevan la recuperación emocional y psicológica, y el reconocimiento público del daño sufrido. Por ejemplo, la ejecución de políticas para evitar la revictimización durante el proceso judicial será determinante para proteger la dignidad y la integridad de las víctimas mientras buscan justicia.

Entre las medidas específicas que podrían adoptarse se incluyen la obligación de investigar los hechos y de identificar, procesar y sancionar a los responsables de las violaciones. Esto no sólo contribuye a la justicia inmediata, sino que también actúa como un disuasivo contra futuras agresiones. Deberían establecerse mecanismos para evitar la revictimización de las afectadas durante los procedimientos judiciales y ofrecer apoyo integral que incluya rehabilitación psicológica, representación legal y servicios sociales para las víctimas y sus familiares, así como las de los perpetradores. Además, incorporar programas de reeducación para los agresores, centrados en género y derechos humanos, para modificar las estructuras subyacentes que perpetúan la violencia de género.

Estas acciones pueden, al ser implementadas de manera coordinada y con un enfoque de derechos humanos, transformar efectivamente las condiciones que permiten la violencia de género, facilitando un camino hacia la justicia y la reparación completa.

Falta de cooperación internacional de las plataformas digitales. Carga de la prueba sobre la víctima. Preservación de los datos

La falta de cooperación internacional de las plataformas digitales en la lucha contra la violencia de género en línea es una preocupación en crecimiento. A pesar de los esfuerzos en algunos sectores, todavía existe una gran disparidad en cómo

los países y las plataformas manejan las denuncias y regulan el contenido nocivo, incluyendo el acoso y la difusión no consentida de imágenes íntimas. Esto se debe en parte a la diversidad de leyes y normativas a nivel internacional que complican la colaboración y la ejecución de medidas uniformes. Las plataformas digitales deben, por lo mismo, adaptarse y responder a estas diferencias legislativas, lo que a menudo resulta en una falta de respuestas efectivas y coordinadas que protejan de manera adecuada a las víctimas en todos los países. Este problema persiste incluso en países que han aprobado el Convenio de Budapest sobre ciberdelincuencia, que contiene disposiciones procesales útiles para la recopilación de pruebas o la cooperación internacional, de aplicarse en este tipo de casos verdaderamente.

Otro problema de magnitud es que la carga de la prueba recae sobre las víctimas. Frecuentemente, para demostrar el abuso ellas tienen que proporcionar evidencia extensa, lo cual puede ser un proceso invasivo y traumatizante. Esta exigencia no sólo aumenta el estrés emocional de las víctimas, sino también puede desalentarlas de reportar los incidentes, especialmente si sienten que el proceso es complicado y poco claro. La necesidad de presentar pruebas concretas pone un peso desproporcionado en las víctimas, las cuales muchas veces carecen de la asistencia de las plataformas digitales para recopilar dicha información.

Para asegurar que las pruebas de violencia de género en línea no se pierdan y puedan ser utilizadas en procesos legales cuando sea necesario, la preservación de los datos es esencial. Las plataformas digitales deben garantizar que los datos relacionados con casos de abuso se mantengan seguros y accesibles para investigaciones y procedimientos judiciales. Sin embargo, la falta de políticas claras y consistentes sobre la retención de datos ha resultado en la pérdida de valiosa información, lo que afecta negativamente la capacidad de las víctimas para buscar justicia. Es urgente que las empresas implementen y cumplan

con políticas de retención de datos que protejan la información relevante durante el tiempo necesario.

Finalmente, el rol de las empresas nacionales y transnacionales que ofrecen servicios de internet es fundamental para la prevención y combate de la violencia de género en línea. Estas empresas no sólo deben adherirse a las leyes locales e internacionales, sino también mejorar proactivamente sus políticas y herramientas para detectar y responder a este tipo de violencia. Deben trabajar en estrecha colaboración con las víctimas y las autoridades para facilitar la entrega de información cuando sea legalmente requerida. Además, la transparencia sobre los procedimientos de reporte y su efectividad es vital para construir una relación de confianza con los usuarios y disuadir la percepción de impunidad en las plataformas. En conjunto, estas medidas son fundamentales para crear un ambiente digital seguro y responsable.

Evaluación de daños de las ciberviolencias. Consecuencias psicológicas, sociales y laborales

Las ciberviolencias representan una de las violaciones más graves a la privacidad e intimidad de las personas, que afectan su dignidad, así como su integridad psicológica y hasta física. El daño que provocan es de tal magnitud que, en muchos casos, resulta irreversible. Las víctimas sufren una amplia gama de consecuencias, desde amenazas de agresión sexual, presión para permanecer en relaciones abusivas, extorsión, acecho y hostigamiento, hasta despidos laborales, expulsiones escolares y el abandono forzoso de sus hogares. Este tipo de violencia tiene un impacto devastador en la salud mental de las víctimas que, a menudo, desarrollan estrés postraumático, depresión, e incluso pueden llegar al suicidio debido a la intensa angustia emocional que experimentan.

La naturaleza persistente y la difusión masiva facilitada por internet agravan aún más el sufrimiento de las víctimas. Una vez que el material ha sido publicado y redistribuido, el daño continúa sin necesidad de nuevas acciones por el perpetrador. Esta perpetuidad de la violencia digital no se refleja adecuadamente en las sentencias judiciales, aunque las víctimas siguen siendo revictimizadas cada vez que un nuevo colega profesional, pareja romántica o cualquier otra persona las busca en línea. La facilidad con la que estas imágenes privadas pueden encontrarse en internet exacerba el trauma, ya que las víctimas temen constantemente ser expuestas y juzgadas por aquellos en su entorno social y profesional (Cybercrime Convention Committee, 2018).

Además de los daños psicológicos y sociales, las ciberviolencias acarrearán importantes consecuencias en el ámbito laboral. Las víctimas pueden enfrentar despidos, obstáculos en sus carreras y dificultades para encontrar trabajo debido a la información perjudicial disponible en línea. Como han señalado Citron y Franks (2014), los daños causados por la divulgación no consentida de imágenes sexualmente explícitas pueden tener consecuencias duraderas y destructivas. Las víctimas internalizan la vergüenza y humillación impuestas por la sociedad, sintiendo un profundo impacto emocional cada vez que ven las imágenes o piensan que otros podrían estar viéndolas. Este ciclo de revictimización perpetúa el daño y subraya la necesidad urgente de abordar la ciberviolencia con soluciones legales y sociales específicas.

La violencia de género digital es un problema complejo y multifacético que para su erradicación requiere un enfoque integral. Es necesario fortalecer los marcos legales, mejorar la formación de los actores de justicia y promover la cooperación internacional. La implementación de tecnologías innovadoras y programas educativos es esencial para crear un entorno digital seguro para todas las personas. Las estrategias deben incluir la

creación de nuevas leyes que aborden específicamente la violencia digital, el desarrollo de herramientas tecnológicas para la denuncia y protección de las víctimas, y la educación continua en temas de seguridad digital.

REFERENCIAS BIBLIOGRÁFICAS

- Citron, D., y Franks, M. A. (2014). *Criminalizing Revenge Porn*. *Wake Forest Law Review*, 49, 364p.
- Comisión Económica para América Latina y el Caribe (2015). *Marco de abordaje integral para la prevención, atención y reparación de la violencia contra las mujeres y las niñas*. https://oig.cepal.org/sites/default/files/2020_-_marco_de_abordaje_integral_para_la_prevenccion_atencion_y_reparacion_de_la_violencia_contra_las_mujeres_y_las_ninas.pdf
- Cybercrime Convention Committee (2018). *Mapping Study on Cyberviolence*. <https://rm.coe.int/t-cy-2017-10-cbg-study-provisional/16808c4914>.
- Fundación Datos Protegidos (2019). *Violencia de género en Internet en Chile*. <https://datosprotegidos.org/wp-content/uploads/2018/12/Informe-Violencia-de-ge%CC%81nero-en-Internet-en-Chile.pdf>.
- Herramientas Eurosocia n° 103 (sf). *Programa para la cohesión social. Estado de la legislación en materia de violencia de género digital en Latinoamérica*. https://eurosocia.eu/wp-content/uploads/2022/06/Herramientas_103_Estado_de_la-legislacion_materia_de_violencia_genero.pdf.
- Instituto Nacional de Estadística y Geografía (INEGI) (2022). *Comunicado sobre módulo sobre cibercoso*. <https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2023/MOCIBA/MOCIBA2022.pdf>.
- Luchadoras (2020). *Justicia en trámite: El limbo de las investigaciones sobre violencia digital en México*. <https://biblioteca.avina.net/biblioteca/justicia-en-tramite-violencia-digital-en-mexico/>.
- ONU Mujeres Chile, Fundación Datos Protegidos y ONG Amaranta (2021). *Violencia digital: Experiencias virtuales de niñas y adolescentes en Chile*. <https://datosprotegidos.org/descarga-resultados-encuesta-violencia-digital-experiencias-virtuales-de-ninas-y-adolescentes-en-chile/>.

Organización de las Naciones Unidas (2018). *Resolución A/HRC/38/L.10 Promoción, protección y disfrute de los derechos humanos en Internet*. https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L10.pdf.

Privacidad y protección de datos en niños, niñas y adolescentes: Desafíos y futuro en la Era Digital

MÓNICA VILLALAZ CHIAL¹

Resumen

Este artículo aborda los desafíos y riesgos relacionados con la protección de datos y privacidad en niños, niñas y adolescentes en la Era Digital. Se analiza la problemática del uso indebido de información y datos personales por esta población y las responsabilidades de los adultos que están a cargo de su cuidado en la protección de la privacidad de los menores. A través de una visión crítica y reflexiva, se exploran las amenazas emergentes, como el ciberacoso y el robo, o la suplantación de identidad, y se discuten estrategias y políticas para mejorar la seguridad digital de la niñez y adolescencia. Este escrito intenta hacer una proyección hacia el futuro de la protección de datos, sugiriendo la necesidad de una mayor formación en temas digitales y de legislaciones más fuertes para salvaguardar la privacidad infantil y adolescente.

Palabras clave: protección de datos, privacidad de menores, ciberseguridad, educación digital, riesgos en internet.

Keywords: child privacy, data protection, online safety, digital education, technological regulations.

¹ Fundadora de Vida Segura.

Summary

This article explores the challenges and risks associated with the privacy and data protection of children and adolescents in the digital environment. As digitalization progresses, minors are exposed to multiple risks that can affect their well-being and development. The responsibilities of adult caregivers in educating and supervising young people online are discussed, along with the strategies and tools available to protect their personal information. The chapter also examines the evolution of policies and regulations and the role of technology companies in safeguarding children's privacy. Finally, it projects what the future of privacy and data protection will look like in an ever-changing digital world, highlighting the need for an ethical and collaborative approach to ensure the safety of minors.

INTRODUCCIÓN

La privacidad y protección de datos de niños, niñas y adolescentes en el entorno digital se ha convertido en un tema de creciente preocupación debido a la masificación de la tecnología y el incremento que tuvo a partir de 2020 cuando inició la pandemia de Covid-19, sin detenerse al día de hoy. En un mundo donde la digitalización avanza a pasos agigantados los menores están expuestos a una variedad de riesgos que pueden tener repercusiones significativas en su bienestar, desarrollo y salud (mental, física y emocional).

Como experta en sensibilización sobre el uso seguro de internet y la ciudadanía digital para niños y adolescentes, he presenciado de primera mano los desafíos que enfrentan los adultos cuidadores al intentar proteger a los más jóvenes en el mundo digital. A lo largo de los últimos ocho años, he trabajado incansablemente para educar y empoderar a esta población, brindándoles las herramientas y el conocimiento necesarios para navegar de manera segura y responsable en internet.

Sin embargo, a pesar de los esfuerzos realizados, los riesgos y amenazas a la privacidad y la protección de datos de los niños, niñas y adolescentes siguen siendo alarmantes. Este artículo examina los desafíos que enfrentamos los adultos en la protección de datos de los jóvenes y los riesgos asociados con

el mal uso de su información personal. Se pretende discutir las responsabilidades de los adultos cuidadores y proyectar cómo será el futuro en términos de privacidad y seguridad de datos para esta población.

EXPOSICIÓN Y VULNERABILIDAD

Los niños, niñas y adolescentes están inmersos en un entorno digital desde una edad, cada vez más temprana, lo que los expone a múltiples riesgos relacionados con la privacidad de sus datos personales. La recopilación de datos comienza muchas veces con el consentimiento de los padres, pero a menudo éstos no comprenden completamente las implicaciones a largo plazo. Aplicaciones educativas, juegos conectados a internet y redes sociales recopilan información que puede ser utilizada de maneras no previstas por los padres o por los propios menores.

Según un estudio de UNICEF, el 75 por ciento de los niños de entre 13 y 17 años posee un perfil en redes sociales, y más de la mitad ha compartido información personal en línea sin comprender las consecuencias potenciales (UNICEF, 2017). Esta vulnerabilidad se agrava cuando consideramos que muchas plataformas no implementan adecuadamente políticas de privacidad que protejan a los menores.

RIESGOS ASOCIADOS AL MAL USO DE DATOS

El mal uso de los datos personales de niños, niñas y adolescentes puede acarrear graves consecuencias. Entre los riesgos más preocupantes se encuentran las diferentes formas de ciberacoso, el *grooming* y el robo de identidad. El ciberacoso —que incluye hostigamiento y humillación en línea— afecta a aproximadamente uno de cada tres adolescentes, según datos de la Organización Mundial de la Salud (OMS, 2022). Además,

los ciberagresores pueden utilizar información personal para ganarse la confianza de los menores y explotarlos.

Otros riesgos son:

- *Exposición excesiva de información personal:* los niños y adolescentes a menudo comparten demasiada información personal en línea sin comprender completamente las implicaciones de privacidad y seguridad. Según un estudio de la Oficina del Comisionado de Información del Reino Unido (Information Commissioner's Office o ICO), el 63 por ciento de los niños de entre 8 y 11 años ha publicado información personal en línea, incluyendo su nombre completo, edad y ubicación (Livingstone, y Helsper, 2020, pp. 1476-1493).
- *Falta de conciencia sobre la huella digital:* muchos jóvenes no son conscientes de que sus actividades en línea dejan una huella digital permanente que puede ser rastreada y utilizada de manera inadecuada. Un informe de la Comisión Federal de Comercio de los Estados Unidos (Federal Trade Commission o FTC) reveló que el 92 por ciento de los sitios *web* y aplicaciones populares para niños recopila información personal sin el consentimiento de los padres (Comisión Federal de Comercio, 2022).
- *Riesgos de sextorsión y ciberacoso:* los ciberacosadores pueden utilizar tácticas de ingeniería social para obtener información personal y luego chantajear o acosar a los niños y adolescentes. Según un reporte del Network Contagion Research Institute (NCRI), la sextorsión financiera es el delito de más rápido crecimiento dirigido a niños en Estados Unidos, Canadá y Australia (Network Contagion Research Institute, 2024).
- *Vigilancia y recopilación de datos por parte de empresas tecnológicas:* las principales empresas tecnológicas como buscadores, redes sociales, plataformas digitales, videojuegos, etcétera, recopilan y monetizan grandes cantidades de

datos de los usuarios, incluyendo a los de niños y adolescentes.

- *Falta de regulaciones nacionales, territoriales, internacionales adecuadas y aplicación de las mismas:* a pesar de la creciente preocupación por la privacidad y la protección de datos de los niños y adolescentes, las regulaciones actuales a menudo son insuficientes o no se aplican de manera efectiva. Un informe de la Comisión Europea reveló que sólo el 38 por ciento de los países miembros ha implementado plenamente el Reglamento General de Protección de Datos (RGPD) en lo que respecta a los menores (EU GDPR, 2020). En Latinoamérica pocos países han implementado legislación referente a ciberseguridad y ciberdelitos, aunque trece países han ratificado el Convenio de Budapest.

EL FUTURO DE LA PROTECCIÓN DE DATOS Y LA PRIVACIDAD INFANTIL

A medida que avanzamos en la era digital, los desafíos relacionados con la privacidad y la protección de datos de los niños, niñas y adolescentes sólo aumentarán. Algunas de las implicaciones futuras incluyen:

- *Mayor exposición a riesgos en línea:* con el aumento de la realidad virtual, la realidad aumentada y las tecnologías de inteligencia artificial, los niños y adolescentes estarán aún más expuestos a riesgos en línea, como la suplantación de identidad, la manipulación de contenido y el acoso cibernético.
- *Mayor recopilación y uso de datos personales:* las empresas tecnológicas continuarán recopilando y utilizando datos personales de los usuarios, incluyendo a los niños y adolescentes, para fines comerciales y de *marketing*. Esto plantea preocu-

paciones sobre la privacidad y la protección de datos a largo plazo.

- *Impacto en el desarrollo y el bienestar emocional:* la exposición excesiva a contenido inapropiado, el acoso cibernético y la violación de la privacidad pueden tener un impacto significativo en el desarrollo y el bienestar emocional de los niños y adolescentes, lo que puede generar problemas de salud mental a largo plazo.
- *Desafíos en la aplicación de regulaciones:* a medida que surgen nuevas tecnologías y plataformas, las regulaciones actuales pueden quedar rápidamente obsoletas, lo que plantea desafíos continuos para garantizar la privacidad y la protección de datos de los niños y adolescentes. Dependerá en gran medida de la evolución de las normativas y políticas a nivel global. Iniciativas como el Reglamento General de Protección de Datos (GDPR) de la Unión Europea y la Ley de Protección de la Privacidad Infantil en Línea (COPPA) en Estados Unidos han establecido estándares importantes, pero es necesario avanzar más allá (Federal Trade Commission, 2021).

El aumento de la conciencia pública y la sensibilización por la privacidad infantil también desempeñarán un papel crucial en la configuración de políticas más efectivas. Las organizaciones de defensa de los derechos de los niños y los grupos de padres deben continuar abogando por mejores prácticas y una mayor transparencia por parte de las empresas tecnológicas.

PERSPECTIVAS Y RECOMENDACIONES

Como experta en promover el uso seguro de internet y la ciudadanía digital, creo firmemente que la educación y la concientización son fundamentales para abordar los desafíos de la privacidad, la seguridad y la protección de datos de los niños, niñas y

adolescentes. A continuación, se presentan algunas perspectivas y recomendaciones:

- *Educación y empoderamiento desde una edad temprana:* es crucial comenzar a educar a los niños y adolescentes sobre la privacidad y la protección de datos desde una edad temprana. Deben comprender los riesgos y las implicaciones de compartir información personal en línea, así como las herramientas y estrategias para proteger su privacidad. La alfabetización digital tomará cada vez más relevancia en el futuro. La currícula educativa debe evolucionar para incluir la formación sobre privacidad de datos, ciberseguridad, la ética en el uso de la tecnología, incluso el pensamiento crítico. Los jóvenes deben contar con las herramientas y habilidades necesarias para navegar en el mundo digital de manera segura, consciente y responsable.
- *Involucrar a los padres, madres y cuidadores:* principalmente los padres y cuidadores, pero también los educadores, desempeñan un papel fundamental en la protección de la privacidad y los datos de los niños y adolescentes. Deben estar bien informados y recibir capacitación acerca de cómo supervisar y guiar a los jóvenes en el uso responsable de la tecnología en espacios como la Escuela para Padres con temas como Crianza Digital. Esa formación debe ser de manera constante para mantenerse informados sobre las amenazas digitales y las mejores prácticas de protección de datos. Otro aspecto importante a recalcar es fomentar una comunicación abierta y asertiva sobre las experiencias en línea de los jóvenes, que puede contribuir a crear un entorno de confianza y apoyo en el hogar.
- *Colaboración entre diferentes actores:* es necesaria una colaboración estrecha y articulada entre los gobiernos, las empresas tecnológicas, los centros educativos y las organizaciones de la sociedad civil para abordar de manera

efectiva los desafíos de la privacidad, seguridad y la protección de datos de los niños y adolescentes.

- *Regulaciones más estrictas y aplicación efectiva:* se deben establecer regulaciones más estrictas y mecanismos de aplicación efectivos para garantizar que las empresas tecnológicas cumplan con los estándares de privacidad y protección de datos para los niños, niñas y adolescentes. Esto podría incluir sanciones más severas por violaciones y la implementación de auditorías regulares.
- *Investigación y desarrollo de tecnologías de privacidad:* es necesario invertir en investigación y desarrollo de tecnologías de privacidad, como el cifrado de extremo a extremo, la privacidad de datos y las herramientas de control parental. Estas tecnologías pueden ayudar a proteger mejor los datos personales de los niños y adolescentes en línea.
- *Fomentar una cultura de privacidad y protección de datos:* debemos trabajar para fomentar una cultura en la que se valore y respete la privacidad y la protección de datos de los niños y adolescentes. Esto implica sensibilizar a la sociedad sobre la importancia de estos temas y promover prácticas responsables en todas las áreas, desde el hogar hasta las instituciones educativas y las empresas.
- *Uso de herramientas de seguridad, controles parentales y configuración de privacidad:* el uso de herramientas de control parental y configuraciones de privacidad es esencial para proteger a los menores en línea. Igualmente, los padres y madres deben familiarizarse con estas herramientas, utilizarlas de manera efectiva para restringir el acceso a contenido inapropiado, limitar la recopilación de datos personales y, en especial, conocer las funcionalidades de las aplicaciones que los menores descargan en sus dispositivos. Es importante actualizar regularmente los sistemas operativos, positivos celulares, aplicaciones y educar a los niños y adolescentes sobre la importancia de utilizar con-

traseñas seguras y de no compartir información personal con desconocidos.

REFLEXIONES SOBRE EL FUTURO

El futuro de la protección de datos y la privacidad infantil dependerá de nuestra capacidad, como sociedad, para adaptarnos a un entorno digital en constante cambio y de nuestra voluntad para priorizar la seguridad y el bienestar de los menores. A medida que la tecnología avanza, es probable que surjan nuevos desafíos y oportunidades. Por tanto, es esencial que continuemos educándonos y adaptando nuestras estrategias para proteger a los jóvenes de manera efectiva.

Papel de la Sociedad en la Protección de Datos: la sociedad en su conjunto desempeña un papel crucial en la protección de la privacidad de los menores. La colaboración entre padres, educadores, legisladores, empresas tecnológicas y organizaciones de defensa de los derechos de los niños es fundamental para crear un entorno digital seguro. La sensibilización pública y el activismo por la privacidad infantil pueden influir en la configuración de políticas más efectivas y en la implementación de mejores prácticas por las empresas tecnológicas.

Adaptación a nuevas realidades digitales: a medida que la tecnología continúa evolucionando, es probable que veamos cambios significativos en la manera en que se recopilan, almacenan y utilizan los datos personales. La aparición de nuevas tecnologías, como la realidad aumentada, la realidad virtual y el Internet de las Cosas (IoT), plantea nuevas consideraciones de privacidad. Es crucial que las futuras normativas aborden estos avances tecnológicos y establezcan estándares claros para la protección de los datos de los menores.

Importancia de la investigación y la innovación: la investigación continua en el campo de la protección de datos y la privacidad infantil es fundamental para identificar nuevas amenazas y desarrollar estrategias efectivas para mitigar los riesgos. Las instituciones académicas, los organismos gubernamentales y las organizaciones sin fines de lucro deben trabajar en conjunto para llevar a cabo estudios y compartir conocimientos sobre las mejores prácticas de seguridad digital. La innovación debe enfocarse en el desarrollo de herramientas y tecnologías que protejan de manera efectiva la privacidad de los menores.

REFLEXIÓN FINAL

La protección de datos, la seguridad y la privacidad de niños, niñas y adolescentes representa un desafío complejo que requiere un enfoque holístico. Como adultos cuidadores, debemos asumir la responsabilidad de educar y proteger a la niñez y adolescencia, mientras abogamos por políticas públicas y normativas que aseguren un entorno digital seguro. En un mundo donde la tecnología y el acceso a la información evolucionan rápidamente, los menores están cada vez más expuestos a una variedad de riesgos que pueden tener consecuencias duraderas en su bienestar y desarrollo. El futuro de la seguridad y la protección de datos dependerá de nuestra capacidad para adaptarnos a las nuevas tecnologías y de nuestra voluntad para priorizar la seguridad y el bienestar de niños, niñas y adolescentes.

Es imperativo que como adultos cuidadores asumamos la responsabilidad de educar y sensibilizar a los jóvenes sobre el uso seguro de internet y la importancia de proteger su información personal. La educación digital debe comenzar en el hogar y ser reforzada en las escuelas mediante programas integrales de ciudadanía digital. Además, es fundamental que los padres y educadores estén informados sobre las amenazas en línea y mantengan una comunicación abierta con los jóvenes sobre sus

experiencias digitales. La supervisión activa y el establecimiento de límites claros pueden ayudar a mitigar los riesgos, aunque es importante respetar la privacidad y fomentar la autonomía de los menores.

El uso de herramientas de control parental y de configuraciones de privacidad son esenciales para proteger a la niñez y adolescencia cuando usa internet. Los padres, madres y cuidadores deben familiarizarse con estas herramientas y utilizarlas de manera efectiva para restringir el acceso a contenido inapropiado (violento o pornográfico) y enseñar a limitar la recopilación y el acceso a sus datos personales. Es importante actualizar regularmente el *software* de seguridad y educar a los jóvenes sobre la importancia de utilizar contraseñas seguras y de no compartir información personal con desconocidos.

El futuro de la protección de datos de menores dependerá, en gran medida, de la evolución de las normativas y políticas a nivel global. Las legislaciones futuras deberán adaptarse a las nuevas tecnologías y asegurar que las empresas que manejan datos de menores implementen medidas de seguridad robustas. El aumento de la conciencia pública y el activismo por la privacidad infantil desempeñarán un papel crucial en la configuración de políticas más efectivas. Las organizaciones de defensa de los derechos de los niños y los grupos de padres deben continuar abogando por mejores prácticas y una mayor transparencia por las empresas tecnológicas.

CONCLUSIÓN

La protección de datos y la privacidad de niños, niñas y adolescentes es un desafío multifacético que requiere la colaboración de padres, educadores, legisladores y empresas tecnológicas. En un entorno digital cada vez más complejo, es primordial adoptar un enfoque proactivo para educar y proteger a los jóvenes.

En última instancia, la protección de datos y la privacidad de niños, niñas y adolescentes requiere un compromiso constante y una adaptación continua a las nuevas realidades digitales. Como adultos cuidadores, tenemos la responsabilidad de educar y proteger a los jóvenes, mientras abogamos por políticas y normativas que aseguren un entorno digital seguro. La colaboración entre todos los actores involucrados y la instrumentación de estrategias multifacéticas serán fundamentales para garantizar que los menores puedan navegar el mundo digital de manera segura y consciente.

La seguridad y la privacidad de los menores en el entorno digital no es sólo una responsabilidad individual, sino un esfuerzo colectivo que requiere la participación activa de toda la sociedad. Únicamente a través de la educación, la utilización de herramientas de seguridad efectivas, la evolución de las normativas y la innovación tecnológica ética, podremos proteger adecuadamente la privacidad de los niños, niñas y adolescentes en la era digital.

REFERENCIAS BIBLIOGRÁFICAS

- Comisión Federal de Comercio (2022). *Alertas al Consumidor 2022*. <https://consumidor.ftc.gov/alertas-para-consumidores/2022/05/tu-hijo-esta-usando-tecnologia-educativa-sigue-leyendo>.
- EU GDPR (2020). *Reglamento General de Protección de Datos (GDPR)*. <https://gdpr.eu/>.
- Fondo de las Naciones Unidas para la Infancia (UNICEF) (2017). *Resumen Estado Mundial de la Infancia 2017. Niños en un mundo digital*. <https://www.unicef.org/media/48611/file>.
- Livingstone, S., y Helsper, E. (2020). Balancing Opportunities and Risks in Teenagers' Use of the Internet: The Role of Online Skills and Internet Self-Efficacy. *New Media & Society*, 22 (8), pp. 1476-1493.
- Network Contagion Research Institute (2024). NCRI *Reports. Una pandemia digital: descubrir el papel de los "Yahoo Boys" en el auge de las redes sociales permitió la sextorsión financiera dirigida a menores*. https://networkcontagion.us/wp-content/uploads/Yahoo-Boys_1.2.24.pdf.

Organización Mundial de la Salud (OMS) (2022). *Global Status Report on Violence Prevention*. <https://www.who.int/teams/social-determinants-of-health/violence-prevention/global-status-report-on-violence-against-children-2020>.

U.S. Federal Trade Commission (2021). *Children's Online Privacy Protection Rule ("COPPA")*. *Regla de protección de la privacidad en línea de los niños*. <https://www.ftc.gov/current/title-16/chapter-I/subchapter-C/part-312>.

Privacidad en la era de la computación cuántica

OLIVIA ANDREA MENDOZA ENRÍQUEZ¹

Resumen

En las siguientes líneas se definirá la computación cuántica y el estado actual de los avances tecnológicos en este tema; asimismo, se analizará el impacto que los ordenadores cuánticos pueden tener al derecho a la privacidad, los factores de riesgo y los desafíos para garantizar el uso seguro de esta nueva tecnología desde la perspectiva de los Derechos Humanos.

Palabras clave: computadoras cuánticas, privacidad, gobernanza tecnológica, Estados Nación, corporaciones, derechos humanos.

Abstract

In the following lines, quantum computing and the current state of technological advances on this topic will be defined. Likewise, will be analyzed the impact that quantum computers can have on the right to privacy, what are the risk factors and the challenges to guarantee the safety use of this new technology from the perspective of human rights.

Keywords: quantum computers, privacy, technological governance, Nation States, corporations, human rights.

¹ Doctora en Derecho cuya línea de investigación es Derecho y Tecnología, profesora investigadora titular de la División de Estudios Jurídicos del Centro de investigación y Docencia Económicas (CIDE).

INTRODUCCIÓN

Cuando hablamos de fenómenos vertiginosos, como el desarrollo tecnológico, la Era Digital y la economía del conocimiento, casi siempre surge la necesidad de plantear estas reflexiones a la luz de derechos como el de la privacidad. Aunado a esto, está la creciente preocupación de acompañar los avances científicos con salvaguardas que garanticen los pocos espacios privados que aún subsisten en un mundo posmoderno.

Algunas posturas manifiestan el esfuerzo infructuoso para salvaguardar la privacidad, sobre todo a partir de la combinación de desarrollos tecnológicos, como la inteligencia artificial, las neurociencias y la computación cuántica. Por otro lado, otras posturas plantean la ingente necesidad de proteger y garantizar los espacios privados que aún quedan, considerando que este derecho no sólo ampara al individuo *per se* sino que permite la materialización de valores colectivos en una sociedad democrática.

Respecto del desarrollo tecnológico, hemos visto que, en los últimos años, la inteligencia artificial (en adelante IA), se hizo presente en todos los ámbitos de las personas, planteando desafíos legales importantes especialmente en torno a la información que necesita para funcionar. A esto se suma el surgimiento de nuevas supercomputadoras que procesan grandes cúmulos de información casi al instante, con lo que se inicia la era de los ordenadores cuánticos.

Así, actualmente, la computación cuántica tiene su foco de reflexión no sólo en las posibilidades que ofrece para almacenar y procesar información con una capacidad nunca antes vista por la humanidad, sino en la necesidad de analizar aquellas dimensiones en torno a la privacidad que, en términos de las características propias de este tipo de computación, serían imposibles de garantizar. Por ejemplo, tenemos las medidas de cifrado seguro en materia de seguridad informática que actualmente conocemos.

En las siguientes líneas, abordaremos algunas reflexiones necesarias en torno al derecho a la privacidad —un derecho configurado en un mundo analógico— y el desafío que supone tratarlo como salvaguarda de algunos derechos fundamentales en la era de los ordenadores cuánticos.

PRIVACIDAD Y COMPUTACIÓN CUÁNTICA

Cuando hablamos de computación cuántica, pareciera ser un concepto abstracto asociado al campo de las ciencias de la computación y la física; no obstante, al igual que el desarrollo tecnológico como fenómeno, tiene distintos abordajes.

Sin duda alguna, uno de éstos es desde el Derecho, especialmente desde la óptica de la privacidad; sin embargo, para mejor entendimiento del lector, antes de entrar al campo jurídico, es necesario definir en qué consiste, en términos generales, la computación cuántica.

En este sentido, una definición amplia es que la computación cuántica utiliza tecnología especializada, incluido el *hardware* informático y los algoritmos que usan la mecánica cuántica, para resolver problemas complejos que las computadoras clásicas o las supercomputadoras no pueden resolver, o no pueden hacerlo lo suficientemente rápido (IBM, sf).

Esta rama de la informática se basa en los principios de la superposición de la materia y el entrelazamiento cuántico para desarrollar una computación distinta a la tradicional. En teoría, sería capaz de almacenar muchísimos más estados por unidad de información y operar con algoritmos mucho más eficientes a nivel numérico, como el de Shor o el temple cuántico (Iberdrola, sf).

Estamos frente a un nuevo paradigma que revolucionará no sólo la computación tradicional sino las posibilidades de usos y aplicaciones de los ordenadores cuánticos —sin dejar de considerar que la democratización de esta tecnología es uno de los

desafíos que se vislumbran en un mundo de grandes desigualdades—.

En términos prácticos, al estar frente a una nueva generación de supercomputadoras, la capacidad de rendimiento, procesamiento y almacenamiento será casi infinita por lo que su uso traerá nuevas posibilidades en diversos sectores: finanzas, economía, movilidad, transporte.

Como se habrá podido adelantar, en toda esta revolución tecnológica, la información será un insumo indispensable para alcanzar el máximo beneficio del uso de los ordenadores cuánticos. Este máximo rendimiento computacional, sumado a un mundo hiperconectado nos lleva a pensar que los espacios privados serán casi inexistentes en un futuro no lejano. Las personas se han convertido en sensores humanos que reportan a un conjunto de corporaciones globales todo tipo de información: financiera, hábitos de alimentación, ejercicio, salud, movilidad, gustos y preferencias, consumo, etcétera.

Por otro lado, un elemento importante que nos introduce a estudiar la computación cuántica desde el derecho a la privacidad es el de la ciberseguridad. En este rubro, hoy día conocemos sistemas de cifrado seguro que hacen posible el procesamiento de información de manera segura al utilizar sistemas de encriptación casi infinitos, los cuales a una computadora tradicional le tomaría muchos años descifrar. No obstante, si estamos entonces frente al máximo rendimiento computacional, aquellas “cerraduras digitales” serán abiertas con facilidad y casi en tiempo real.

Lo descrito también supone una nueva dimensión de estudio para garantizar la ciberseguridad, que algunos expertos han situado en tres categorías: criptografía cuántica, nuevos algoritmos de encriptación y detección de intrusiones cuánticas (Guillén y Navarro, 2006).

Entrando al tema de los ordenadores cuánticos vistos desde el derecho a la privacidad, es pertinente decir que estamos frente a

fenómenos donde las categorías jurídicas tradicionales no alcanzan para proteger y brindar certeza jurídica a las personas, por ejemplo, la falta de desarrollo normativo sobre el derecho a la privacidad mental, el derecho a no ser sometidos a decisiones automatizadas o el derecho de reconsideración frente a las decisiones adoptadas por IA que afecten los Derechos Humanos, sin duda alguna, figuras jurídicas que harían más factible un uso seguro de tecnologías como las neurociencias, la IA y la computación cuántica.

Otro elemento indispensable para abordar el derecho a la privacidad en los ordenadores cuánticos tiene que ver con estas corrientes propuestas desde la *lex mercatoria*, que plantean comercializar los datos de las personas a través de pagos como contraprestación por la explotación del dato en la economía digital. Este tipo de posturas llevan a pensar que la privacidad queda en un segundo término, siempre que exista un beneficio tangible para el titular del dato y que éste consienta el tratamiento. En opinión de la autora, a largo plazo esto traería como consecuencia una sobremercantilización de la información de carácter personal (más de lo que ya se da), una reducción del concepto “de lo privado” y por encima del individuo —de manera colectiva—, un debilitamiento de la vida democrática de los países.

Estos procesos han dado lugar a un modelo de sociedad que se ha impuesto en las últimas décadas: la llamada “sociedad del conocimiento”, donde la generación de riqueza estaría principalmente basada en el control y el desarrollo de nuevas formas de producción y aprovechamiento del conocimiento (UNAM, 2023).

No obstante, otras posturas —sobre todo aquéllas formuladas desde los derechos humanos— plantean el derecho a la privacidad como un tesoro, primero colectivo y segundo como un derecho fundamental que permite establecer límites al desarrollo tecnológico, pensando en la dignidad humana como eje y límite natural para la innovación.

Ahora bien, no se está planteando la idea de detener el inminente desarrollo de los ordenadores cuánticos, sino de trabajar desde las instituciones, desde la política pública, los ordenamientos constitucionales, los Derechos Humanos y desde los Estados en general, mecanismos que garanticen que, en un futuro no lejano, una máquina no decida las personas candidatas a vivir o a morir, las personas que deben o no recibir un préstamo bancario o las personas que deban recibir una donación de órganos; es decir, no se puede romantizar el desarrollo tecnológico sin hablar, por ejemplo, de la falta de supervisión estatal sobre los sistemas de IA que trabajan en campos tradicionalmente regulados (sector financiero), o la falta de mecanismos que garanticen la transparencia algorítmica o incluso la falta de entidades público-privadas que auditen los sistemas desde un enfoque preventivo, lo cual permitiría salvaguardar los Derechos Humanos de las personas.

Por otro lado, el derecho a la privacidad —que cobra vida a través pero no exclusivamente, del derecho a la protección de datos personales—, aplicado a la tecnología, también se ha enfrentado al debate teórico-doctrinario sobre si los Derechos Humanos tradicionales son suficientes para proteger a las personas, como un principio espejo, como sostiene Pérez Luño (2012), o si, por el contrario, estamos frente a la necesidad de construir nuevas figuras legales que protejan a la persona frente al desarrollo tecnológico y, por ende, permitan el uso seguro de la tecnología.

Como adelantamos, parece que estamos frente a la configuración de figuras legales que den vida al derecho a la privacidad mental, a no ser sometidos a decisiones automatizadas y a solicitar la intervención humana, en caso de errores en las decisiones tomadas por las máquinas.

Aunque no es objetivo de este apartado, aquí el rol de la transparencia, la trazabilidad y la auditoría algorítmica en los sistemas será indispensable para garantizar derechos como la no discriminación de las personas.

ACTORES EN EL DESARROLLO DE ORDENADORES CUÁNTICOS E IMPACTO A LA PRIVACIDAD

Cuando hablamos de la naturaleza de las computadoras cuánticas, los beneficios y aplicaciones, pensaríamos que su desarrollo debe estar en manos de los Estados para garantizar un equilibrio para la democratización de estas tecnologías; sin embargo, no es así.

En la carrera por el desarrollo de ordenadores cuánticos, participan unos pocos actores que son en su mayoría corporaciones con montos altos de inversión a través de fondos privados y cuya representación geográfica se concentra mayoritariamente en Estados Unidos de América y China.

Autores como Jeutner indican que existe el riesgo de que el Norte global de alta tecnología obtenga una ventaja estratégica significativa, mientras que otras naciones caen en la “pobreza cuántica” (Jeutner, 2021, pp. 52-59).

Algunos ejemplos de la carrera por desarrollar los ordenadores cuánticos más potentes son:

- *La computadora cuántica de Google*: la última versión utiliza el procesador cuántico *Sycamore* de 70 qubits, lo que representa un salto sustancial de los 53 qubits de su versión anterior; es aproximadamente 241 millones de veces más robusto que el modelo anterior y capaz de resolver instantáneamente las tareas que el resto de superordenadores actuales tardarían unos 47 años en completar (Romero, 2023).
- *La computadora cuántica JiuZhang 3 de la Universidad de Ciencia y Tecnología de China en Hefei*: es capaz de solucionar un complicadísimo problema matemático en una millonésima de segundo, un cálculo para el que el superordenador más rápido del mundo hubiera empleado 20,000 millones de años. Los resultados de esta computadora superan los logros del ordenador cuántico de Google. El *JiuZhang* pertenece a

los computadores cuánticos fotónicos, que es diferente a la tecnología de cúbits superconductores como los de Google o IBM (La Cour, 2023).

- IBM: la compañía tecnológica anunció un nuevo avance publicado en la portada de la revista científica *Nature*, que demuestra, por primera vez, que los computadores cuánticos pueden producir resultados precisos a una escala de más de 100 qubits, superando los principales enfoques clásicos (IBM, sf).

Una vez que se han identificado a los actores principales en el desarrollo de ordenadores cuánticos, se pueden conocer los intereses y objetivos corporativos que, en muchos de los casos, plantean dilemas entre el desarrollo tecnológico, las políticas para democratizar su uso, y las garantías sobre el respeto a la dignidad humana.

Frente a estos dilemas, Valenti Jeutner afirma:

...las decisiones relativas al diseño de la tecnología nunca son neutrales porque, por necesidad, están teñidas por los valores, las convicciones de los desarrolladores y por el contexto histórico y social en el que se insertan. Por tanto, plantea un concepto que denomina el *imperativo cuántico*, el cual establece que los reguladores y desarrolladores deben asegurar que el desarrollo de las computadoras cuánticas:

- No creen ni exacerben las desigualdades.
- No socaven la autonomía individual ni datos personales;
- No se produzcan sin consultar a aquellos cuyos intereses afectan (Jeutner, sf).

Sin duda alguna, la computación cuántica permitirá grandes beneficios para algunos actores (aquellos que puedan acceder a estas tecnologías) y la lógica que impera en su desarrollo a través de las corporaciones es la eficiencia y la eficacia; sin embargo, surge la necesidad de articular un discurso para el desarrollo y el uso de los computadores cuánticos desde los derechos humanos (en el que los conceptos de eficacia y eficiencia no sean el objetivo primario y único a alcanzar), porque ello garantizará la propia subsistencia humana.

En otras palabras, si bien son indispensables los fondos privados para el desarrollo de los ordenadores cuánticos, este camino sin la participación, rectoría y/o liderazgo de los Estados Nación e instituciones supranacionales, puede derivar en un desequilibrio que impida la democratización de este tipo de tecnologías, por lo que prácticamente se acentuarán las desigualdades preexistentes en el mundo físico: países desarrollados a la luz de países en vías de desarrollo y ciudadanos conectados a la luz de la población mundial que no tiene acceso a las tecnologías; es decir, brechas y desigualdades económicas, manifestadas no sólo a través de acceso o no, a los ordenadores cuánticos, sino a las posibilidades que éstos brindan a quienes puedan acceder a ellos, como, por ejemplo, ciudadanos que en un futuro puedan acceder a la cura de enfermedades complejas, como el Parkinson, donde las neurociencias se acercan a dar respuesta contundente a enfermedades otrora sin remedio.

Esto permite sin duda vislumbrar la necesidad de hacer un llamado a los Estados Nación para revertir el fenómeno de reducción que han experimentado en los últimos años, donde los actores principales que dirigen la agenda digital son los actores corporativos y en el cual los Estados se limitaron a ser observadores incapaces de garantizar el escrutinio en materia de derechos humanos.²

² Por ejemplo, el Consejo Asesor de Contenido de Meta tiene funciones que sustituyen en algunos casos particulares a los jueces —necesarios para el derecho continental en el marco de los estados constitucionales de derecho—; es decir, tenemos a actores privados determinando contenidos que deben permanecer o ser removidos de esta plataforma digital, lo cual, por ejemplo, para algunos derechos de la infancia, podría ser una medida inmediata de protección a niños, niñas y adolescentes en el ciberespacio (pensando, por ejemplo, en imágenes que afecten la dignidad de la infancia), pero que, por otro lado, en casos generales podría derivar en mandarar la restricción del ejercicio de derechos humanos como el de acceso a la información, el cual para el sistema legal mexicano sólo puede ser restringido por un juez.

En esta tesitura, el grupo de países que conforman el denominando G7,³ hizo en mayo del 2023 un llamado a los Estados a ejercer un liderazgo sobre la regulación en materia de IA,⁴ al determinar que no tiene que ver con eficacia y eficiencia del mercado a partir de la explotación de los datos, sino con una necesidad de garantizar cuestiones, como la democracia, la privacidad y, en algunos casos, la subsistencia misma de la humanidad. En octubre del mismo año, el G7 anunció un Código de Conducta Internacional, cuyo objetivo es minimizar los riesgos en materia de IA y los principios rectores internacionales para los desarrolladores de IA. A pesar de que este instrumento no es vinculante y sólo tiene carácter de orientador, es un paso importante para visibilizar la necesidad de que las discusiones del rumbo de la IA deben articularse desde lo público, porque los efectos afectarán o beneficiarán a los individuos de forma colectiva.

Para llegar a este consenso, prácticamente se plantearon tres posturas:

- Estados Unidos de América planteó la idea, proveniente de la teoría económica *laissez faire*, en la cual la rectoría del Estado cede frente al mercado y permite que sea éste el que imponga las reglas a través de la autorregulación.
- La Unión Europea propuso la necesidad de una regulación ética, en consonancia con sus propias normas comunitarias sobre IA, sobre la privacidad y protección de datos personales y, en general, sobre Derechos Humanos. En este modelo, la dignidad humana es el límite natural de cualquier avance científico.

³ Los países que conforman este grupo son: Alemania, Canadá, Estados Unidos, Francia, Italia, Japón y Reino Unido.

⁴ A pesar de que el objetivo de este trabajo no es analizar la privacidad en la IA, este fenómeno político nos permite identificar los próximos pasos para regular la computación cuántica y las posibles vías para articular el liderazgo que fortalezca a los Estados Nación.

- Japón formuló el Proceso de Hiroshima sobre IA, una propuesta más laxa que la de los países de la UE, pero que aborda cuestiones como la protección de los datos personales o los derechos de autor. Esta postura fue finalmente la que se impuso sobre las dos previas. El marco político global del proceso de Hiroshima consta de cuatro pilares: análisis de los riesgos prioritarios, los retos y las oportunidades de la IA generativa, los Principios Rectores Internacionales del Proceso de Hiroshima para todos los agentes de la IA en el ecosistema de la IA, un código de conducta internacional del Proceso de Hiroshima para las organizaciones que desarrollan sistemas avanzados de IA, y cooperación basada en proyectos en apoyo del desarrollo de herramientas y mejores prácticas de IA responsables (Declaración de los dirigentes del G-7 sobre el proceso de la IA de Hiroshima, sf).

Por otro lado, también se destaca la reciente intervención histórica del papa Francisco en el debate sobre IA en la cumbre del G7, llevada a cabo en Italia en junio de 2024, haciendo un llamado para que el desarrollo de la IA esté al servicio de la humanidad. De igual forma, el Papa ha expresado su preocupación sobre la posibilidad del surgimiento de una *dictadura tecnológica*, si no se establece una regulación suficiente y ha hecho un llamado a un tratado internacional vinculante para prevenir las prácticas perjudiciales para las personas y fomentar las que sean mejores.⁵

⁵ Esto, recordando que en 2023 la imagen del Papa fue utilizada por una IA generativa que creó fotografías falsas (*deep fake*) en las que se podía ver al Pontífice vistiendo atuendos extravagantes. A esto se debe sumar que el Vaticano designó al padre Paolo Benanti como experto para los debates sobre el desarrollo y rumbo de la IA. Horowitz (5 de junio de 2024). <https://www.nytimes.com/es/2024/02/17/espanol/fraile-inteligencia-artificial-vaticano.html>.

Como se ha visto, existe cada vez una preocupación mayor por parte de actores no convencionales para regular avances científicos que puedan poner en riesgo los derechos de las personas de manera colectiva. Se advierte una disparidad entre las capacidades y los hallazgos a los que han llegado algunas corporaciones con proyectos de computación cuántica vigentes, y la participación del Estado frente a los planes de ciencia y tecnología nacionales, las políticas públicas y la regulación; es decir, estamos frente a una tecnología disruptiva que romperá muchos paradigmas y cuyo eje decisonal —hasta el momento— está mayoritariamente en manos del mercado. Esto se agrava cuando se manifiestan fenómenos, como el de los países periféricos que se convierten en sólo espectadores y consumidores de tecnologías obsoletas en otras latitudes del mundo que paradójicamente comercializan estos productos.

Una vez complejizado el problema, es evidente que el desarrollo de ordenadores cuánticos sin reglas claras, incidirá en la salvaguarda de varios derechos humanos que pueden ir desde el derecho a la no discriminación hasta derechos como la propia vida, a la protección de datos personales y a la privacidad.

LA PRIVACIDAD SÍ IMPORTA

El título de este apartado pareciera una obviedad cuando pensamos en una sociedad hiperconectada que reduce a las personas a sensores que reportan datos en tiempo real a corporaciones dueñas de tecnologías que “simplifican la vida”; sin embargo, de lo expuesto en apartados previos se advierte la necesidad de hablar de los ordenadores cuánticos, reconociendo la importancia de derechos, como la privacidad, con nuevos enfoques que realmente permitan garantizar espacios privados para las personas.

En el mundo ciber-físico posdigital, existe una excesiva dependencia de la protección de datos y de los marcos de privacidad centrados en los datos como herramienta fallida para la gobernanza

tecnológica. Cada vez estamos más expuestos y vulnerables frente al poder privado en constante expansión, sostenido en parte, por el trato excepcional dado a las empresas tecnológicas. Este poder debe ser controlado. Este enfoque implica identificar los límites de la ratificación y la interpretación, imponer límites normativos, incluso mediante límites a los mercados y definir las reglas de la ratificación permisible. Por lo anterior, es necesario regresar a las conceptualizaciones originales del derecho a la privacidad y protección de datos personales, basada en derechos humanos, previo a que dieran un giro a las TIC; es decir, a un marco basado en proteger a las personas en lugar de garantizar la privacidad o seguridad de los datos (Renieris, 2023):

El ecosistema de la Red exige una noción amplia de privacidad como derecho, comprensiva de conceptos como los de intimidad, confidencialidad, seguridad, protección de datos e identidad (Barrio, 2018).

Una de las preguntas necesaria entonces es ¿por qué vale la pena proteger la privacidad?. En este sentido, Simitis reconocía que la privacidad no es un fin en sí mismo. es un medio para conseguir un determinado ideal de política democrática en la que se confía en que los ciudadanos sean más que sólo proveedores acríticos de información a tecnócratas que todo lo ven y todo lo optimizan.

Quando se dismantela la privacidad, tanto la oportunidad de evaluar el proceso político por uno mismo, como la oportunidad de desarrollar y mantener un estilo de vida concreto se desvanecen.⁶

⁶ Spiros Simitis, principal estudioso y practicante de la privacidad en Alemania —en aquel momento era el Comisario de Protección de Datos del *land* de Hesse—, daba una conferencia ante la Facultad de Derecho de la Universidad de Pennsylvania (Estados Unidos). Su discurso exploraba exactamente el mismo tema que preocupaba a Baran: la automatización del procesado de datos. Pero Simitis no perdía de vista la historia del capitalismo y la democracia, así que veía los cambios tecnológicos bajo una luz mucho más ambigua, MIT (10 de junio de 2024). <https://www.technologyreview.es/s/3837/el-verdadero-problema-de-la-privacidad-una-contradiccion-tolerada>

Otro elemento a destacar es la privacidad como un derecho de las personas y como herramienta para garantizar otros derechos colectivos y la democracia en las sociedades modernas. Ejemplos como *Cambridge Analytica* explican esta afirmación.

En este punto, Simitis expresó una idea auténticamente revolucionaria que se ha perdido en los debates contemporáneos sobre la privacidad: “no se puede lograr ningún progreso, mientras la protección de la privacidad se equipare, más o menos, con el derecho del individuo a decidir cuándo y qué datos son accesibles”. La trampa en la que caen muchos defensores bienintencionados de la privacidad es creer que con que pudieran dar al individuo un mayor control sobre sus datos —mediante leyes más fuertes o un régimen de propiedad robusto— el alambre de espino invisible se volvería visible y se rompería. No lo hará, no si esos datos se acaban devolviendo a las propias instituciones que erigen el alambre a nuestro alrededor (Morozov, sf).

DESAFÍOS PARA GARANTIZAR LA PRIVACIDAD EN UN MUNDO POSMODERNO DE ORDENADORES CUÁNTICOS

Estamos en una etapa temprana de desarrollo de los ordenadores cuánticos, por lo que los desafíos se modificarán a medida que se logren nuevos hallazgos en el este tecnológico.

Hasta el momento, es importante destacar la necesidad de partir del análisis de la privacidad en su dimensión de derecho humano y en su dimensión de instrumento político para mantener otros valores sociales como la democracia. Los espacios privados son necesarios para mantener intacta la capacidad de reflexión crítica y de pensamientos propios, sin entregarle esta posibilidad a los algoritmos, a la IA o a los ordenadores cuánticos, y, por ende, a las corporaciones detrás de estos servicios o productos.

Otro de los desafíos tiene que ver con la necesidad de garantizar la democratización de los computadores cuánticos y esto, a pesar de parecer a simple vista un factor de índole política, le abre al Derecho un campo de acción importante a través de acuerdos supranacionales que articulen la obligatoriedad de estándares mínimos para el uso seguro de tecnologías disruptivas como la IA, los ordenadores cuánticos y las neurociencias.

Como vimos en algunos ejemplos de ordenadores cuánticos, parte del problema para su desarrollo y democratización son las condiciones que requieren estas supercomputadoras para funcionar y, salvo la propuesta de China, el resto de ordenadores cuánticos requieren actualmente temperaturas muy bajas (casi imposibles de lograr) para cumplir con su función, y para hacer esto posible, se está generando un impacto en el medio ambiente, en términos de recursos como el agua y la energía necesaria para alcanzar esas temperaturas.

Por otro lado, el foco deberá estar en la maximización de beneficios tecnológicos sin sacrificar el respeto a los derechos de las personas en todas sus expresiones. Esto exige un fuerte trabajo para el desarrollo de políticas de ciencia y tecnología encaminadas a lograr una menor dependencia tecnológica, ejercer el liderazgo regional, el desarrollo de regulación acorde a los derechos de las personas, y la presencia del Estado para definir el camino que se trace para la computación cuántica.

En este sentido, el Estado no puede seguir obviando lo que sucede desde la ubicuidad tecnológica y tendrá que ejercer un papel más activo que permita la salvaguarda de los Derechos Humanos.

Se puede concluir que estos dilemas descritos no se agotan o resuelven únicamente desde la lógica del Derecho, pues muchos de ellos deben ser abordados como dilemas éticos; hemos visto que hasta ahora y, en muchos casos, el bien común cede frente al mercado.

¿Quién decidirá si la privacidad importa en la era de los ordenadores cuánticos?...

REFERENCIAS BIBLIOGRÁFICAS

- Barrio Andrés, Moisés (2018). *Ciberderecho. Bases estructurales, modelos de regulación e instituciones de gobernanza de internet*. Tirant lo Blanch, p. 89.
- Declaración de los dirigentes del G-7 sobre el proceso de la IA de Hiroshima (sf). <https://digital-strategy.ec.europa.eu/es/library/g7-leaders-statement-hiroshima-ai-process>.
- Guillén, E. P., y Navarro Gasca, J. J. (2006). Sistema de distribución de claves mediante criptografía cuántica para evadir ataques del tipo “*Man in the middle*”. *Ciencia e Ingeniería Neogranadina*, 16(2), pp. 64-73. <https://doi.org/10.18359/rcin.1235>.
- Horowitz, Jason (2024). El fraile que se convirtió en el especialista en inteligencia artificial del Vaticano. *New York Times*. <https://www.nytimes.com/es/2024/02/17/espanol/fraile-inteligencia-artificial-vaticano.html>.
- Iberdrola (sf). *La computación cuántica y las supercomputadoras que revolucionarán la tecnología*. <https://www.iberdrola.com/innovacion/que-es-computacion-cuantica>.
- IBM (2023). El ordenador cuántico de IBM demuestra el siguiente paso para ir más allá de la supercomputación clásica. <https://es.newsroom.ibm.com/announcements?item=122773>.
- IBM (sf). *¿Qué es la computación cuántica?*. <https://www.ibm.com/mx-es/topics/quantum-computing>.
- Jeutner, Valentin (2021). The Quantum Imperative: Addressing the Legal Dimension of Quantum Computers. *Morals & Machines*, 1 (1), pp. 52-59. <https://ssrn.com/abstract=3820003>.
- La Cour, Brian (2023). Advances in Quantum Computing. *Entropy* 25, no. 12: 1633. <https://doi.org/10.3390/e25121633>.
- Morozov, Evgeny (sf). *El verdadero problema de la privacidad: una contradicción tolerada*. <https://www.technologyreview.es/s/3837/el-verdadero-problema-de-la-privacidad-una-contradiccion-tolerada>.
- Pérez Luño, Antonio Enrique (2012). *Los derechos humanos en la sociedad tecnológica*. Universitas.
- Renieris, Elizabeth (2023). *Beyond Data. Reclaiming Human Rights at the Dawn Metaverse*. MIT Press, 149p.

Romero, Sarah (sf). El nuevo ordenador cuántico de Google alcanza la supremacía cuántica. *Muy Interesante*, <https://www.muyinteresante.com/actualidad/60875.html>.

UNAM (sf). *Estudios filosóficos y sociales sobre ciencia y la tecnología*. UNAM. <https://posgrado.unam.mx/filosofiadela-ciencia/programa/campos/estudios-filosoficos-sociales-ciencia-tecnologia.html>.

Panorama de la regulación del derecho a la protección de datos personales en México ante la era digital

LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ¹

Resumen

La era digital en México ha llegado para intensificar el uso de múltiples herramientas tecnológicas, planteando desafíos para la protección de los datos personales. Si bien en el país se cuenta con un marco normativo sólido para garantizar la privacidad de las personas, las nuevas tecnologías han supuesto retos para esta regulación. En el presente capítulo se realizará un breve repaso sobre el estado actual que guarda la regulación de la protección de datos personales en algunos de estos temas, como son el derecho a la protección de niñas, niños y adolescentes; la inteligencia artificial; los neuroderechos; la ciberseguridad y la violencia digital.

Abstract

The digital era in Mexico has arrived to intensify the use of multiple technological tools, posing challenges for the protection of personal data. Although the country has a solid regulatory framework to ensure people's privacy, new technologies have presented challenges for this regulation. This chapter will provide a brief overview of the current state of personal data protection regulation in some of these areas, such as the right to the protection of children and adolescents; artificial intelligence; neuro-rights; cybersecurity; and digital violence.

¹ Tiene estudios doctorales en Administración Pública y maestría en Gestión Pública Aplicada, es licenciada en Ciencia Política por el ITAM. Actualmente es Comisionada Ciudadana del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, desde donde coordina el Área de Protección de Datos Personales.

Palabras clave: México, protección de datos personales, marco normativo, inteligencia artificial, violencia digital.

Keywords: Mexico, personal data protection, regulatory framework, artificial intelligence, digital violence.

INTRODUCCIÓN

Nos encontramos indiscutiblemente en una era caracterizada por la intensificación del uso de herramientas tecnológicas, en la que el Internet se ha convertido en una herramienta utilizada por la mayoría de la población y en la que, particularmente a través de las redes sociales, el intercambio de información, así como los datos que compartimos en la esfera digital, también se han acrecentado de manera exponencial.

Naturalmente, este escenario, presentado a escala global, se ha hecho latente en México, donde la población usuaria de internet ha incrementado de manera importante. De acuerdo con datos de la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH), dada a conocer por el INEGI, en 2022, 93.1 millones de personas usaron internet, es decir, el 78.6 por ciento de la población mexicana de seis años o más.

Asimismo, a escala nacional el 68.5 por ciento de los hogares en México contaba con acceso a internet y el 97 por ciento de las personas usuarias utilizó un *smartphone* como medio más frecuente para conectarse a la red. Además, el 90.9 por ciento de la población usuaria de teléfono inteligente reportó que utiliza aplicaciones de mensajería instantánea, seguido del 78.6 por ciento que reportó haber ingresado a redes sociales.

Esta realidad, sumada a la aparición de nuevas tecnologías, herramientas y desafíos que plantea la intensificación del uso de las tecnologías, ha planteado retos para la regulación del derecho a la protección de datos personales en nuestro país. El objetivo del presente capítulo será realizar un breve repaso

sobre el estado actual que guarda la regulación de la protección de datos personales en algunos de estos temas, como son el derecho a la protección de niñas, niños y adolescentes; la inteligencia artificial; los neuroderechos; la ciberseguridad y la violencia digital.

MARCO NORMATIVO MEXICANO

La protección de datos personales en México está respaldada por un sólido marco normativo que busca garantizar la privacidad y seguridad de la información personal de la sociedad. En el artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos (CPEUM), se reconoce el derecho fundamental a la protección de datos personales, así como el reconocimiento de los derechos de acceso, rectificación, cancelación y la oposición de éstos.

Sumado a lo anterior, el 5 de julio de 2010 se publicó la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (LFPDPPP) (Cámara de Diputados del H. Congreso de la Unión, 2010), la cual regula el tratamiento de datos personales por parte de personas físicas o morales privadas. Esta ley establece principios y deberes que los entes privados deben seguir para la garantía de los derechos en cuestión.

Además, el 26 de enero de 2017 se publica la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados (LGPDPPSO) (Cámara de Diputados del H. Congreso de la Unión, 2017) que establece las bases, los principios y los procedimientos necesarios para la garantía de la protección de datos personales en posesión de sujetos obligados del sector público. Esta ley aplica a cualquier autoridad, entidad, órgano y organismo de los poderes ejecutivo, legislativo y judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos.

Como se advierte, en México un robusto marco jurídico regula el tratamiento de los datos personales, tanto en el sector privado como el público, estableciendo principios, deberes y obligaciones para garantizar la privacidad y el adecuado tratamiento de la información personal, marco normativo vigilado y aplicado por autoridades especializadas y autónomas, como el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales, para el sector público federal y para el privado, así como los 32 organismos garantes locales en las entidades del país.

EL DERECHO A LA PROTECCIÓN PARA NIÑAS, NIÑOS Y ADOLESCENTES

Según la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares 2022, el 92.4 por ciento de las personas entre 12 a 17 años son personas usuarias de internet (Instituto Nacional de Estadística y Geografía, 2022), representando un aumento significativo desde la pandemia. Por ello, este grupo se vuelve cada vez más una población vulnerable, como resultado de una mucha mayor interacción en redes sociales, pero con la misma protección, lo que los sitúa cada vez en mayores posiciones de riesgo.

Esta vulnerabilidad se muestra en el hecho de que, según datos del Estudio Nacional sobre Violencia Digital contra la Niñez, se han incrementado los diferentes tipos de violencia digital hacia este grupo (Hurtado, sf). De acuerdo con el Sistema Nacional de Protección Integral de Niñas, Niños y Adolescentes, el 22 por ciento de las personas pertenecientes a esta población en México ha sido víctima de conductas negativas a través de las tecnologías digitales.

En ese sentido, las leyes referidas en materia de protección de datos personales aplican a todas las personas, incluyendo niñas, niños y adolescentes; sin embargo, la Ley General de los Derechos de Niñas, Niños y Adolescentes (LGDNNA) también

establece disposiciones específicas para la protección de datos personales de los menores de edad. En esta ley se reconoce el derecho a la intimidad personal y familiar, así como el derecho de protección de los datos personales de las niñas, niños y adolescentes. Además, prohíbe cualquier injerencia arbitraria o ilegal en la vida privada de los menores, así como la divulgación ilícita de su información personal,² y reconoce que cualquier manejo de datos personales debe atender al interés superior del menor.³ Por demás, la LGPNNa establece en su artículo 101 bis 2 que las niñas, niños y adolescentes tienen el derecho al acceso y uso seguro de internet.

Sin embargo, esta ley no cuenta con mecanismos específicos que acoten la violencia digital o para la protección de este grupo de la población. En ese sentido, entre otras iniciativas, la Comisión de Derechos de la Niñez y Adolescencia de la Cámara de Diputados ha avalado un dictamen del proyecto de decreto por el cual se adiciona el artículo 101 bis 3 a la referida ley en materia de acceso a internet libre de violencia contra niñas, niños y adolescentes, reconociendo al internet y las redes sociales como

² Artículo 76. Niñas, niños y adolescentes tienen derecho a la intimidad personal y familiar, y a la protección de sus datos personales. Niñas, niños y adolescentes no podrán ser objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia; tampoco de divulgaciones o difusiones ilícitas de información o datos personales, incluyendo aquella que tenga carácter informativo a la opinión pública o de noticia que permita identificarlos y que atenten contra su honra, imagen o reputación. [...]

³ Artículo 77. Se considerará violación a la intimidad de niñas, niños o adolescentes cualquier manejo directo de su imagen, nombre, datos personales o referencias que permitan su identificación en los medios de comunicación que cuenten con concesión para prestar el servicio de radiodifusión y telecomunicaciones, así como medios impresos, o en medios electrónicos de los que tenga control el concesionario o medio impreso del que se trate, que menoscabe su honra o reputación, sea contrario a sus derechos o que los ponga en riesgo, conforme al principio de interés superior de la niñez.

espacios de amenaza para esta población, a fin de garantizar la seguridad cibernética y proteger los derechos de la infancia al usar estos medios.

INTELIGENCIA ARTIFICIAL

Por otro lado, la intensificación tecnológica ha traído consigo la aparición de nuevas herramientas cuyo uso se ha amplificado y que nos obligan a plantearnos una eventual regulación de los potenciales efectos de dichas materias. Uno de estos temas es, indudablemente, la inteligencia artificial.

En México, se han llevado a cabo esfuerzos para abordar la regulación de dicha materia, desde la Estrategia de Inteligencia Artificial MX presentada en 2018, que delineó cinco áreas de acción para el gobierno mexicano: gobierno y servicios públicos; datos e infraestructura digital; investigación y desarrollo; capacidad, habilidades y educación; y ética y reglamentación.

Dicha estrategia incluyó iniciativas como el desarrollo de un marco de gobernanza, mapeo de usos y necesidades en la industria, impulso al liderazgo internacional, publicación de recomendaciones y colaboración con expertos y ciudadanos. No obstante, debido a las transiciones políticas el proyecto no tuvo continuidad.

Hasta el momento, se han presentado 33 iniciativas de ley en el Congreso mexicano relacionadas con la inteligencia artificial, 21 en la Cámara de Diputados y 12 en el Senado de la República, aparte de dos reformas constitucionales en la materia.

El 20 de abril de 2023 el Senado de la República presentó la Alianza Nacional de Inteligencia Artificial (ANIA), con el propósito de fortalecer la IA en México basada en Derechos Humanos, colaboración e interoperabilidad ética, inclusiva y multidisciplinaria. Esta alianza ha generado una iniciativa de reforma constitucional para facultar al Congreso para legislar sobre esta materia, así como sobre ciberseguridad y neurodere-

chos. Al mismo tiempo, se hizo hincapié en la promoción de la educación sobre los riesgos de la IA y el fomento de una cultura de innovación, además de poner énfasis en el cumplimiento de derechos fundamentales en el uso de la tecnología.

Entre las otras propuestas que se han presentado, destaca la iniciativa que plantea reformar la fracción decimoséptima del artículo 73 de la Constitución, con el objetivo de facultar al Congreso de la Unión a emitir las normas necesarias que regulen la investigación, el desarrollo y las aplicaciones de la inteligencia artificial.

Por parte de la Cámara de Diputados, se han presentado diversas iniciativas en esta materia; es de destacarse la iniciativa presentada en mayo de 2023, con el objetivo de expedir la Ley de Regulación Ética de la Inteligencia Artificial y la Robótica, la cual intenta regular el uso de estas tecnologías en diversas áreas como el gobierno, la economía, el comercio, la administración, la comunicación y las finanzas, basándose en principios éticos y legales. Asimismo, propone establecer lineamientos de políticas públicas para regular éticamente el uso de la IA y la robótica en México, respetando los Derechos Humanos y la igualdad de género. Incluye la creación del Consejo Mexicano de Ética para la Inteligencia Artificial y la Robótica, así como la Red Nacional de Estadística de Uso y Monitoreo de la IA y la Robótica.

Entre las iniciativas presentadas en la cámara baja, se han propuesto ajustes al marco legal para que se faculte al Congreso la regulación de esta materia.

Hasta el momento se tratan de esfuerzos incipientes hacia una eventual regulación de esta tecnología. Entre estos esfuerzos, se encuentra la Carta de Derechos de la Persona en el Entorno Digital —impulsada por el Sistema Nacional de Transparencia— que en uno de sus capítulos aborda la necesidad de darle un uso ético a la inteligencia artificial, a partir de principios, como el derecho al uso de esta tecnología centrada en la persona, el derecho a la privacidad y a la protección de datos,

la transparencia y el acceso a la información, así como el derecho a la seguridad.

NEURODERECHOS

Por otro lado, otro de los temas que han aparecido con mayor intensidad en el debate tecnológico son los llamados “neuroderechos”, considerados como la cuarta generación de los Derechos Humanos, que intentan salvaguardar aspectos, como la identidad personal, la libertad de decisión, la privacidad de datos neuronales, la equidad en el mejoramiento de la capacidad, y la protección contra los sesgos algorítmicos (García, González y Hernández, 2022). En otras palabras, éstos son considerados derechos universales que buscan proteger las actividades cognitivas y la integridad mental de las personas. En México, al no encontrarse reguladas la privacidad mental y la información obtenida del análisis de la actividad cerebral, la regulación de los neuroderechos se encuentra rezagada.

Así, en la Cámara de Diputados de México se han propuesto diversas iniciativas para salvaguardar la privacidad de los usuarios y asegurar el acceso a los avances de la neurotecnología, que abarcan la inclusión de la perspectiva de inteligencia artificial en la Ley General de Educación, una nueva ley de Ciencia, Humanidades e Innovación, y la iniciativa para adherir los neuroderechos al artículo 4 constitucional.

En 2023 se presentó una iniciativa ante el Congreso mexicano que busca que se legisle en materia de neuroderechos desde dos ejes fundamentales: la privacidad e integridad, y la soberanía de las personas. Esta iniciativa resalta la importancia de establecer salvaguardas legales para proteger la privacidad de los datos cerebrales y garantizar el consentimiento informado en las intervenciones cerebrales. Un aspecto indispensable que se resalta en esta iniciativa es la promoción del desarrollo ético de la neurociencia y las tecnologías neuronales.

Además de buscar añadir al párrafo cuarto constitucional la garantía del derecho a la protección de la privacidad y la integridad de la mente y el pensamiento de las personas. En ese sentido, el Estado se encontraría obligado a garantizar el respeto a la privacidad de los datos cerebrales y neuronales, así como a la integridad mental en el ámbito de la neurociencia y las tecnologías neuronales.

Por otra parte, en la referida Carta de Derechos de la Persona en el Entorno Digital los neuroderechos son recogidos como un elemento necesario en la práctica de la protección de datos personales, a partir del derecho a la preservación de la identidad personal, de la privacidad neuronal, del libre albedrío, de la equidad en el mejoramiento de la capacidad cerebral, así como en contra del sesgo y discriminación.

CIBERSEGURIDAD

Otro de los elementos presentes en el debate tecnológico ante esta intensificación tiene que ver con la ciberseguridad, la práctica de proteger equipos, redes, aplicaciones, entre otros elementos, de posibles amenazas digitales, y en cuyos contenidos los datos personales pueden estar presentes.

México representa un mercado enorme con potenciales ganancias económicas para cibercriminales. Esto se puede ver en ejemplos como los ataques a las instituciones mexicanas, como Condusef, el Servicio de Administración Tributaria (SAT), el Banco de México, la Secretaría de la Función Pública, el Instituto de Seguridad y Servicios Sociales de los Trabajadores del Estado (ISSSTE), entre otras. Según datos de la compañía de ciberseguridad Fortinet, durante 2023 los ciberataques en México representaron el 47 por ciento del total de los ataques en América Latina, lo que equivale a 94 mil millones de intentos de ataques (Riquelme, 2024).

La Estrategia Nacional de Ciberseguridad del gobierno federal es una guía rectora para combatir estos casos. No obstante, instituciones como la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) indican que esto se ha limitado al papel y no se ha convertido realmente en una política de Estado (Congreso de la Ciudad de México, sf).

En México hemos tenido, sin embargo, diversos avances en materia de ciberseguridad, como se puede ver en la iniciativa de 2015 que buscaba incluir los delitos cibernéticos en el Código Penal Federal, el Código Federal de Procedimientos Penales, la Ley Federal Contra la Delincuencia Organizada, y la Ley de la Policía Federal Preventiva.

Estos esfuerzos de 2015 llegaron a consolidarse en una iniciativa para expedir una Ley Federal para Prevenir y Sancionar los Delitos Informáticos. Finalmente, en 2018 se trató de expedir la Ley General de Seguridad Privada; en 2019 la Ley de Seguridad Informática y en 2020 la Ley General de Ciberseguridad (Congreso de la Ciudad de México, sf), esfuerzos que hasta el momento no se han concretado.

VIOLENCIA DIGITAL

La violencia digital ha sido uno de los fenómenos que también se ha acrecentado con la intensificación del uso de tecnologías. De acuerdo con la encuesta de ciberacoso realizada por Bumble en conjunto con Ipsos, uno de cada dos internautas ha experimentado acoso digital o conoce a alguien que lo ha vivido en México, afectando particularmente a personas de la comunidad de la diversidad sexual y de género y a las mujeres; el 95 por ciento y 75 por ciento de estas poblaciones respectivamente ha sido afectada por agresiones en línea (Iheme, 2023).

En la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y en el Código Penal Federal se ha incluido la

violencia digital y la tipificación de violaciones a la intimidad sexual de las personas a través de medios digitales.

A su vez, a través del caso emblemático de la activista Olimpia Corral Melo, quien después de ser víctima de la difusión de un video íntimo sin su consentimiento, se logró que se expidiera la ley que se conoce como Ley Olimpia. Se trata de un conjunto de reformas legales que contempla sanciones de tres a seis años de prisión por realizar estas acciones, así como multas que van de 500 a 1,000 Unidades de Medida y Actualización (UMA), reconociendo la violencia digital y sancionando los delitos que involucran la intimidad sexual a través de medios digitales (Gobierno de México, sf).

CONCLUSIONES

La Era Digital ha traído consigo múltiples beneficios, indudablemente, pero también problemas y riesgos, entre los que destacan la necesidad de fortalecer la protección de los datos personales y la privacidad de las personas.

En ese sentido, si bien en México contamos con robustos marcos normativos que regulan la protección de los datos personales, desde la propia Constitución, es cierto que ante los nuevos desafíos y desarrollos tecnológicos se requiere una mayor atención a los mismos, abordando temáticas como el énfasis en la protección de niñas, niños y adolescentes, la regulación de los efectos de la inteligencia artificial, el fortalecimiento del marco normativo contra posibles ciberataques, y, desde luego, la necesidad de contrarrestar la creciente violencia digital.

Todo ello deberá ser atendido por las autoridades, incorporando los mejores estándares y buenas prácticas internacionales, sumando al diálogo a voces de todos los sectores involucrados y teniendo siempre presente el objetivo superior de maximizar la tutela de los derechos humanos para todas las personas.

REFERENCIAS BIBLIOGRÁFICAS

- Cámara de Diputados del H. Congreso de la Unión (2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares*. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf>.
- Cámara de Diputados del H. Congreso de la Unión (2017). *Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados*. <https://www.diputados.gob.mx/LeyesBiblio/pdf/LGPDPPSO.pdf>.
- Congreso de la Ciudad de México (sf). *Ciberseguridad*. <https://www.congreso-socdmx.gob.mx/archivos/legislativas/Ciberseguridad.pdf>.
- García, J., González, J., y Hernández, P. (2022). El neuroderecho como un nuevo ámbito de protección de los derechos humanos. *Revista Mexicana de Derecho Constitucional*, (1), 65. https://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S1405-91932022000100065.
- Gobierno de México (sf). La “Ley Olimpia” y el combate a la violencia digital. *Profeco*. <https://www.gob.mx/profeco/es/articulos/la-ley-olimpia-y-el-combate-a-la-violencia-digital?idiom=es>.
- Hurtado Razo, L. A. (sf). Violencia digital contra niños y adolescentes. *UNAM Global*. https://unamglobal.unam.mx/global_revista/violencia-digital-contra-ninos-y-adolescentes/.
- Iheme, P. (2023). Violencia digital en México afecta más a mujeres y genera mayor consciencia entre ellas. *El Economista*. <https://www.eleconomista.com.mx/arteseideas/Violencia-digital-en-Mexico-afecta-mas-a-mujeres-y-genera-mayor-consciencia-entre-ellas-20230829-0036.html>.
- Instituto Nacional de Estadística y Geografía (2022). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTITH) 2022*. <https://www.inegi.org.mx/programas/dutih/2022/>.
- Riquelme, R. (2024). México recibió la mitad de los ciberataques en América Latina en 2023: Fortinet. *El Economista*. <https://www.eleconomista.com.mx/tecnologia/Mexico-recibio-la-mitad-de-los-ciberataques-en-America-Latina-en-2023-Fortinet-20240327-0063.html>.



Inteligencia jurídica en expansión

Trabajamos para
mejorar el día a día
del **operador jurídico**

Adéntrese en el universo
de **soluciones jurídicas**

 +52 1 55 65502317

 atencion.tolmex@tirantonline.com.mx

prime.tirant.com/mx/