DESAFÍOS PARA TENER MAYOR SEGURIDAD ANTE LA INTELIGENCIA ARTIFICIAL

CLAUDIO M. DE ROSA

OBSERVATORIO DE POLÍTICAS PÚBLICAS
UNIVERSIDAD FRANCISCO GAVIDIA

UFG
UNIVERSIDAD FRANCISCO GAVIDIA
Powered by Arizona State University®

DESAFÍOS PARA TENER MAYOR SEGURIDAD ANTE LA INTELIGENCIA ARTIFICIAL

OBSERVATORIO DE POLÍTICAS PÚBLICAS (OPP-UFG)
UNIVERSIDAD FRANCISCO GAVIDIA

CLAUDIO M. DE ROSA
INVESTIGADOR ECONÓMICO

OBSERVATORIO DE POLÍTICAS PÚBLICAS UNIVERSIDAD FRANCISCO GAVIDIA

UFG UNIVERSIDAD FRANCISCO GAVIDIA
Powered by Arizona State University®

MISIÓN

La Universidad Francisco Gavidia es una institución educativa incluyente de clase global, comprometida con la calidad de sus servicios docentes y científicos, para lograr el progreso social, la productividad y la competitividad de El Salvador, formando a los mejores profesionales del país.

VISIÓN

Ser la principal y mejor universidad privada de carácter global que contribuya a elevar la competitividad y productividad de El Salvador a través de la formación de profesionales emprendedores, innovadores y con visión global.

CONSEJO DIRECTIVO

DIRECCIÓN Y CONTACTO

Universidad Francisco Gavidia: Calle El Progreso n.° 2748,
Edificio de Rectoría, San Salvador, El Salvador.
Tel. (503) 2249-2700
www.ufg.edu.sv

OBSERVATORIO DE POLÍTICAS PÚBLICAS
UNIVERSIDAD FRANCISCO GAVIDIA

UFG
UNIVERSIDAD FRANCISCO GAVIDIA
Powered by Arizona State University®

DE ESTA EDICIÓN

Título: "Desafíos para tener mayor seguridad ante la Inteligencia Artificial"

Autor: Claudio Manuel de Rosa

Colección: Educación
Primera Edición: ©Observatorio de Políticas Públicas (OPP), 2024.

Para citar: de Rosa, C.M.(2024). *Desafíos para tener mayor seguridad ante la Inteligencia Artificial.* Universidad Francisco Gavidia. Observatorio de Políticas Públicas.

Observatorio de Políticas Públicas de la Universidad Francisco Gavidia.

Hecho el depósito que dicta la ley

Publicación de carácter electrónica, octubre de 2024, San Salvador, República de El Salvador, Centroamérica.

Dirección y contacto
Universidad Francisco Gavidia, edificio de Atención al Estudiante, nivel 4, 55 Av. Sur, condominio Centro Roosevelt, entre Av. Olímpica y alameda Roosevelt, San Salvador, El Salvador, C.A.
Teléfono: (503) 2209-2870
Email: observatoriopp@ufg.edu.sv

Edición y corrección de estilo
Lya Ayala Arteaga

Diagramación y diseño de cubierta
Alexandra María Rivera Torres

006.3

D437d
slv

De Rosa Ferreira, Claudio Manuel
Desafíos para tener mayor seguridad ante la inteligencia artificial [recurso electrónico] / Claudio Manuel de Rosa Ferreira ; edición y corrección de estilo Lya Ayala Arteaga ; diagramación y diseño de cubierta Alexandra María Rivera Torres. -- 1ª ed. -- San Salvador, El Salv. : Observatorio de Políticas Públicas (UFG), 2024.
1 recursos electrónico, <275 p. ; il. col. : 21 cm>

Datos electrónicos : <1 archivos, formato pdf, 3.5 mb>. -- https: //ri.ufg.edu.sv/.

ISBN: 879-99983-906-1-4 <E-Book, pdf>

1. Inteligencia artificial – Investigaciones. 2. Computadores neurales. 3. Informática – Medidas de seguridad. I. Título

BINA / jmh

ISBN: 978-99983-906-2-1

AGRADECIMIENTOS

Agradezco de manera especial:

Al ingeniero y doctor Mario Antonio Ruíz Ramírez, rector de la Universidad Francisco Gavidia, por la oportunidad para realizar este trabajo como miembro del Observatorio de Políticas Públicas de la UFG (OPP-UFG).

Al Dr. Roberto Morán Argueta, Coordinador del OPP-UFG, por sus observaciones que contribuyeron a mejorar esta investigación.

Al Dr. Mario Rafael Ruiz Vargas, Director de Tecnología y Sistemas de la UFG, por sus comentarios y observaciones técnicas que constituyen un aporte significativo y de gran relevancia para esta investigación

A la MSc. Yasmín Franco, docente e investigadora de la Facultad de Ciencias Jurídicas, por la revisión y aportes a las propuestas de Ley de Inteligencia Artificial y Ley de Protección de Datos.

Y, por último, le agradezco a ustedes estimados lectores por su interés en conocer la situación que enfrentarán las Instituciones de Educación Superior ante los desafíos de la sociedad digital.

Claudio M. de Rosa

ÍNDICE

CUADROS

GLOSARIO

EUA:	Estados Unidos de América
FMI:	Fondo Monetario Internacional
FTI:	*Future Today Institute*
GPT:	*Generative Pre-Training*
ILIA:	Índice Latinoamericano de Inteligencia Artificial
IA:	Inteligencia Artificial
IP:	Dirección única de identificación de un dispositivo
MIT:	*Massachusetts Institute of Technology*
OEA:	Organización de los Estados Americanos
OECD:	*Organisation for Economic Co-operation and Development* (Organización para la Cooperación y el Desarrollo Económico)
ONU:	Organización de las Naciones Unidas
PYMES:	Pequeñas y medianas empresas
RGPD:	Reglamento General de Protección de Datos (Unión Europea)
TIC:	Tecnologías de la Información y las comunicaciones
UNESCO:	Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura
UE:	Unión Europea
WEF:	*World Economic Forum*

RESUMEN CONCEPTUAL

Esta investigación *Desafíos para tener mayor seguridad ante la Inteligencia Artificial* presenta las oportunidades y amenazas relacionadas con esta tecnología desde su concepción, desarrollo, aplicación y uso. Para tener mayor seguridad y proteger a las personas naturales y organizaciones privadas y públicas resalta la necesidad de cumplir con los derechos humanos y evitar la discriminación, el sesgo y el uso de aplicaciones maliciosas que causan graves daños personales a grupos de personas.

Basado en una revisión exhaustiva de la legislación relativa a tecnologías en el mundo, se hace una propuesta de Ley de Inteligencia Artificial y otra de Protección de Datos Personales, incluyendo el impacto que puede tener en este campo la inteligencia artificial. Estas propuestas deben discutirse con diversos sectores de la sociedad para lograr un consenso y tener dos leyes de alta calidad jurídica apegadas a normas internacionalmente aceptadas. Además, que sirva de base para legislar en esto dos temas en los países que no tengan estas disposiciones legales.

ABSTRACT

This research "Challenges to have greater security in the face of Artificial Intelligence" pre-sents the opportunities and threats related to this technology, from its conception, develop-ment, application, and use. To have greater security and protect natural persons and private and public organizations, it highlights the need to comply with human rights and avoid dis-crimination, bias and the use of malicious applications that cause serious harm to individuals or groups of people.

Based on an exhaustive review of legislation related to technologies in the world, a proposal for an Artificial Intelligence Law and another for the Protection of Personal Data is made, including the impact that artificial intelligence can have in this field. These proposals must be discussed with various sectors of society to achieve consensus and have two laws of high legal quality and attached to internationally accepted standards. Furthermore, it can serve as a basis for legislating on these two issues in countries that do not have these legal provisions.

PALABRAS CLAVE	Seguridad, discriminación, derechos humanos, daños personales, riesgos, oportunidades, El Salvador.
KEYWORDS	Safety, discrimination, human rights, personal injuries, risks, opportunities, El Salvador.

DESAFÍOS PARA TENER MAYOR SEGURIDAD ANTE LA INTELIGENCIA ARTIFICIAL

I. Introducción

El mundo se enfrenta a un dilema crucial ante el vertiginoso avance en el uso y alcance de la Inteligencia Artificial (IA). Este avance está transformando y acelerará de manera determinante la vida humana, gracias a sus capacidades para impulsar importantes progresos científicos y mejorar las condiciones de vida. Sin embargo, también, conlleva serias amenazas, lo cual subraya la necesidad urgente de regular sus procesos de desarrollo, aplicaciones y uso.

Este estudio tiene el objetivo general dar a conocer los beneficios y riesgos que implica el creciente e intensivo uso de la IA en todos los campos de la vida humana (económico, social, jurídico, político, de seguridad y ambiental), así como identificar la legislación necesaria para maximizar los primeros y contener o evitar los segundos. En este contexto, los objetivos específicos son:

- Identificar los principales beneficios que traerá el creciente uso de IA, así como los mayores riesgos e impactos socioeconómicos, jurídicos, políticos, en la seguridad de las personas naturales y jurídicas, y en el medio ambiente.

- Conocer las propuestas de leyes que ya se están aplicando y las continúan en estudio en las sociedades más avanzadas del mundo para regular la creación y uso de la IA y, tenerlas como base para proponer el articulado que debería tener una ley que regule y controle el uso de la IA en El Salvador, así como en cualquier país que lo requiera.

- Evaluar las necesidades de cambio en educación, desde los niveles iniciales hasta la educación superior y educación continua o de por vida, para que toda la población salvadoreña conozca sus derechos y deberes en el uso de la IA.

En este contexto, las preguntas clave de la investigación (hipótesis) son:

- ¿Cuáles son los beneficios potenciales que traerá el uso cada vez más grande de la IA?
- ¿Cuáles son los riesgos potenciales que traerá el uso cada vez más grande de la IA?
- ¿Cómo puede ser afectada la vida personal y laboral con el creciente uso de la IA?
- ¿Cuáles son los problemas que una ley debe abordar para proteger a la sociedad sin limitar el desarrollo de la IA y su uso?
- ¿Qué elementos debería incluir una ley en El Salvador para proporcionar mayor seguridad a la sociedad frente a la Inteligencia Artificial?
- ¿Qué debería tener una Ley de Protección de Datos Personales en un entorno cada vez más tecnológico, dominado por la tecnología y la Inteligencia Artificial?

Para cumplir con los objetivos e hipótesis planteados se utilizará una metodología propia de una investigación documental tanto a nivel nacional como internacional para realizar un análisis de situación, siempre considerando el cumplimiento de los derechos humanos, el desarrollo de las personas y el respeto ambiental.

Como resultado de esta investigación se espera presentar los beneficios y riesgos que generará el mayor uso de IA, así como su impacto socioeconómico, jurídico, político, de seguridad y ambiental, y tenerlos como base del articulado que conformará la propuesta de Ley de IA para dar mayor seguridad a las personas naturales, empresas y sociedad, en general. Como factor complementario, se presentará una propuesta de ley de Protección de Datos Personales, ajustada al nuevo entorno tecnológico, en general, y de la IA, en particular.

II. Los desafíos ante el creciente uso de la inteligencia artificial

1. Historia de la inteligencia artificial

En esta segunda parte se presenta un resumen de la Historia de la inteligencia artificial que se expone en detalle con sus respectivas fuentes en el Anexo I.

El concepto de la inteligencia artificial (IA) se originó tras la publicación del artículo *A Logical Calculus of Ideas Immanent in Nervous Activity* (Un cálculo

lógico de ideas inmanentes a la actividad nerviosa) de Warren McCullochy Walter Pitts en 1943. Posteriormente, en 1950, Alan Turing publicó *Computing Machinery and Intelligence*, dando vida al concepto conocido como el 'Test de Turing' que sirvió para precisar si la inteligencia de una máquina puede considerarse similar o igual a la del ser humano. En 1951, Marvin Minsky y Dean Edmonds crearon el primer ordenador de red neuronal (*SNARC* por sus siglas en inglés de *Stochastic Neural Analog Reinforcement Calculator*). En 1952, Arthur Samuel creó un software que permitió aprender a jugar ajedrez de forma autónoma. Luego, en 1956, John McCarthy acuñó el término 'Inteligencia Artificial' durante la conferencia de Dartmouth, donde Marvin Minsky, John McCarthy y Claude Shannon presentaron la idea de la IA. A fines de los años 50, Roger Easton contribuyó a crear el Sistema de Vigilancia Espacial Naval y el Proyecto *Vanguard*, con el primer sistema para detectar y rastrear todo tipo de objetos en la órbita terrestre, dando origen al GPS (*Global Positioning System*).

Ante los pocos avances en el desarrollo de la IA, el parlamento del Reino Unido solicitó a Sir James Lighthill, en 1973, evaluar la situación de la investigación de la IA en el país, quien señaló su fracaso e incapacidad para lograr los grandes objetivos. Así, tanto en el Reino Unido como en Estados Unidos de América (EUA) hubo reducciones de presupuestos y disminuciones en el número de proyectos de investigación en IA, dando inicio al *primer invierno de la IA* que duró hasta 1980.

En 1966, Joseph Weizenbaum del MIT (*Massachusetts Institute of Technology*) desarrolló ELIZA, considerado el primer chatbot para enseñar a las computadoras a comunicarse con los seres humanos. Más adelante, en 1978, John P. McDermott presentó el R1 (luego llamado XCON, por *eXpert CONfigurer*), un sistema que permitía ayudar con los pedidos de acuerdo con lo solicitado por el cliente.

Luego, se crearon las máquinas *Lisp* (*LISt Processor*, Procesamiento de listas) que tuvieron éxito hasta 1987. Esto causó el «segundo invierno de la IA» porque los gobiernos de EUA y Japón abandonaron los proyectos de investigación en sistemas expertos. En 1979, Hans Moravec presentó el *Stanford Cart*, uno de los primeros vehículos autónomos controlados por computadora. Seguidamente, en los años 80 surgió el nuevo enfoque del *conexionismo* que considera que el comportamiento inteligente se puede modelar para representar una estructura y funcionamiento similar al de las redes neuronales del cerebro. Más tarde, en 1997, *Deep Blue* de IBM logró ganarle a Gary Kasparov, el campeón mundial de ajedrez.

Google logró grandes avances a partir de 2008 con el reconocimiento de voz en aplicaciones que utilizaron en smartphones. En 2012, Andrew Ng alimentó una red neuronal con 10 millones de vídeos de YouTube, los cuales utilizó

como base de datos de entrenamiento. Así nació una nueva etapa para el Deep Learning. Después, en 2016, el sistema *AlphaGo* de Google venció a Lee Sedol, el campeón de Go. Además, la IA comenzó a utilizarse en los videojuegos empleando el *DeepMind AlphaStar*. El Deep Learning y el Machine Learning se fueron introduciendo en todos los sectores: económico, social, político, jurídico, seguridad y medio ambiente. Amazon presentó a Alexa, el primer asistente de voz; lanzó Google Allo, aplicación de mensajería móvil que permitió aprender del usuario y adaptarse a sus costumbres; e IBM presentó a Watson, creado con General Motors, que memoriza las preferencias y decisiones del conductor.

En 2017, la IA continuó posicionándose en la vida cotidiana de las personas por su uso en las redes. A partir de 2018, la IA comenzó a utilizase en el blockchain, Internet de las Cosas, ciberseguridad, la nube y los asistentes virtuales, así como el uso de *chatbots*. En 2019, se utilizaron de manera creciente los asistentes virtuales con características cada vez más humanas. En febrero de 2019 se dio a conocer el sistema Generative Pre-Training (GPT), aunque sin acceso al público. Y Samsung mostró un sistema para transformar imágenes faciales, crear vídeos y texto falsos. Así tomó fuerza el concepto de *DeepFake* y los debates sobre la ética en torno a la IA.

Entre 2020 y 2021, la IA experimentó uno de los períodos de mayor crecimiento y avances, en gran parte, por la creciente disponibilidad de datos (Big Data). Posteriormente, el 5 de enero de 2021, *OpenAI* presentó el programa *DALL-E* (*DALL-E* combina los nombres del personaje de Pixar Wall-E y de Salvador Dalí) el cual crea imágenes una vez que se solicitan en lenguaje natural. En 2022, hubo avances altamente disruptivos, especialmente por el ChatGPT de *OpenAI*, puesto a disposición del público el 30 de noviembre de ese año. Los avances continuaron en 2023, destacando los relacionados con la IA generativa –técnicas de aprendizaje profundo (*deep learning*)– y el uso de grandes bloques de datos para crear nuevos contenidos en textos, imágenes, vídeos y música (ChatGPT, y *Dall E*, entre otros).

Por su parte, Google presentó *Bard* en marzo de 2023 antes de haberlo desarrollado totalmente; más tarde, presentó a *Gemini* como su modelo definitivo en diciembre de 2023. Así, también, Microsoft lanzó GitHub *Copilot*, en junio de 2021; y OpenAI dio a conocer el sistema *Sora* en 2023, una herramienta para crear vídeos a partir de una descripción de lo que se desea reproducir en la pantalla. Las tecnologías de IA han seguido progresando aceleradamente, y las nuevas aplicaciones innovadoras siguen irrumpiendo con fuerza en el mercado, entre las cuales destacan: ChatGPT, lanzado en noviembre de 2022; la nueva versión de Amazon Alexa, presentada en junio de 2024; *GitMind*, actualizado en mayo de 2024; *Google Assistant*, versión actualizada en enero de 2024; FaceApp, con nueva versión de junio de 2024;

QuillBot, actualizado en mayo de 2023; *Elsa*, lanzada en 2024; *Databot*, con su actualización de febrero de 2023; Canva, con su versión actualizada en febrero de 2020; *Otter.AI*, en su versión de 2024; y el *AI Pin* (broche IA) presentado en 2024 que son descritas en el Anexo I.

Ante el avance de la IA, el Fondo Monetario Internacional (FMI) señaló la necesidad de crear entornos seguros y responsables mediante la formulación de sólidos marcos de regulación para mantener la confianza pública. En este sentido, la Unión Europea promulgó en 2023 el Reglamento de Inteligencia Artificial (AI Act), la primera ley mundial sobre regulación de la IA (Georgieva, 2024). Cada vez hay más conciencia sobre la necesidad de contar con sólidos marcos legales, tanto para proteger a personas naturales y empresas como para estimular las inversiones en infraestructura digital y en la formación de competencias digitales en los trabajadores.

2. Predicciones futuristas sobre la evolución tecnológica de la IA

En este apartado se presenta un resumen de las predicciones futuristas sobre la evolución tecnológica que se expone en detalle con sus respectivas fuentes en el Anexo II.

Ante el vertiginoso avance de la IA es importante conocer las predicciones de los grandes futurólogos en el mundo como Raymond Kurzweil, Bill Gates, Elon Musk y Amy Webb. Por su parte, Raymond Kurzweil, experto en tecnología de sistemas y de IA, director de ingeniería de Google, creador de la *Singularity University*, ha acertado alrededor del 86 % de sus predicciones futuristas. En 1990, predijo la rápida expansión del internet; en 1998, presentó su visión futura de la IA y su capacidad para controlar el universo en el siglo XXI, afirmando que no habrá diferencias entre el ser humano y la máquina que superará la velocidad de respuesta del cerebro humano y logrará tener atributos propios del ser humano (Resiliente Digital, 2023).

Kurzweil, en 2005, en su libro L*a singularidad está cerca* visualizó que los cambios tecnológicos se darían con más frecuencia y vertiginosidad, donde la evolución tecnológica permitirá a los seres humanos superar el envejecimiento y las enfermedades; y se prevé que mediante la IA se terminará con el hambre y la pobreza en todo el mundo. Entre las predicciones de Kurzweil (presentadas de manera extensa y con sus respectivas fuentes en el Anexo II) destacan:

- En torno a 2023, los *nanobots* (pequeños robots de 50 a 100 nanómetros de ancho) serán los protagonistas de lograr revertir la edad del ser humano.

- En los años 20 los seres humanos se relacionarán con las máquinas de manera similar a como se relacionan con otro ser humano.
- Para 2029, los ordenadores tendrán una inteligencia similar a la del ser humano y en el año 2030 la realidad virtual será muy similar a la real.
- Las máquinas alcanzarían un nivel de inteligencia similar a la del ser humano en 2029 y la superarán en un billón de veces en 2045.
- Antes de 2030, habrá un uso masivo de robots domésticos.
- Hacia fines de los 30, el ser humano podrá cargar la mente/consciencia.
- En 2040, la inteligencia no biológica será mil millones de veces más capaz que la biológica.
- En los años 40, se podrá obtener comida de la nada y cualquier objeto se podrá hacer aparecer en el mundo físico.
- Hacia 2045, se estima que la inteligencia del ser humano se habrá multiplicado por mil millones, permitiendo una conexión inalámbrica con la nube a través del neocórtex.

Según Bill Gates (2024) hay un alto riesgo debido a «una carrera armamentística donde la IA puede usarse para diseñar y lanzar ciberataques contra otros países», potenciando la creación de nuevas y peligrosas ciberarmas. Por otro lado, Gates considera que los avances en IA tendrán un impacto positivo en diversos aspectos, incluyendo el desarrollo humano por sus aportes a la educación (tutores personalizados a cada estudiante); a la salud, por los avanzados tratamientos del Alzheimer, la obesidad y la anemia falciforme; y dar mejores respuestas a futuras pandemias y atender de manera más adecuada los embarazos de alto riesgo, mediante innovadores procesos de ultrasonidos impulsados por la IA. Para Gates, la IA tendrá un impacto positivo en la vida laboral, pero, también, perjudicará a muchos trabajadores, lo que plantea un gran desafío tanto para la formulación de políticas públicas como para las estrategias empresariales privadas en términos de cómo protegerlos. Además, prevé un importante boom tecnológico hacia finales de los 20, marcando así el inicio de una nueva era de la IA.

Sin embargo, a Gates le preocupa la brecha tecnológica que existe entre diferentes regiones del mundo. Señala que –para lograr un uso significativo de la IA en los países de altos ingresos como EUA –su población podría tardar entre 18 y 24 meses en adoptar de manera significativa la IA, mientras que en países de bajos ingresos este proceso podría llevar alrededor de tres años.

Por su parte, Elon Musk se pregunta: «¿Podemos tener un año normal en 2024? (...) después de cuatro años de locura?» (Musk, 2024, párr.1). Luego predijo que el «2024 será aún más loco» (párr.2), mostrando cierta coincidencia con lo expresado por Gates, sobre los grandes avances que tendrá la IA en 2024.

A su vez, la reconocida futurista Amy Webb, CEO del *Future Today Institute* (FTI), advierte que habrá 10 temas clave en 2024 que deberían estar en el radar:

1. El *concepto a lo concreto* creará una ola de nuevas herramientas de IA que permitirán idear y perfeccionar continuamente el trabajo hasta conseguir un marco concreto.
2. Habrá un nuevo *cripto invierno* por la volatibilidad del mercado de criptomonedas.
3. Se hará «sostenible la sostenibilidad».
4. Los algoritmos se convertirán en nuestra fuerza laboral y es posible que necesiten licencias profesionales.
5. Los *wearables* (usables) están de vuelta marcando el comienzo de una nueva era de respuestas visuales y de voz: los teléfonos inteligentes serán reemplazados por los «wearables omnipresentes».
6. La inteligencia organoide (IO) dará forma tanto a la informática como a la geopolítica. ¿Qué pasaría si hubiera una carrera por ganar en la computación biológica?
7. Se vislumbran desafíos legales para las grandes tecnologías y esta vez podrían tener éxito si logran arreglos «para mantenerse inmunes a la responsabilidad legal cuando se trata de contenidos de los usuarios».
8. «La biotecnología crea accidentalmente un nuevo sistema de castas genéticas» para brindar nuevas terapias de manera masiva.
9. «Un mundo de nuevos materiales»: habrá muchas opciones el próximo año.
10. «Elecciones y desinformación involuntaria»: habrá más herramientas para «manipular intencionadamente a los votantes mediante desinformación creada con contenido sintético de alta calidad (deepfakes) y difundirla por toda la web».

Estos futurólogos coinciden que debido a los avances de la IA en 2024 se mejorará la productividad, la salud, la educación y la investigación, entre otras áreas; aunque, habrá amenazas que pueden afectar negativamente a toda la sociedad, en general, y a los gobiernos y empresas, en particular; e incluso cambiando la forma que se conduce una guerra o se conforma un ejército, por lo que ha sucedido en la guerra de Rusia contra Ucrania, donde se han experimentado tecnologías que utilizan la IA con gran precisión y eficacia.

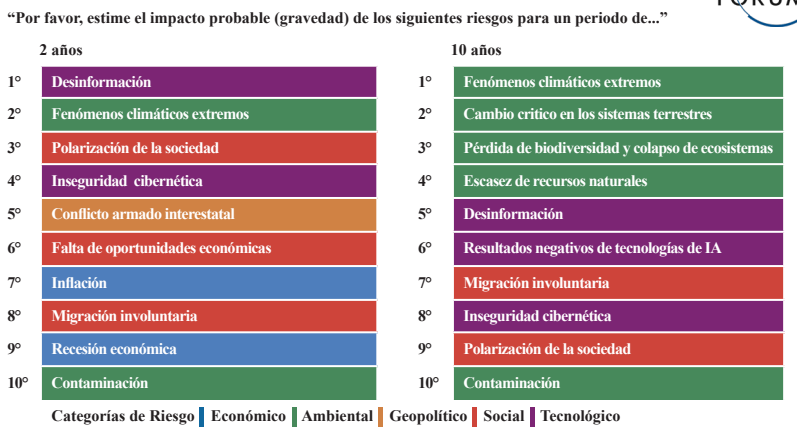
Por tanto, los gobiernos deberán ajustar sus planes de defensa para estudiar, adoptar, incluir y utilizar con gran precisión las tecnologías que utilizan la IA en las diversas etapas de un conflicto armado, desde la planificación, el uso de inteligencia, la toma de decisiones de todo tipo; incluyendo los aspectos logísticos, identificar todo desplazamiento de tropas, realizar bombardeos, ataques con drones inteligentes y lo relacionado con la guerra de información, todo realizado en tiempo real (Wagstaff, 2023).

3. Amenazas fraudulentas de la IA: ¿Se puede enseñar ética a las máquinas?

En medio de la rápida evolución y grandes aportes de la IA, también, hay cada vez más amenazas que deben superarse para evitar consecuencias socioeconómicas negativas. Isabel Rubio (2024) presenta en su artículo *El hermano maligno de ChatGPT y otras amenazas de la inteligencia artificial generativa que en el dark web* se puede crear un *malware* (programa maligno) o la presentación de sitios web que podrían inducir a la defraudación, como el envío de mensajes falsos que simulan ser de un banco. De esta manera, la IA generativa puede convertirse en una herramienta con fines maliciosos: estafas sofisticadas, pornografía no consentida, campañas de desinformación e incluso dar información para crear armas bioquímicas y de tipo militar.

En el Foro Económico Mundial (FEM) se presentó el informe de Riesgos Globales 2024, el 10 de enero de 2024, elaborado por el FEM, *Zurich Insurance Group* y Marsh McLennan, quienes realizaron una encuesta de opinión en septiembre de 2023 «entre más de 1,400 expertos en riesgos globales, políticos y líderes del sector» (*World Economic Forum* 2024, WEF por sus siglas en inglés, párr. 3). Preocupa ver que el 30 % de los encuestados estima que, en los próximos dos años, esto es 2024-2025, «la probabilidad que se produzcan catástrofes globales será mayor, y cerca de dos tercios esperan que esto ocurra en los próximos diez años» (WEF 2024, párr. 2).

Cuadro 1. Informe de Riesgos Globales 2024



Fuente: Encuesta de percepción de riesgos globales del Foro Económico Mundial 2023-2024.
Nota: Este cuadro es una reproducción de los cuadros presentados por el WEF 2024.

El informe de Riesgos Globales 2024 estableció cinco «categorías de riesgo»: económico, ambiental, geopolítico, social y tecnológico (Cuadro 1), y solicitó a los encuestados que estimaran el «impacto probable (gravedad)» de los riesgos en cada categoría en un período de dos años y de 10 años. Los riesgos en el campo económico solo se observan dentro del plazo de dos años, destacando la «inflación» y la «recesión económica», dos problemas que están presente a mediados de 2024 y con perspectivas de mantenerse en 2025.

En el campo «tecnológico», la «desinformación» está presente en la visión de riesgos que se tiene tanto a dos años y en un lapso a 10 años. Según Carolina Klint, directora comercial en Europa de Marsh McLennan, «los avances de la inteligencia artificial alterarán radicalmente las perspectivas de riesgo de las organizaciones, ya que muchas de ellas tendrán dificultades para reaccionar ante las amenazas derivadas de la información errónea, la desintermediación y los errores de cálculo estratégicos» (WEF, 2024, párr. 10). A esto se agrega la «inseguridad cibernética» que se ubica en la cuarta posición de riesgos de cara a los próximos dos años y en el octavo lugar para un período de 10 años. Sin embargo, mirando los riesgos a 10 años ya se visualizan los «resultados negativos de la IA», así como la «inseguridad cibernética».

En el ámbito «geopolítico» preocupan los conflictos armados interestatales– como la guerra Rusia-Ucrania iniciada en febrero de 2022– que se amplió con la guerra entre Israel-Gaza, el 7 de octubre de 2023 y que amenaza a toda la región, porque Israel considera está «luchando en siete frentes a la vez» que son Cisjordania, Siria, Líbano, Irak, Irán y Yemen (El País, 2023, párr. 1). Además, hay otros conflictos armados en el mundo y las crecientes tensiones en el Pacífico Sur. Dado este escenario, las tensiones geopolíticas también presionarán a las empresas a negociar sus cadenas de suministros en condiciones muy complejas que, además, serán agravadas por el cambio climático y las ciberamenazas. A esto, se deben agregar las transiciones demográficas que se viven en diferentes partes del mundo. También, el WEF 2024 recomienda fortalecer la cooperación mundial para crear salvaguardas ante los riesgos más disruptivos, como es el caso donde mediante el uso e integración de la IA se tomen decisiones sobre conflictos (WEF, 2024).

En la categoría «social» destaca como riesgo importante la «polarización de la sociedad», algo que es exacerbado con la «desinformación». Se suma la «falta de oportunidades económicas», que junto con la inflación (costo de la vida más alto), y crecimientos económicos más débiles en muchos países del mundo (menor generación de empleos) presionan hacia mayores migraciones. Además, diversos conflictos armados también causan un aumento en la «migración involuntaria». Lo lamentable es que este tipo de riegos globales se dan tanto en el lapso de dos años como en la perspectiva a 10 años.

En la categoría «ambiental» entre los riesgos a dos años están los «fenómenos climáticos extremos», entre los cuales destacan severos cambios de temperaturas, así como grandes lluvias en terrenos que normalmente eran secos y de sequías en lugares que tenían abundancia de agua. También, la «contaminación» que se mantiene en el décimo lugar tanto en la visión a dos años como en la de diez años, corre el riesgo de aumentar por diversos actos que realiza prácticamente todo ser humano y empresas productivas en el mundo. En la perspectiva a 10 años, los riesgos de la categoría «ambiental» toman los cuatro primeros lugares, donde «Fenómenos climáticos extremos» se eleva al primer lugar, y le siguen «Cambio crítico en los sistemas terrestres», «Pérdida de biodiversidad y colapso de ecosistemas» y «Escasez de recursos naturales», ubicados entre el segundo y el cuarto lugar, respectivamente.

Ante todos los riesgos globales presentados por el WEF 2024, John Scott, encargado de Riesgo de Sostenibilidad en la *Zurich Insurance Group*, señaló que «las acciones individuales de la ciudadanía, las empresas y los países podrían ser decisivas para reducir los riesgos globales y contribuir a la creación de un mundo más próspero y seguro» (Weo, 2024, párr. 11).

Retomando las potenciales amenazas fraudulentas que se pueden dar mediante el uso de la IA, es pertinente continuar con lo expresado por *Netenrich* en diversos eventos del *Dark Web Forum*, donde se mostraron evidencias sobre el surgimiento del *FraudGPT*, un chatbot de IA, disponible en los canales de Telegram desde el 22 de julio de 2023, el que es utilizado por cibercriminales. Además de las amenazas socioeconómicas que se dan con el *FraudGPT*, los investigadores de *Proofpoint* señalan que los ciberdelincuentes también utilizan esta tecnología maligna para engañar a funcionarios de gobierno, políticos, empresarios o celebridades. Mediante el uso de IA generativa crean campañas con imágenes modificadas e incluso vídeos relacionados con estas personas destacadas (Rubio, 2024).

El uso de la tecnología con fines maliciosos ha aumentado la *pornificación* de las mujeres mediante el uso de IA. Este tipo de incidentes se disparó en 2023, incluyendo celebridades y otras personas comunes que fueron víctimas de fotografías y vídeos transformados en lo que se conoce como *deepfake* porno. Estas acciones maliciosas han generado un creciente interés público sobre el daño que puede causar esta tecnología cuando se utiliza para crear imágenes falsas. Entre muchos casos está el de la cantante española Rosalía quien, en mayo de 2023, denunció la publicación de una foto falsa en la cual muestra sus pechos, que fue alterada y subida a las redes por el cantante JC, Juan Manuel Cortés Reyes (Brascia, 2023).

Igualmente, los *deepfakes porno* han afectado a celebridades como Meghan Markle, Megan Fox y Kate Upton, así como a la cantante estadounidense Taylor

Swift que sufrió un ataque de este tipo en enero de 2024, con publicaciones de imágenes sexualmente explícitas en la red social X que «acumularon más de 35 millones de visualizaciones, 24,000 reenvíos y cientos de miles de *me gusta,* antes que la plataforma interviniera para suspender la cuenta del usuario –verificado– que compartió las fotografías, por violar las políticas de la red» (Brascia, 2024, párr. 1). Estas imágenes circularon prácticamente por un día, lo que volvió a poner atención sobre el peligro del creciente uso de pornografía falsa contra las mujeres generada por IA. También, causó gran impacto la difusión de cientos de miles de imágenes de jóvenes mujeres estudiantes del Instituto Politécnico Nacional en México (Brascia, 2024).

Ante este tipo de abusos, la organización Home Security Heroes presentó el estudio 2023 *State of Deepfakes: Realities, Threats, and Impact*, basado en una encuesta en la que participaron 1,522 hombres estadounidenses. Los principales resultados muestran que:

1. Los *deepfakes* vídeos en línea totalizaron 95,820, con un aumento de 550 % en comparación con 2019.
2. Los *deepfakes porno* constituyen el 98 % de los *deepfakes* en línea.
3. 99 % de los *deepfakes porno* son de mujeres.
4. Los cantantes y actrices surcoreanos constituyen el 53 % de las personas que aparecen en *deepfakes porno* y son el grupo objetivo más común.
5. 94 % de las personas que aparecen en *deepfakes porno* vídeos trabajan en la industria del entretenimiento.
6. Una de cada tres herramientas de *deepfake* permite a los usuarios crear *deepfakes porno.*
7. Ahora toma menos de 25 minutos y cuesta $0 crear un vídeo pornográfico *deepfake* de 60 segundos de cualquier persona usando solo una imagen de rostro clara.
8. 48 % de los hombres estadounidenses encuestados vieron *deepfakes porno* al menos una vez.
9. 74 % de los usuarios de *deepfakes porno* no se sienten culpables por ello.
10. 20 % de los encuestados ha considerado aprender a crear *deepfakes porno* con celebridades o personas conocidas por ellos.

Ante este tipo de situaciones, es importante trabajar en la creación de mecanismos tanto jurídicos como tecnológicos que establezcan normas éticas para el uso de la IA. Una propuesta interesante es la que se refiere a enseñar un código deontológico a las máquinas, similar a lo que se enseña a las personas, basado en tres principios fundamentales: acción, valor y norma, para establecer controles sobre el comportamiento de las diferentes aplicaciones que utilizan IA (Bejerano, 2023).

En este sentido, la profesora del área de Lógica y Filosofía de la Ciencia en la Universidad de Salamanca, Ana Cuevas señala que «La ética se desarrolla de formas muy diferentes. En algunos casos tendremos que hacer cálculos utilitarios, de minimización de los riesgos o de los daños... Otras veces a lo mejor tenemos que usar códigos deontológicos más fuertes, como establecer que un sistema no puede mentir. Cada sistema necesita incorporar ciertos valores y para esto tiene que haber un acuerdo comunitario y social» (Bejerano, párr. 13).

Si bien hay expertos en IA que defienden la necesidad de tener limitaciones y controles, hay otros que se oponen a cualquier forma de regulación. Entre estos últimos se encuentran los que propugnan el *aceleracionismo efectivo,* quienes apoyan un desarrollo tecnológico desregulado para que las tecnologías disruptivas emergentes progresen rápidamente. Estos expertos consideran que la IA es clave para transitar hacia la 'Singularidad', un concepto en el cual la tecnología supera la inteligencia humana. Este movimiento fue presentado por *The New York Times*, en un artículo de Kevin Roose titulado *This A.I. Subculture's Motto: Go, Go, Go* (2023), donde describe la reunión del grupo que se denominó «*Keep AI Open*» (mantengan abierta la IA), donde exhibían carteles con consignas como «acelerar o morir», «ven y tómalo» y «el mensajero de los dioses está disponible para usted».

Obviamente, ante los profundos y disruptivos avances de la IA, su creciente adopción por parte de las empresas y en la vida diaria de las personas, será necesario reflexionar profundamente sobre la necesidad que todos los gobiernos apliquen una regulación estricta ante los efectos negativos de la IA en la sociedad, pero sin limitar sus avances por las grandes contribuciones positivas que puede generar. Entonces, la gran pregunta es: ¿hasta qué punto regular? para proteger a todos los miembros de la sociedad sin crear límites al inexorable avance tecnológico. «Ser o no ser, esa es la cuestión» (Shakespeare, 1600-1603).

4. El uso generalizado de la inteligencia artificial: un gran mercado global

En artículo del Parlamento Europeo (2021) titulado *Qué es la inteligencia artificial y cómo se usa*, presenta las definiciones realizadas por la Comisión Europea sobre los tipos de IA, que los cataloga como: (1) Software: que comprende asistentes virtuales, software de análisis de imágenes, motores de búsqueda, sistemas de reconocimiento de voz y rostro; y (2) Inteligencia artificial integrada que incluye: robots, drones, vehículos autónomos, Internet de las Cosas. También destaca que la IA es utilizada a diario por una

gran cantidad de usuarios para realizar compras por internet y publicidad, búsquedas en la web, como asistentes personales digitales, para traducciones automáticas, saber sobre casas, ciudades e infraestructuras inteligentes, conocer sobre vehículos de conducción autónoma, sobre ciberseguridad y la lucha contra la desinformación, entre otros.

¿Qué es IA? para la Unión Europea (UE), «La inteligencia artificial es la habilidad de una máquina de presentar las mismas capacidades que los seres humanos, como el razonamiento, el aprendizaje, la creatividad y la capacidad de planear» (Parlamento Europeo, 2021, párr.1).

En este sentido, la UE destaca que la IA tiene la capacidad para que los sistemas tecnológicos observen lo que sucede en su entorno y relacionarse con él, lo que les permite resolver problemas y proceder con un fin específico. Los sistemas de IA reciben una gran cantidad de datos que procesa y que le sirven para dar una respuesta, lo que les da una capacidad para adaptar su comportamiento a una situación específica basado en acciones e información anterior que le permiten trabajar de manera autónoma (Parlamento Europeo, 2021). Como lo señala la UE, «La inteligencia artificial tiene un papel central en la transformación digital de la sociedad y ha pasado a ser una prioridad» no solo en esta región, sino que también en todo el mundo (Parlamento Europeo, 2021, párr.5).

Obviamente, el continuo y vertiginoso desarrollo de la IA transformará la vida de las personas, porque mejorará significativamente los servicios de salud, potenciará la eficiencia en la agricultura, hará grandes aportes para contener los daños relacionados con el cambio climático, proveerá mayor seguridad a las personas, aumentará las capacidades productivas y mejorará las comunicaciones y servicios de la administración pública.

Sin embargo, como se vio anteriormente, también presenta grandes riesgos por acciones delictivas y por el mal uso de información privada personal utilizando IA. Además, las empresas correrán riesgos por la incorporación de la IA generativa, que ha tomado más fuerza desde el lanzamiento de ChatGPT, demandando nuevas regulaciones en las empresas y por los gobiernos. Por tanto, las legislaciones deben estar orientadas a supervisar sistemáticamente los actuales y próximos modelos de IA para garantizar su uso ético velar por la transparencia y proteger a toda la sociedad del uso indebido de toda información personal o empresarial.

Ante estos riesgos en el uso de la IA, es preocupante que, en general, no haya una clara comprensión que cada vez que una persona natural o una empresa utiliza internet provee una gran cantidad de información, aunque no se dé el nombre y se sea muy cuidadoso en lo que se pone, porque la dirección IP –dirección única de identificación de un dispositivo en internet o en una

red local– se transforma en un documento de identidad personal que circula instantáneamente por todo el mundo *on line*. Esta información es captada por las grandes empresas como Facebook, Google y numerosas de organizaciones más pequeñas especializadas en capturar e integrar rastros digitales de todos los sitios web que se accede, correos electrónicos y toda la información que se envía (García, 2023).

El volumen de información que se genera diariamente es inmenso y es cada vez mayor día a día. Considere que el internet de las cosas, conectado en diversos medios electrónicos ya genera una gran cantidad de información diversificada, como la temperatura que se tiene en la casa y el tiempo que se utiliza cada aplicación. Ante esta situación, se plantean serios cuestionamientos éticos, incluyendo los relacionados con las *cookies* de navegación o el rastreo de direcciones IP que son propias de la privacidad de las personas y que, de una u otra forma, terminan convirtiéndose en información altamente deseada por múltiples empresas, para luego venderla (García, 2023).

Por tanto, se debe saber que el rastro digital se crea en el momento mismo que un usuario brinda información personal en sus correos electrónicos y en las redes sociales, el cual permite conocer a profundidad el tipo de publicaciones que utiliza, sus comentarios, la ubicación que tiene en tiempo real, el estado de ánimo ante determinados asuntos, la percepción sobre la economía general o personal, el nivel cultural y las cosas o acciones que son de su mayor interés. En resumen, «saben todo» de usted o de la empresa.

La huella digital se manifiesta por medio de tres fuentes:

1. Datos públicos que son los que tienen información de obligaciones y beneficios sociales, todo lo relacionado a aspectos tributarios y declaraciones de impuestos, información sobre tarjetas de crédito, becas estatales, legislación y resoluciones judiciales, entre otras.
2. Datos publicados por otras personas como son fotos, publicaciones de familiares, amigos, organizaciones que están presentes en redes sociales.
3. Datos generados por uno mismo que resultan del envío de comentarios, publicaciones, fotos, eventos, así como cuando se envía el currículum, formularios de diversos tipos, perfiles de contactos en redes, contenidos especiales como reproducciones y vídeos favoritos (Gobierno de Argentina, 2023).

Con toda esta información personal–junto con la de miles de otras personas y organizaciones de todo tipo–las empresas especializadas en capturar e integrar rastros digitales crean perfiles y generan estadísticas de usuarios. Estos perfiles proporcionan información detallada y precisa sobre

los potenciales consumidores de los productos que están en el mercado o que esperan lanzar al mercado. Los usuarios, en general, no ponen atención al uso y comercialización de sus datos, ni que mediante el uso de *cookies* capturan un gran número de datos personales que son vinculados con las de otros usuarios y convertidos en un hilo conectado. Las cookies se emplean para mejorar la experiencia de uso en línea al agilizar la carga de los sitios web más visitados de manera frecuente se carguen más rápidamente y proporcionando mayor seguridad en las transacciones individuales (Gobierno de Argentina, 2023).

En efecto, todas las empresas especializadas en capturar e integrar rastros digitales, conocidas como *data brokers*, trabajan para satisfacer un gran mercado sombra donde la información personal de los usuarios la venden a terceros. Además, los *data brokers* también brindan servicios de análisis sectorial o especializado, para ayudar a capturar clientes directamente o para realizar campañas de mercadeo (Bejerano, 2023).

Muchas de estas empresas tratan de diferenciarse, donde algunas dicen que *ceden* los datos y otras que los *venden*. Entonces, la pregunta pertinente es ¿cuál es la diferencia entre *ceder* los datos y venderlos? Las actividades comerciales de estas empresas ya llamaban la atención desde 2005, y el *Congressional Research Service,* mostró su preocupación de las actividades y seguridad de los *data brokers* y en su informe RS22137 del 3 de mayo de 2007, donde expresa en su Introducción:

> En los primeros meses de 2005, dos corredores de datos líderes, LexisNexis y ChoicePoint, anunciaron que personas no autorizadas habían violado sus medidas de seguridad y habían obtenido información personal... de cientos de miles de personas. Estas empresas y otras similares (data brokers) operan en gran medida libres de regulaciones federales y estatales. Los escándalos recientes han llevado a solicitar una regulación más estricta de la industria del corretaje de datos, creando la necesidad de información más completa sobre el tipo de empresas que componen esta industria y los tipos de servicios que brindan (párr.1).

Más adelante, el *Congressional Research Service,* señaló los creciente ingresos de estas dos empresas:

> ChoicePoint vende datos a una amplia variedad de entidades, desde aseguradoras hasta autoridades policiales. Originalmente formada como una escisión de la agencia de informes crediticios Equifax en 1997, ChoicePoint ha crecido hasta dominar el mercado de corretaje de datos mediante la compra de una serie de empresas de data brokers más pequeñas y especializadas y operando varias subsidiarias en varios

> estados. Los ingresos anuales totales de ChoicePoint han crecido en este período de $585 millones en 2000 a más de $1 billón en 2006. (Congressional Research Service, 2007, párr. 6)

La actividad e ingresos de este tipo de empresas han continuado creciendo por lo que la empresa analista *Transparency Market Research* (2022) estimó los ingresos globales de los *data brokers* en US$240.3 billones en 2021 y los proyectó hasta US$ 462.4 billones en 2031, dada una tasa de crecimiento esperada de 6.8 % anual. Otra perspectiva de crecimiento del mercado de corretaje de datos es el volumen esperado de datos que se transmiten. Según Estatista (2023) el número de usuarios de internet en el mundo llegó a 5,282 millones en 2023, lo que representa el 65.7 % de los 8,045 millones de habitantes; mientras que los dispositivos conectados en el mundo rondarían los 16,700 millones, y los usuarios de redes sociales serían uno 4,898 millones. Además, diversos estudios muestran que a mediados de 2023 se generaban alrededor de 16 yottabytes de datos que equivalen a alrededor de 1.3 trillones de tuits (García, 2023).

Obviamente, todo indica que el mercado de corretaje de datos seguirá creciendo con fuerza y la venta de datos continuará subiendo, lo que requerirá la formulación de leyes que protejan a los usuarios de la venta de sus informaciones personales y la manipulación a que pueden someterse.

5. Un mundo de mucha información que está convirtiendo a los seres humanos en menos pensantes

Actualmente, las sociedades disponen de más información, pero, en general, no la transforman en sabiduría. Al contrario, parece que nos volvemos más estúpidos, ya que, sin verificarla, utilizamos y repetimos informaciones falsas (fake news) y mal intencionadas que fomentan conflictos y dividen a las sociedades. En el pasado, la información buscaba la verdad, para tener más sabiduría y, con ella, más poder; ahora, la información se ha convertido en una expresión de poder.

El mundo ha entrado en un nuevo colonialismo basado en datos. Antes, para conquistar un territorio o país y convertirlo en una colonia se necesitaban fuerzas militares; ahora, necesita apoderarse, controlar y utilizar datos para convertir a las sociedades o al mundo en una colonia supeditada. «Unas pocas compañías o un gobierno que consigan recolectar los datos de todo el mundo, podrían convertir el resto del globo en colonias de datos: territorios dominados no mediante la fuerza militar manifiesta, sino con información» (Harari, 2024, p. 429). Esta situación se manifestará con mayor fuerza si no se establecen marcos regulatorios sólidos y bien definidos que los controlen.

Harari (2024) alerta que, si este entorno es dominado por unos pocos y utilizado por políticos populistas o de pensamiento totalitario que cuenten con algoritmos y manejen una gran cantidad de chabots, influirán directamente en la forma de pensar de las personas, poniendo en riesgo a los sistemas democráticos que se sustentan en la libertad, la libre expresión, la tolerancia y la búsqueda de la justicia en todos sus sentidos.

Retomando la pregunta central que plantea Harari: «¿por qué somos tan autodestructivos (los seres humanos)? Somos, a un tiempo, los animales más inteligentes y los más estúpidos de la Tierra. Somos tan inteligentes que podemos producir misiles nucleares y algoritmos superinteligentes... (pero) somos tan estúpidos que, aunque no estemos seguros de poder controlarlos, y aunque no hacerlo podría conducirnos a la destrucción, seguimos produciendo estas cosas» (p.464).

Por esto, en este estudio se enfatiza la necesidad de formular políticas públicas y marcos jurídicos para controlar y castigar los abusos en el uso de la IA. Si el poder lo retienen individuos con características como las de Stalin y Hitler que utilizaron la información para manipular a la gente y crear situaciones especiales para beneficiar sus «causas», ahora potenciada por la IA, el riego de caer en un régimen totalitario es cada vez mayor; y si esto ocurre a nivel mundial, la civilización humana estaría en peligro de caer en la ley de la jungla. Entonces, el desafío de las sociedades es enfocar sus esfuerzos para que la IA no actúe en contra del progreso de la humanidad, sino que se convierta en una herramienta tecnológica que contribuya a construir una nueva etapa de mayor prosperidad y justicia (Harari, 2024). Además, será fundamental crear condiciones que permitan a cada persona responder a una pregunta esencial: ¿qué somos, para qué vivimos y cómo podemos ser mejores y alcanzar la felicidad? Esa es la cuestión.

III. Legislaciones en vigencia y en procesos de aprobación

La preocupación ante el avance de la IA y el impacto que está teniendo en el mundo se manifestó en la Cumbre del Grupo de los Siete (G7) realizada en Hiroshima en mayo de 2023. En el punto 1, del comunicado expresaron que estaban «más unidos que nunca (para) hacer frente a los retos mundiales... y fijar el rumbo hacia un futuro mejor». Sobe la IA declararon estar «decididos a trabajar juntos y con otros» para «avanzar en... la gobernanza inclusiva de la inteligencia artificial y la interoperabilidad para lograr nuestra visión común y el objetivo de una IA digna de confianza, en consonancia con nuestros valores democráticos compartidos» (Centro de Documentación Europea, 2023).

Obviamente, este comunicado reitera la necesidad de contar con marcos jurídicos que permitan crear o mantener un entorno seguro y de confianza en el uso de la IA, sin restarle espacio a la innovación en esta área tecnológica. Luego, el 21 de marzo de 2024, la Organización de las Naciones Unidas (ONU) adoptó una resolución histórica ante el rápido e innovador avance tecnológico de la IA y su creciente utilización en todo el mundo para establecer una regulación global que tienda a garantizar a los usuarios su utilización de manera segura y confiable, y reducir las desigualdades entre los países, dando las primeras directrices para que las normativas estén apegadas a estándares internacionales. Esta resolución de la ONU para regular un área innovadora emergente fue propuesta por Estados Unidos y copatrocinada por otras 122 naciones, fue adoptada por consenso, sin votación, lo que significa que cuenta con el apoyo de los 193 países miembros de la ONU. Ella no es vinculante, es una *ley blanda*, porque los firmantes no están obligados a cumplirla (ONU, 2024).

Esta resolución solicita a los Estados que no utilicen sistemas de IA si ellos no cumplen las normas internacionales de derechos humanos o los puedan poner en riesgo. Por tanto, la promoción de los sistemas de IA debe estar sustentada en medios «seguros y confiables», desde su diseño, desarrollo y despliegue, para que su uso beneficie el desarrollo sostenible de todos los países, para facilitar el logro del Objetivos de Desarrollo Sostenible. En la resolución también se enfatizó que «Los mismos derechos que tienen las personas fuera de línea deben protegerse también en línea, incluso durante todo el ciclo de vida de los sistemas de inteligencia artificial» (párr. 6). En consecuencia, se exhortó «al sector privado, a la sociedad civil, a las organizaciones de investigación y a los medios de comunicación a desarrollar y apoyar enfoques y marcos normativos y de gobernanza relacionados con el uso seguro y fiable de la IA» (párr. 7).

Entre los países del mundo hay grandes diferencias en el nivel de desarrollo económico, social, político, jurídico y ambiental. Ahora se debe incluir el área tecnológica, porque se ha convertido en un factor clave para el progreso de las sociedades. Por tanto, será determinante que los países más avanzados y organismos multilaterales creen y ejecuten programas de cooperación para potenciar y lograr un acceso inclusivo y equitativo en las sociedades menos avanzadas, para aminorar o, en lo posible, eliminar tanto la brecha como el analfabetismo digital, para que, con las nuevas, innovadoras y disruptivas tecnologías, especialmente de IA, logren mejorar el nivel y condiciones de vida de la gente.

1. Legislación en la Unión Europea

En esta parte se presenta un resumen de la Legislación en la Unión Europea (UE) que se expone en detalle con sus respectivas fuentes en el Anexo III.

Desde octubre de 2020, el Parlamento Europeo visualizaba una legislación sobre la IA en la UE para promover la innovación, garantizar la seguridad y proteger los derechos humanos. En noviembre de ese año la Comisión Especial del Parlamento Europeo sobre Inteligencia Artificial en la Era Digital (AIDA, por sus siglas en inglés) comenzó una investigación y después de 18 meses publicó un informe, donde propuso una *hoja de ruta* y dio una visión integral «para conseguir una posición común a largo plazo que destaque los valores y objetivos principales de la UE sobre la IA» (Parlamento Europeo, 2022, párr. 1). El informe, también, resaltó el compromiso de trabajar para reforzar la infraestructura digital para que todos los ciudadanos tengan acceso a los servicios disponibles, apoyar la expansión de la banda ancha, la fibra y la 5G, y dar prioridad a las tecnologías innovadoras. Además, se manifestó el compromiso de enseñar competencias de IA para quienes deseen tener y utilizar estas habilidades en la vida y en el trabajo (Parlamento Europeo, 2022).

Así se dieron los primeros pasos para legislar sobre la IA en la UE y tras diversos estudios y consultas abiertas se lograron aprobar o actualizar diferentes leyes. Entre 2022 y 2023 el Parlamento Europeo trabajó para regular la transformación digital, y aprobó la Estrategia y actualizó o aprobó las siguientes leyes y reglamentos:

a. Reglamento General de Protección de Datos (27 de abril de 2016)
b. Ley de ciberseguridad de la Unión Europea (17 de abril de 2019)
c. Estrategia europea sobre datos (19 de febrero de 2020)
d. Ley de Gobernanza de Datos, DGA (6 de abril de 2022)
e. Código de buenas prácticas en materia de desinformación reforzado de 2022 (presentado el 16 de junio de 2022)
f. Ley de Mercados Digitales, DMA (19 de octubre de 2022)
g. Ley de Servicios digitales, DSA (19 de octubre de 2022)
h. Ley de Resiliencia Operacional Digital, DORA (14 de diciembre de 2022)
i. Ley de ciberresiliencia de la Unión Europea, CRA, (15 de septiembre de 2022)
j. Ley del mercado de criptoactivos, MICA (20 de abril de 2023)
k. Ley de Datos (9 de noviembre de 2023)
l. Ley de Inteligencia Artificial de la Unión Europea, (8 de diciembre de 2023 y respaldado por la Eurocámara el 13 de marzo de 2024)

a. El 27 de abril de 2016 (216/679) se aprobó el *Reglamento General de Protección de Datos* (RGPD) de la UE en el que establecieron los principios y normas para la protección en el tratamiento de los datos de carácter personal, sin discriminar por nacionalidad o residencia y mantener un pleno respeto de sus libertades y derechos fundamentales.

b. En septiembre de 2017, se propuso una *Ley de Ciberseguridad* para enfrentar los ciberataques y garantizar una ciberseguridad sólida; se aprobó el 17 de abril de 2019. El objetivo de esta Ley es «garantizar el correcto funcionamiento del mercado interior... (y) alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión Europea». Con esta Ley también se creó el marco europeo de certificación de la ciberseguridad.

c. *La Estrategia Europea de Datos*, difundida en Bruselas el 19 de febrero de 2020, reconoció que las tecnologías digitales ya estaban transformando la economía y a toda la sociedad. Por esto, ante el desarrollo del mundo digital puso al centro a las personas, su defensa y la promoción de sus valores y derechos, demandando «delimitar el rumbo del modelo de economía digital de la Unión Europea... (para) crear un mercado único de datos que garantice la competitividad mundial y la soberanía de los datos de Europa».

d. El 6 de abril de 2022, se aprobó la *Ley de Gobernanza de Datos* (DGA por sus siglas en inglés), para aumentar la confianza en el intercambio de datos, promover la innovación, la creación de nuevos productos y servicios, como medios para facilitar la transición ecológica y la transformación digital en Europa. La DGA, también, reguló los vacíos para evitar los abusos del sistema que pudieran realizar operadores de países que no son de la UE.

e. El 16 de junio de 2022 se aprobó *el Código de buenas prácticas en materia de desinformación reforzado de 2022*, luego de un proceso de revisión iniciado en junio de 2021. El Código tiene como objetivo convertirse en una medida de mitigación y un Código de Conducta incluido en el marco co-regulador de la Ley de Servicios Digitales (DSA).

f. El 14 de septiembre de 2022, se adoptó el *Reglamento de la Ley de Mercados Digitales* (DMA por sus siglas en inglés) que fijó como objetivo «contribuir al correcto funcionamiento del mercado interno mediante el establecimiento de normas armonizadas que garanticen a todas las empresas mercados competitivos y justos en el sector digital» en la UE.

g. El 19 de octubre de 2022, se aprobó la *Ley de Servicios Digitales* (DSA, siglas de Digital Services Act) que estableció nuevos derechos para los usuarios para mejorar los servicios, brindar mayor transparencia en la publicidad, que las plataformas de gran tamaño y motores de búsqueda asumieran mayores responsabilidades y proteger de mejor manera a los menores. Además, incluyó normas para regular los servicios digitales, enfrentar contenidos ilegales y mitigar los riesgos causados por «la desinformación o la manipulación electoral, la ciberviolencia contra las mujeres o las agresiones a menores en línea».

h. El 14 de diciembre de 2022, se aprobó la *Ley de Resiliencia Operacional* Digital (DORA por sus siglas en inglés de Digital Operational Resilience Act) que estableció que las normas de las finanzas digitales son vinculantes en todos sus elementos por lo que las deberán aplicar todos los Estados miembros de la UE.i. El 15 de septiembre de 2022, se presentó una propuesta de Ley de Ciber Resiliencia (CRA, siglas en inglés de *Cyber Resilience Act*) para establecer requisitos de ciberseguridad para todos los productos con elementos digitales, aumentar la capacidad sistémica y habilidades de una organización para resistir y/o recuperarse de ataques cibernéticos malignos. Se espera que sea sometida a votación en abril de 2024.

j. El 1º de abril de 2022 el Parlamento Europeo señaló los «peligros de las criptomonedas» y la necesidad de tener una legislación para regular sus actividades, evitar manipulaciones, fraudes financieros y otras actividades ilícitas. El 20 de abril de 2023 se aprobó la *Ley del mercado de criptoactivos*, Ley MICA (Markets in Crypto-Assets) que regula la emisión y uso de criptoactivos y *'stablecoins'*, y que facilita la inclusión financiera. En ella, también se establecieron medidas para prevenir el uso de criptomonedas en actividades delictivas.

k. El 11 enero de 2024 se aprobó la *Ley Europea de Datos* para estimular la innovación, eliminar los obstáculos al acceso a los datos y abrirlos a todos los sectores. Con esta Ley, los productos conectados deberán ser diseñados y fabricados para que los usuarios puedan tener acceso, utilizar y compartir sin dificultades y de manera segura los datos. Además, protege a las MIPYMES ante las grandes empresas que tratan de imponer cláusulas abusivas en los contratos de intercambio de datos y para resguardar los secretos comerciales.

l. La primera propuesta de regulación de la IA se presentó el 21 de abril de 2021 y después de múltiples consultas y debates, el Consejo Europeo adoptó esta propuesta el 21de mayo de 2024. Esta normativa tuvo como objetivo establecer un marco normativo y jurídico común en la UE para garantizar que los sistemas sean «seguros, transparentes, trazables, no discriminatorios y respetuosos con el medio ambiente» (Parlamento Europeo, 2024, párr. 3), sin ponerle trabas a la innovación en esta área tecnológica.

2. Regulación de la Inteligencia Artificial en el Reino Unido

En esta parte se presenta un resumen de la Legislación en el Reino Unido que se expone en detalle con sus respectivas fuentes en el Anexo IV.

La Oficina de Inteligencia Artificial (*Office for Artificial Intelligence* – OAI) presentó al Parlamento en septiembre de 2021 el *Plan decenal para hacer de Gran Bretaña una superpotencia mundial en IA* cuyos puntos estratégicos son:

1) invertir y planificar las necesidades a largo plazo del ecosistema de IA para mantener un liderazgo como superpotencia científica y de IA; 2) apoyar la transición hacia una economía basada en la IA, garantizando que la IA beneficie a todos los sectores y regiones; y 3) garantizar que el Reino Unido implemente correctamente la gobernanza nacional e internacional de las tecnologías de IA para fomentar la innovación, la inversión y proteger al público.

El Proyecto de *Ley de Protección de Datos e Información Digital* (DPDIB, siglas de *Data Protection and Digital Information Bill*), se presentó el 18 de julio de 2022, incluyó un conjunto de propuestas de regulación de la inteligencia artificial (IA), sin considerar las normas establecidas en el Reglamento General de Protección de Datos (RGPD) de la UE. En este contexto, se propusieron condiciones para garantizar la protección de los usuarios y mantener una libre y sana competencia para estimular su desarrollo y uso responsable, especialmente, del ChatGPT y Office 365 *Copilot.*

El 15 de marzo de 2023, se comenzó a preparar un código de prácticas sobre los derechos de autor e IA, que tiene como objetivo facilitar que las licencias para la minería de datos estén totalmente disponibles, para superar las barreras que enfrentaban las empresas y usuarios de IA y garantizar las debidas protecciones para los titulares de derechos de propiedad.

En relación con el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales firmado por la UE el 10 de junio de 2013, el Reino Unido se comprometió a ratificarlo e implementarlo. Si bien la legislación del Reino Unido ya cumple en gran parte con el tratado, se reconoce que hay ciertas áreas que requerirán cambios para proteger a los artistas audiovisuales y evitar todo trato ofensivo de sus interpretaciones, incluyendo las actuaciones de actores, músicos, bailarines y otros artistas en películas, programas de televisión y otras grabaciones audiovisuales. En el Reino Unido preocupa que el Tratado no tiene disposiciones para que los artistas audiovisuales protejan sus derechos contra los deepfakes generados con IA.

3. Acuerdos para regular la Inteligencia Artificial en diversos países del mundo

La Primera Cumbre Mundial sobre los Riesgos de la IA tuvo lugar en *Bletchley Park*, Reino Unido, el 1º de noviembre de 2023, en la que participaron altos dirigentes políticos, grandes empresas tecnológicas, representantes del sector académico y de la sociedad civil para iniciar una conversación global crítica sobre los peligros que presentan los vertiginosos avances de esta tecnología. El Acuerdo que se logró en *Bletchley Park* fue firmado por 29 países (Anexo IV).

La preocupación de los asistentes a esta cumbre se centró en que los sistemas de IA son utilizados a diario en múltiples áreas de trabajo y otras que se sumarán en el futuro. Ante esta irreversible situación, los formuladores de políticas públicas deben formular regulaciones para que el potencial transformador de la IA se aprovechado de manera amplia e inclusiva, sin discriminaciones, protegiendo los derechos humanos, especialmente, de los menores y personas de la tercera edad. Estas regulaciones, también, deberán garantizar transparencia, explicabilidad, seguridad, privacidad, consideraciones éticas, protección de datos, métodos de rendición de cuentas y sanciones, entre otras.

Además, hubo consenso en que gran parte de los riesgos relacionados con la IA son de tipo internacional, por lo que, se deben abordar mediante la cooperación y el intercambio de información a nivel internacional y la creación de un marco regulatorio y de gobernanza en todos los países para reducir los riesgos, garantizar la transparencia y la rendición de cuentas, manteniendo un enfoque pro-innovación para maximizar los beneficios de la IA. También, se acordó continuar las investigaciones relacionadas con la seguridad de la IA para garantizar que los beneficios de los avances tecnológicos puedan aprovecharse de manera responsable en beneficio de todos.

Una visión interesante sobre la IA la dio a conocer Brad Smith (2024), presidente de Microsoft, quien expresó «cuanto más poderosa se vuelve una tecnología, más fuertes tienen que ser los controles que la acompañen» (Fernández de Lis, 2024, párr. 1), un claro mensaje sobre qué deben hacer las autoridades en todos los países del mundo.

4. Legislación en Estados Unidos de América

En esta parte se presenta un resumen de la Legislación en Estados Unidos de América que se expone en detalle con sus respectivas fuentes en el Anexo V.

Joseph R. Biden, presidente de EUA, firmó el 30 de octubre de 2023, el *Decreto Ejecutivo sobre el desarrollo y uso seguro y confiable de la inteligencia artificial (Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence)* para reducir los riesgos de un desarrollo sin control de esta tecnología. Este Decreto Ejecutivo se consideró como un mensaje de liderazgo y acción estratégica previa a la participación de EUA en la Primera Cumbre Mundial sobre los Riesgos de la IA en *Bletchley Park.*

El decreto reconoce que el uso responsable de la IA puede ayudar a resolver desafíos y contribuir a que el mundo sea más próspero, productivo, innovador

y seguro; pero, también, señala que su uso irresponsable puede causar daños sociales como fraudes, discriminación, prejuicios y desinformación; desplazar y quitar poder a los trabajadores, reprimir la competencia y crear riesgos para la seguridad nacional. Para mitigar estos riesgos, considera necesaria la participación de toda la sociedad para garantizar una IA segura y confiable (Giandana, 2024).

Además, este Decreto Ejecutivo contiene mandatos específicos para garantizar la seguridad de la tecnología de IA, la promoción de la innovación y la competencia, la protección de los trabajadores de apoyo asegurando que la IA en los trabajos promueva el bienestar de los empleados; promover la equidad y los derechos civiles; proteger los consumidores, pacientes, pasajeros y estudiantes, así como la privacidad de las personas.

5. Regulación de la IA en la República Popular China

En esta parte se presenta un resumen de la regulación de la IA en la República Popular China que se expone en detalle con sus respectivas fuentes en el Anexo VI.

El gobierno de la República Popular China, de aquí en adelante 'China', formuló un Plan de País, así como una serie de leyes, normas y documentos orientadores en torno al uso de tecnologías, así como en el área de IA, entre las que destacan 11 documentos:

1. Reglamento sobre la Administración de los Servicios de Información de Noticias en Internet del 25 de septiembre de 2005.
2. Plan *Made in China* 2025 presentado en 2015.
3. Ley de Ciberseguridad de la República Popular China del 1º de junio de 2017.
4. Plan de desarrollo de inteligencia artificial de próxima generación, presentado el 8 de julio de 2017.
5. Marco de IA Confiable propuesto en julio de 2021.
6. Normas Éticas para la Inteligencia Artificial de Nueva Generación 25 de septiembre de 2021.
7. Orientación sobre el fortalecimiento de la gobernanza integral de los algoritmos de los servicios de información de Internet presentado el 29 de septiembre de 2021.
8. Ley de Protección de Datos Personales o Ley de Seguridad de Datos de la República Popular China del 30 de septiembre de 2021.
9. Ley de Protección de Información Personal de la República Popular China del 20 de agosto de 2021, en vigor desde el 10 de noviembre de

2021.Ley de Protección de Datos Personales o Ley de Seguridad de Datos de la República Popular China del 30 de septiembre de 2021.

10. Ley de Protección de Información Personal de la República Popular China del 20 de agosto de 2021, en vigor desde el 10 de noviembre de 2021.

11. Disposiciones de gestión de recomendaciones algorítmicas del servicio de información de Internet, en vigor el 10 de marzo de 2022 –modificó la normativa de septiembre de 2021–.
12. Medidas de Gestión del Servicio de Inteligencia Artificial Generativa, en vigencia desde el 1 de enero de 2023

1. *El Reglamento sobre la Administración de los Servicios de Información de Noticias en Internet*, entró en vigor el 25 de septiembre de 2005, y fue preparado antes del impacto de nuevas aplicaciones y de la IA, que tuvo una concepción eminentemente reguladora con el objeto de «estandarizar los servicios de información de noticias de Internet y satisfacer la demanda del público de información de noticias de Internet» para mantener «la seguridad nacional y los intereses públicos, proteger los derechos e intereses legítimos de las unidades de servicios de información de noticias de Internet y promover la información de noticias de Internet» de modo que se pudiera «asegurar el sano y ordenado desarrollo de los servicios de información».

Este reglamento aplica a todo proveedor «de servicios de información de noticias de Internet dentro del territorio de la República Popular China», y aplica a toda «información de noticias de actualidad, incluida la política, la economía, el ejército, la diplomacia, etc. ... (así como a) Informes y comentarios sobre asuntos sociales y públicos, así como informes y comentarios sobre emergencias sociales» difundida por internet.

2. Con el Plan «*Made in China 2025*», presentado en 2015, el gigante asiático dejó en claro su objetivo de convertirse en una potencia con la capacidad de liderar e influir en los estándares mundiales de innovación y en las cadenas de suministros hacia 2030. Este plan, con una clara visión de libre mercado tiene como objetivo principal convertir a China en una potencia líder en innovación y tecnología para el año 2025 y más allá. Está centrado en incentivar la innovación, mejorar la calidad de los productos manufacturados, crear marcas globales chinas, aplicar métodos de fabricación ecológicos, mejorar la eficiencia y la producción industrial. Además, aumentar la autosuficiencia tecnológica y reducir la dependencia de tecnologías extranjeras en áreas clave como la inteligencia artificial, la robótica, la tecnología de la información y la energía renovable.

3. La *Ley de Ciberseguridad de la República Popular China*, aprobada el 6 de noviembre de 2016, entró en vigor el 1º de junio de 2017, tiene como propósito

«garantizar la ciberseguridad; salvaguardar la soberanía del ciberespacio y la seguridad nacional, y los intereses sociales y públicos; proteger los derechos e intereses legítimos de ciudadanos, personas jurídicas y otras organizaciones; promover el sano desarrollo de la informatización de la economía y la sociedad»; y se aplica a la «construcción, operación, mantenimiento y uso de redes, así como a la supervisión y gestión de la ciberseguridad» en el territorio continental de China. la cual es «aplicable a la construcción, operación, mantenimiento y uso de redes, así como a la supervisión y gestión de la ciberseguridad dentro del territorio continental de la República Popular China».

Esta normativa establece que «el Estado debe tomar medidas para proteger la infraestructura de información crítica contra ataques, intrusiones, interferencias y destrucción... (así como) sancionar las actividades cibernéticas ilícitas y delictivas»; propugnar «una conducta en línea sincera, honesta, sana y civilizada», para que se adopten «medidas para aumentar la conciencia y el nivel de ciberseguridad de toda la sociedad... (para que) participe conjuntamente en el avance de la ciberseguridad». Además, señala que es un deber del Estado establecer «un sistema de monitoreo, de alerta temprana y comunicación de información... para fortalecer los esfuerzos de recopilación, análisis y presentación de informes de información de ciberseguridad».

Finalmente, en su articulado establece severas sanciones que van desde «una suspensión temporal de operaciones, una suspensión de negocios por correcciones, el cierre de sitios web, la cancelación de los permisos de operación pertinentes o la cancelación de licencias comerciales».

Ante la creciente utilización y desarrollo de la IA, el Consejo de Estado de la República Popular China presentó, el 8 de julio de 2017, el *Plan de desarrollo de inteligencia artificial de próxima generación* que estableció las normas éticas en el uso como en la protección de la información personal y el control humano, así como evitar monopolios en las aplicaciones de IA y otras tecnologías relacionadas, evitar la violación de la privacidad, y la pérdida de información.

El plan demanda cumplir estrictamente sus reglas, normas y regulaciones del mercado, la competencia, las transacciones y otras actividades similares, sin alterarlo con la conformación de monopolios de plataformas; prohíbe las violaciones de derechos y actos maliciosos en el uso de productos y servicios de IA, y demanda «Fortalecer el autocontrol en Actividades relacionadas con la I+D de IA, incorporar activamente la ética de la IA en cada eslabón del proceso tecnológico de I+D, y realizar conscientemente autoexámenes, fortalecer la autogestión y no participar en I+D de IA que sea poco ético o inmoral».

5. En julio de 2021, la Academia China de Tecnología de la Información y las Comunicaciones propuso un *Marco de IA Confiable* con el objetivo de lograr una gobernanza de la IA desde la perspectiva de la industria que trabaja y desarrolla esta tecnología. Además, señaló que, aparte de definir normativas para el estado de la tecnología, los productos y los servicios relacionados, se debe incluir una metodología para generar «confiabilidad» en todos los aspectos tecnológicos, como fiabilidad y controlabilidad, transparencia y explicabilidad, protección de datos, responsabilidad, diversidad e inclusividad, entre otros.

En este marco se presentaron propuestas para reducir los riesgos asociados con la tecnología de IA, las cuales han generado una crisis de confianza por la falta de seguridad de los algoritmos que se utilizan en sus aplicaciones. Se han identificado casos de opacidad algorítmica, discriminación en el uso e información sobre los datos que conlleva a toma de decisiones sesgadas, dificultades para atribuir responsabilidades a empresas y personas en acciones incorrectas o resultados negativos, así como el uso inapropiado, el abuso y la fuga de datos. Este Marco responde a los señalamientos expuestos, mediante la puesta en marcha de un conjunto de normas que garanticen una gobernanza ética y busquen un equilibrio entre la innovación y una sólida gestión de riesgos.

6. El 25 de septiembre de 2021, China publicó las Normas Éticas para la Inteligencia Artificial de Nueva Generación. Estas normas tienen como objetivo «incorporar la ética en todo el ciclo de vida de la IA y promover la equidad, la justicia, la armonía y la seguridad», evitando «problemas como el sesgo, la discriminación, la privacidad y las fugas de información». Con esto, China buscar convertirse en el líder mundial en IA y, hacia el 2025, ser el mayor referente de esta tecnología.

7. *Orientación sobre el fortalecimiento de la gobernanza integral de los algoritmos de los servicios de información de Internet* que responde al continuo proceso de normar los avances tecnológicos, se presentó el 29 de septiembre de 2021. Luego, el 11 de abril de 2023, se publicó el borrador *Medidas de Gestión del Servicio de Inteligencia Artificial Generativa,* para recibir comentarios y promover el desarrollo sano y robusto de las aplicaciones que utilizan IA generativa. Estas medidas, que entraron en vigor el 10 de enero de 2023, tienen como «finalidad de establecer un modelo de gobernanza integral de la seguridad algorítmica en alrededor de tres años».

Esta orientación, realmente, es una guía que orienta los métodos y normas para administrar, utilizar y desarrollar nuevas tecnologías y sus capacidades para utilizarse en redes, así como para garantizar alta seguridad y contar eficientes sistemas de supervisión, sin coartar el desarrollo y avances tecnológicos. También, demanda, entre otros, «Adherirse a la orientación correcta, fortalecer la conciencia sobre la ética científica y tecnológica, la conciencia

sobre la seguridad... (para) aprovechar plenamente el papel de los servicios algorítmicos en la difusión de energía positiva y crear un ciberespacio limpio y recto (que) sea justo, transparente y explicable, y (logre) proteger plenamente los derechos e intereses legítimos de los internautas» así como «promover vigorosamente el trabajo de investigación de innovación de algoritmos... los derechos de propiedad intelectual de los algoritmos, fortalecer el despliegue y la promoción de algoritmos... (para) mejorar la competitividad central de los algoritmos de China».

8. La nueva *Ley de Seguridad de Datos,* también, conocida como *Ley de Protección de Datos Personales* fue aprobada el 20 de agosto de 2021 (en vigor el 10 de noviembre de 2021), en la que se establece que «La información personal... está protegida por la ley y ninguna organización o individuo puede infringir los derechos e intereses... (en el uso de esta) información». De esta manera, se busca promover el uso razonable de la información personal, estandarizar su tratamiento y salvaguardar el flujo legal y libre de la información. Esta norma jurídica tiene un alto grado de coincidencia con lo que dicta el Reglamento General de Protección de Datos de la UE.

El concepto de *información personal* lo define como toda «información relacionada con personas identificadas o identificables registradas electrónicamente o por otros medios, excluida la información anónima» y establece que el *procesamiento de información* es «la recopilación, almacenamiento, uso, procesamiento, transmisión, suministro, divulgación, eliminación... de información personal» que se debe realizar «de acuerdo con los principios de legalidad, legitimidad, necesidad y buena fe». Además, sentencia que nadie «puede comprar, vender, proporcionar o divulgar ilegalmente información personal de otras personas (ni) participar en actividades de procesamiento de información personal que pongan en peligro la seguridad nacional, seguridad o intereses públicos».

Esta norma define el concepto de información personal *sensible* como aquella que al ser utilizada ilegalmente o filtrada indebidamente viole los derechos de las personas o ponga en peligro su seguridad personal, especialmente, por la difusión de datos biométricos, condiciones de su salud, información financiera y creencia religiosa, entre otros. A esto, se suma, en China, la protección especial de la información de menores de 14 años. Asimismo, establece sanciones a quien maneje datos personales y viole las disposiciones de esta Ley.

Los procesadores de información personal que por razones comerciales necesiten proporcionar información fuera del territorio de China, deberá solicitar autorización y cuando sea solicitada por «organismos judiciales o de aplicación de la ley extranjeros» se podrá proveer «de conformidad con el principio de igualdad y reciprocidad».

Es de desatacar que si una persona encuentra que su información personal es inexacta o está incompleta tiene derecho a solicitar al procesador... que (la) corrija o complemente (Artículo 46). En caso de que se trate de una persona natural que ha fallecido, sus familiares, por derecho, pueden solicitar «copia, rectificación, supresión... (de) los datos personales relevantes... para sus propios intereses legales y legítimos, a menos que el causante haya otros arreglos antes de su muerte».

9. *La Ley de Protección de Información Personal* fue aprobada 20 de agosto de 2021 (Creemers y Webster, 2021), y entró en vigor desde el 10 de noviembre, la cual tiene como objeto «proteger los derechos e intereses de la información personal, estandarizar las actividades de manejo de la información personal y promover el uso racional de la información personal» (Artículo 1) por considerar que «ninguna organización o individuo puede infringir los derechos e intereses de información personal de las personas» (Artículo 2).

En adición, esta Ley señala que «Ninguna organización o individuo puede recopilar, usar, procesar o transmitir ilegalmente información personal de otras personas, ni vender, comprar, proporcionar o divulgar ilegalmente información personal de otras personas, ni participar en actividades de manejo de información personal que perjudiquen la seguridad nacional o el interés público». Además, dicta que «Las personas tienen derecho a conocer y decidir sobre sus datos personales, y tienen derecho a limitar o negar el tratamiento de sus datos... por parte de otros», salvo que las leyes o reglamentos estipulen lo contrario.

10. *Las Disposiciones de gestión de recomendaciones algorítmicas del servicio de información de Internet,* en vigor el 10 de marzo de 2022 –modificó la normativa de septiembre de 2021–. Estas disposiciones tienen como objeto «... estandarizar las actividades de recomendación algorítmica... promover la visión de valores fundamentales socialistas, salvaguardar la seguridad nacional y el interés social y público... estimular el sano desarrollo de los servicios de información en Internet».

En las disposiciones se establece que se «deberá respetar... la moral y la ética social, la ética comercial y la ética profesional y... los principios de equidad y justicia, apertura y transparencia... sinceridad e integridad». En adición, los proveedores «deberán obtener un permiso de servicio (licencia)... y estandarizar ... (los) servicios de recopilación, edición y difusión de información» y no podrán «generar ni sintetizar información noticiosa falsa». Sobre la base del concepto de mercado, se les ordena a los proveedores no «imponer restricciones irrazonables a otros proveedores... ni obstruir o destruir el funcionamiento regular de sus servicios de información de Internet prestados lícitamente, ni realizar actos monopólicos o de competencia indebida».

Como mecanismo de defensa de los derechos de los menores de edad las disposiciones requieren de los proveedores de este tipo de servicios proteger «en línea (a) los menores de edad... y facilitar que... obtengan información beneficiosa para su salud física y mental... adaptadas a las características específicas de los menores». En el caso de personas mayores, los proveedores deberán defender sus derechos «considerar plenamente (sus) necesidades... a la hora de salir, someterse a tratamientos médicos, consumir, manejar asuntos, y proporcionar servicios inteligentes... adaptados a las personas mayores... (prevenir fraudes) y facilitar que las personas mayores utilicen de forma segura» estos servicios.

11. Las *Medidas de Gestión del Servicio de Inteligencia Artificial Generativa* se publicaron, como *borrador*, el 11 de abril de 2023 para recibir comentarios y entraron en vigor el 15 de agosto de 2023. El objeto de estas medidas es «promover el desarrollo saludable y la aplicación estandarizada de la inteligencia artificial generativa». El concepto de *inteligencia artificial generativa* lo definió como la tecnología que genera texto, imágenes, sonidos, videos, códigos y otros contenidos basados en algoritmos, modelos y reglas.

En este contexto, se establece que el Estado tiene el deber de «apoyar la innovación, promoción y aplicación independientes y la cooperación internacional de tecnologías básicas como algoritmos y marcos de inteligencia artificial, y fomentar el uso prioritario de software, herramientas, recursos informáticos y de datos seguros y confiables», aunque dejando en claro que en la prestación de estos bienes o servicios se deberá cumplir con los requisitos de las diferentes normativas y «respetar la moral social, el orden público y las buenas costumbres». Consecuentemente, la normativa señala que las organizaciones e individuos *proveedores* «asumen la responsabilidad del productor del contenido... (y) la responsabilidad legal» si no cumple con «las obligaciones de protección de información personal». Por tanto, «los proveedores serán responsables de la legalidad de las fuentes de datos... para productos de inteligencia artificial generativa».

Los proveedores tampoco deben generar «contenidos discriminatorios por razón de raza, nacionalidad, género... del usuario».

Como se puede observar, de todo lo presentado anteriormente, China ha normado visionariamente el uso de nuevas tecnologías y su entorno desde 2005 incluyendo su visión estratégica de largo plazo. Por esto, Sundar Pichai, director ejecutivo de Google considera que por «la escala de trabajo que está llevando a cabo China en el ámbito de la IA [...] va a estar a la vanguardia de esta disciplina. Es un hecho» (López, 2023, párr. 5), y será imbatible en IA.

6. Legislación de IA en América Latina

En este apartado se presenta un resumen de la Regulación de la IA en América Latina, listando las normativas y propuestas que se exponen en detalle con sus respectivas fuentes en el Anexo VII.

Durante la Cumbre de Bletchley Park de 2023, en Reino Unido, 29 países, acordaron establecer normas para el desarrollo seguro de la IA para el bien de todos a nivel mundial (ver Parte III). El propósito de estas normativas es dar mayor seguridad y calidad en su uso en el sector público y establecer condiciones en el ámbito privado para generar confianza, dar transparencia, establecer principios y códigos de ética, y evitar el uso indebido de la IA.

Para evaluar la situación en el sector público se presentó el *Reporte de Gobierno Electrónico 2022 de las Naciones Unidas* (*UN E-Government Survey in 2022*) que ofrece una visión del gobierno digital, en los 193 países miembros, donde establece el Índice de Desarrollo del Gobierno Electrónico. En el caso de América Latina, el Índice ubica en el primer lugar a Uruguay, Chile en el segundo, Argentina en el tercero, Brasil en el cuarto y Costa Rica en el puesto cinco. El Salvador está ubicado en la 14ª posición entre 19 países de América Latina y en el 1170 en el mundo. Honduras está en la posición 19 en la región en el puesto 155 en el mundo (Ver Anexo VII, Cuadro 2).

Para medir la situación de seguridad en el sector privado, la Unión Internacional de Telecomunicaciones (UIT) presentó el 29 de junio de 2021 el *Índice de Ciberseguridad Global* 2020, que da a conocer el progreso de los compromisos sobre ciberseguridad en los 193 países miembros y Palestina. El propósito de este índice es «identificar las carencias, servir de hoja de ruta para orientar las estrategias nacionales, fundamentar los marcos jurídicos, ofrecer capacitación, destacar las prácticas idóneas, reforzar las normas internacionales y fomentar una cultura de la ciberseguridad». Este informe destacó que aún hay insuficiencias en cibercapacidad y demandó «abordar la brecha cibernética», así como tomar medidas de protección más firmes cuidando que sean accesibles y de fácil uso.

Según el *Índice de Ciberseguridad Global 2020*, en América Latina, Brasil ocupa el primer lugar y el 18º a nivel mundial; segundo, está México en el puesto 52 en el mundo; tercero, se ubica Uruguay y en el lugar 64 en el mundo. El Salvador está en el puesto 16 en América Latina y es el número 148 en el mundo. Cierra el índice Honduras, en el 19º lugar en la región, y en el puesto 178 en el mundo entre 181 países.

En adición se tiene el *Índice Latinoamericano de Inteligencia Artificial 2023* (ILIA 2023) que brinda una visión del estado actual de la IA en 12 países de América Latina: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Paraguay, Perú y Uruguay. Para cada país se generó una ficha con los hallazgos específicos en cada una de las tres dimensiones de estudio. Dimensión No 1. Factores habilitantes: «para que se constituyan y desarrollen sistema de IA robustos en cada país»; Dimensión No 2. Investigación, desarrollo y adopción: que «mide los avances del ecosistema de investigación y el desarrollo e innovación (I+D+i) del país considerando el desempeño del sector privado, la academia y el sector público»; y Dimensión No 3. Gobernanza, que «mide el nivel de desarrollo del entorno institucional y regulatorio con respecto a los ecosistemas de IA en América Latina», incluyendo las brechas que hay entre los países y las oportunidades para «impulsar un desarrollo en IA con un enfoque ético, transparente y equitativo».

Según los puntajes obtenidos por cada país en el ILIA 2023, en cada una de las tres dimensiones en América Latina; Chile, se ubica en el primer lugar; Brasil, en la segunda posición y; Uruguay, tiene el tercer puesto. De los países de Centro América, Costa Rica ocupa el 8º lugar y le sigue Panamá en el 9º puesto; y cierra este índice Bolivia, ubicada en 12º lugar (ver Anexo VII, Cuadro 9).

Según los resultados para los 12 países evaluados, más información de normas y leyes obtenida directamente de cada país, se tiene que, salvo Perú, ningún otro país cuenta con una ley específica para IA a marzo de 2024. Perú tiene la *Ley que promueve el uso de la Inteligencia Artificial en favor del desarrollo económico y social del país* del 13 de junio de 2023. En proceso, se tienen los siguientes casos:

1. En Brasil se formuló un *Proyecto de Ley para regular la IA* en febrero de 2022, aún no aprobado.

2. En Chile hay propuestas en proceso de aprobación, como el Proyecto de *Ley para regular los sistemas de IA, la robótica y las tecnologías conexas en sus distintos ámbitos de aplicación* desde el 26 de abril de 2023.

3. En Colombia hay en proceso cuatro Proyectos de Ley para regular la IA: dos para crear un marco regulatorio para el desarrollo, uso e implementación de IA, uno para normar el derecho de información y otro para complementar su uso con el derecho al trabajo. Además, en febrero de 2024 se presentó la *Hoja de Ruta* para garantizar la adopción ética y sostenible de la IA.

4. Uruguay se adhirió a la declaración regulatoria en la 4ª Asamblea de la Alianza Europea de IA en noviembre de 2023 para avanzar en

la cooperación conjunta de políticas y marcos regulatorios de esta tecnología.

Sobre la existencia de un Plan Nacional de IA, ocho países lo tienen y dos se enfocan en ciberseguridad:

- Argentina: cuenta con el *Plan Nacional de Inteligencia Artificial* que preparó entre 2018 y 2019. No hubo avances ni se retomó el tema, por lo que hay una estrategia nacional.
- Bolivia: no dispone de una ley específica para IA ni leyes para proteger los datos personales ni para combatir la ciberdelincuencia. No hay evidencias de casos de aplicación de regulaciones para el uso de IA.
- Brasil: a pesa de no tener un Plan de IA, tiene la *Estrategia Nacional de Ciberseguridad –E-Ciber–*, establecida por Ley del 5 de febrero de 2020, para aplicar durante cuatrienio 2020-2023.
- Chile: cuenta con una Política Nacional de IA en el año 2021 que establece lineamientos estratégicos para aplicar en materia de IA en los próximos 10 años.
- Colombia: posee una Política Nacional para la Transformación Digital e Inteligencia Artificial establecida el 8 de noviembre de 2019 con fundamentos para potenciar la generación de valor social y económico en el país.
- Costa Rica: está en proceso de formular la Estrategia de Inteligencia Artificial presentada el 27 de febrero de 2023 con el fin de establecer procesos destinados a la vinculación y transformación social y productiva. El objetivo es convertirse en un Hub centroamericano para el desarrollo de IA.
- México: tiene la Estrategia de Inteligencia Artificial de 2018, promulgada el 21 de marzo de 2018, con el objetivo de establecer un marco de gobernanza para fomentar el diálogo multisectorial, definir los usos y necesidades en la industria e identificar las mejores prácticas.
- Panamá: presentó la E*strategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas* el 12 de marzo de 2013, la cual no llegó a implementarse. Posteriormente, el 10 se septiembre de 2021, se aprobó la *Estrategia Nacional de Ciberseguridad para el período 2021-2024.*
- Paraguay: no dispone actualmente de un Plan o una Estrategia Nacional de IA, solo tiene el *Plan Nacional de Ciberseguridad* del 24 de abril de 2017, el cual busca coordinar las políticas públicas de ciberseguridad en un ambiente confiable y resiliente.
- Perú: cuenta con la *Estrategia Nacional de Inteligencia Artificial (ENIA)* para el período 2021-2026, cuyo objetivo es impulsar el desarrollo de la IA y convertir al país «en un referente regional en investigación, desarrollo y aplicaciones de esta tecnología».

- Uruguay: tiene la *Estrategia de Inteligencia Artificial* del 23 de abril de 2021 que fijó «las bases para la transformación digital, así como para promover y fortalecer su uso responsable en la Administración Pública».

Con relación a la vigencia de una ley sobre protección de datos, la situación por país es la siguiente:

- Argentina: tenía una Ley de Protección de Datos establecida el 4 de octubre de 2000 que, posteriormente, fue derogada y reemplazada por una nueva versión en junio de 2023, lo que indica una actualización de las normativas de protección de datos en el país.
- Brasil: cuenta con la Ley General de Protección de Datos del 14 de agosto de 2018 para garantizar la protección y privacidad de los datos personales. Además, se está preparando un proyecto para crear prototipos de políticas orientadas a que las empresas utilicen tecnologías para proteger y mejorar la privacidad, así como reducir los riesgos de violación de ella.
- Chile: cuenta con la *Ley Sobre Protección de la Vida Privada* del 18 de agosto de 1999.
- Colombia: tiene la *Ley de Protección de Datos Personales* del 17 de octubre de 2012, con nuevos conceptos normativos incorporados en el decreto único 1074 de mayo de 2015.
- Costa Rica: cuenta con la *Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales* del 27 de junio de 2011.
- Ecuador: tiene la *Ley orgánica de protección de datos personales* del 10 de mayo de 2021.
- México: posee la *Ley orgánica de protección de datos personales* de julio de 2010.
- Panamá: cuenta con la *Ley Protección de Datos Personales* del 26 de marzo de 2019.
- Paraguay: tiene la *Ley de Protección de Datos Personales Crediticios* del 28 de abril de 2020 para «garantizar la protección de datos crediticios de toda persona».
- Perú: posee la *Ley de Protección de Datos Personales* del 21 de junio de 2011.
- Uruguay: tiene la *Ley de Protección de Datos Personales* del 11 de agosto de 2008. Además, tiene la *Ley sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo*, del 6 de agosto de 2013, para la protección de la intimidad, la vida privada y la integridad de las personas en el uso de datos por parte de la Administración Pública.
- República Dominicana no se incluyó entre los 12 países que evaluó el Índice Latinoamericano de Inteligencia Artificial 2023. Sin embargo,cuenta con la *Ley de Protección Integral de los Datos Personales* del 13 de diciembre de 2013.

Están trabajando en el desarrollo y regulación de *Sandboxes* cinco países:

- Brasil: publicó Análisis Preliminar sobre el PL 2338/2023, el 6 de julio de 2023, que incluye normativas para la regulación de *sandboxes* para incentivar la innovación responsable y ética de la IA.
- Chile: se están realizando estudios para crear un *sandbox* regulatorio de IA para potenciar la innovación, atraer la inversión y estimular el aprendizaje conjunto público-privado.
- Colombia: se han aplicado *sandboxes* regulatorios de IA para la establecer normas y regulaciones para responder a los rápidos avances innovadores de la IA y la tecnología financiera (FINTECH).
- Costa Rica: comenzó a trabajar en un proceso que tomará nueve meses (agosto de 2018 y abril 2019) para hacer una propuesta para la creación de un *sandbox* de innovación, para estimular el crecimiento económico del país.
- México: es considerado pionero en regulación *sandbox* en América Latina, considerando que en marzo de 2018 introdujo en su legislación lo que denominó como «modelos novedosos», en la propuesta de Ley Fintech. El objetivo es el desarrollo de productos y servicios innovadores con ciertas excepciones regulatorias (Seminario, 2021).

Un sandbox es un entorno de prueba que permite experimentar con nuevas tecnologías en condiciones seguras y controladas. En el contexto regulatorio, un sandbox regulatorio es un marco legal que permite a las empresas innovadoras probar productos y servicios sin cumplir con todas las regulaciones existentes, bajo la supervisión de un regulador. A marzo de 2024, Australia, Reino Unido y Singapur han aprobado sandboxes regulatorios para incentivar el desarrollo de tecnologías de IA que sean seguras para utilizarlas en sectores como el financiero y tecnológico (Sandoval, 2024). De esta manera, establecer un sandbox regulatorio en México podría convertirse en una decisión determinante para crear una regulación tecnológica inteligente y efectiva.

Por otra parte, en América Latina, hay nueve países que tienen legislación o convenios o lineamientos relativos a ciberdelitos.

- Argentina: *Ley Convenio sobre Ciberdelito* del 22 de noviembre de 2017 mediante la cual aprobó el Convenio sobre Ciberdelito del Consejo de Europa (Budapest, 2001); el 4 de junio de 2008, se reformó e l Código Penal para incorporar el concepto de delito informático.
- Chile: *Ley Normas sobre delitos informáticos,* del 9 de junio de 2022, para cumplir con el Convenio de Budapest sobre ciberseguridad; además, tiene la Ley FINTEC del 22 de diciembre de 2022 para promover la competencia e inclusión financiera mediante el uso de tecnologías

- innovadoras en la provisión de servicios financieros, proteger al cliente financiero y sus datos utilizados, contribuir a la integridad y estabilidad financiera, prevenir el lavado de activos, el financiamiento del narcotráfico y del terrorismo.
- Colombia: *Lineamientos Generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital*, Decreto 338 del 8 de marzo de 2022, para fortalecer la gobernanza de la seguridad digital.
- Costa Rica: dictamen Afirmativo Unánime del *Proyecto de Ley de Ciberseguridad de Costa Rica.*
- Ecuador: propuesta de *Ley orgánica de seguridad digital, ciberseguridad, ciber defensa y ciberinteligencia,* para establecer un Sistema de Seguridad Digital.
- México: *Proyecto de Ley Federal de Ciberseguridad,* en estudio, que tiene como objeto, entre otros, «Regular la integración, organización y funcionamiento de la instancia encargada de las actividades de ciberseguridad a nivel nacional» (Gobierno de México, 2024).
- Paraguay: el 8 de septiembre de 2011, modificó el Código Penal, para definir y castigar ciberdelitos. Así, se cumplieron los estándares mínimos del Convenio de Budapest. Aprobó la *Convención sobre Ciberdelincuencia* (Budapest, 2001), y el Protocolo Adicional al Convenio sobres Ciberdelincuencia Relativo a la Penalización de Actos de Índole Racista y Xenófoba cometidos por medio de Sistemas Informáticos (Estrasburgo) el 27 de julio de 2017.
- Panamá: proyecto de *Ley sobre Ciberseguridad* presentado en la Asamblea Nacional, el 10 de agosto de 2017, para cumplir con los estándares internacionales de seguridad informática, así como el convenio de Budapest probado por Panamá en 2013.
- Perú: *Ley de ciberdefensa* del 26 de agosto de 2019 para «establecer el marco normativo en materia de ciberdefensa del Estado».

Por otra parte, en términos internacionales, hay dos eventos de alto nivel. Primero, se tiene el *Encuentro Latinoamericano de Inteligencia Artificial* (6-10 de marzo de 2023) KHIPU 2023 en el que participaron expertos referentes en tecnología internacional de 18 países: Argentina, Bolivia, Brasil, Canadá, Colombia, Costa Rica, El Salvador (Universidad Centroamericana José Simeón Cañas), Ecuador, España, Estados Unidos de América, Guatemala, Francia, Israel, México, Paraguay, Reino Unido, Uruguay, Venezuela; así como representantes de ONG que trabajan en áreas relacionadas con la IA. En KHIPU 2023 firmaron la *Declaración de Montevideo sobre la Inteligencia Artificial*, que insta a los gobiernos y empresas «a que los desarrollos de IA se pongan al servicio de las personas, reflejando las particularidades y problemáticas de América Latina».

Segundo, se tiene la *Cumbre Ministerial sobre la Ética de la Inteligencia Artificial* que se realizó en octubre de 2023. Participaron más de 20 ministros, representantes de gobiernos, academia, organismos internacionales y sector privado, donde tomaron la decisión de trabajar conjuntamente en la regulación, ética, gobernanza y adopción de estándares relacionados con la IA. Hubo representantes de Argentina, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Perú, Paraguay, República Dominicana, Santa Lucía, San Vicente y las Granadinas, Surinam, Uruguay y Venezuela.

En esta cumbre se dio la *Declaración de Santiago* en la que reiteraron «la universalidad, la indivisibilidad, interdependencia e interrelación de todos los derechos humanos y libertades fundamentales» (Gobierno de Chile, 2023, numeral 1). Además, hubo un reconocimiento que la IA «puede contribuir a la transformación de los modelos de desarrollo en los países de América Latina y el Caribe (y que para) mitigar sus potenciales amenazas se requiere reflexión, visión estratégica, regulación, gobernanza y coordinación regional y multilateral» (Ibidem, numeral 2). También, expresaron su preocupación por que algunas aplicaciones de la IA pueden afectar adversamente los derechos humanos.

Además, se enfatizó la necesidad «de elaborar y adoptar medidas de política pública y normas jurídicas que tengan como marco todas las normas y principios transversales de derechos humanos» (Ibidem, numeral 9).

Finalmente, la *Declaración de Santiago* proclamaron que ante las oportunidades y riesgos que presenta el uso de la IA, los Estados deben anticiparse y diseñar de «políticas, planes y estrategias nacionales, regionales e internacionales, para el diseño, desarrollo y uso seguro, ético y responsable de esta tecnología... con un enfoque de Derechos Humanos» (Gobierno de Chile, 2023, Proclama, numeral 1). Concluye la declaración expresando que tiene beneficios «fortalecer la gobernanza, representatividad y calidad de los datos utilizados para entrenar los sistemas de IA, y promover e invertir en mecanismos que permitan el intercambio seguro, equitativo, legal y ético de datos, en coherencia con la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO» (Gobierno de Chile, 2023, cierre de la Declaración).

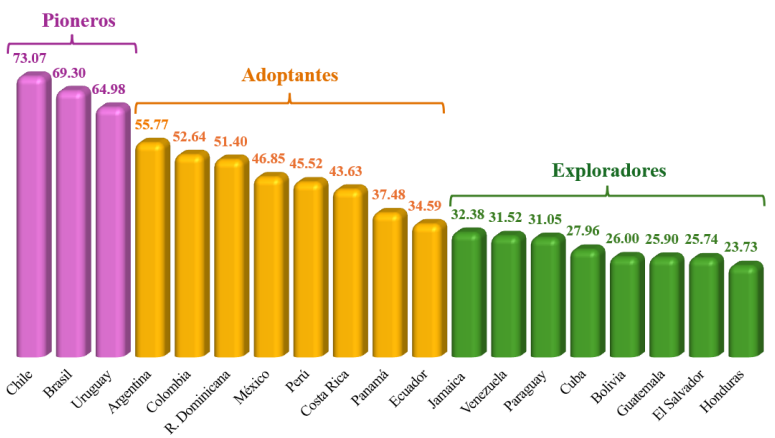
7. Legislación de IA en El Salvador

Como se presenta en el Anexo VII, la ONU realizó una evaluación del estado de desarrollo del Gobierno Electrónico en el sector público (*Reporte de Gobierno Electrónico, 2022*) que brindó un panorama del gobernó digital en los 193 países miembros, mediante el cual se construyó un índice que ubica a El Salvador en la posición 117 en el mundo con 0.5519 y en el lugar 14 entre los 19 países de América Latina.

El Salvador es uno de los países de Latinoamérica que no tiene una ley sobre protección de datos ni legislación sobre inteligencia artificial, aunque sí tiene una estrategia nacional establecida mediante la Política Nacional de Innovación, Ciencia y Tecnología en 2018.

Con estas legislaciones y otros apoyos adicionales, se debería ver cómo aumentar el uso de inteligencia artificial (IA) en El Salvador, que es el país con menor uso de esta tecnología en Latinoamérica. Según el Índice Latinoamericano de IA, preparado por el Centro Nacional de Inteligencia Artificial de Chile (CENIA) y la Comisión Económica para América Latina y el Caribe (CEPAL), presentado el 24 de septiembre de 2024, El Salvador es el segundo país de Latinoamérica con menor uso de IA, con 25.74 puntos, en comparación con Chile, que ocupa el primer lugar con 73.07 puntos.

Índice Latinoamericano de Inteligencia Artificial (ILIA)



Fuente: Reproducción de gráfico de ILIA 2024.

Además, El Salvador está catalogado como un país «explorador», categoría que incluye a países con puntajes dentro del primer tercio del rango total, esto es, con los valores más bajos. Esta clasificación se basa en que estos

países «están en las primeras etapas de sondeo de la IA», inmersos en el desarrollo de capacidades básicas, no cuentan con una comunidad de investigación consolidada, y las políticas públicas no cuentan con el potencial necesario para fomentar el desarrollo de la IA y establecer las bases para que esta área del conocimiento crezca con fuerza en el futuro.

Por su parte, Laura Hernández (2021) señala que El Salvador es uno de los pocos países en la región que aún no cuenta con una legislación específica para la protección de los datos personales, aunque algunas normas hacen algún tipo de referencia a este tópico como es un capítulo en la Ley de Acceso a la Información Pública (LAIP) y, en algunas leyes sectoriales, como la Ley de Regulación de los Servicios de Información sobre el Historial de Créditos de las Personas, y la Ley de la Firma Electrónica. A estas leyes se suma el desarrollo de jurisprudencia con la sentencia del 4 de marzo de 2011, Amparo 934-2007, de la Sala de lo Constitucional de la Corte Suprema de Justicia en lo relativo al derecho de acceso a la información personal, Habeas Data, en la que señaló que «... el derecho a la autodeterminación informativa tiene por objeto preservar la información de las personas que se encuentra contenida en registros públicos o privados frente a su utilización arbitraria –especialmente la almacenada a través de medios informáticos–, sin que necesariamente se deba tratar de datos íntimos» (Hernández, 2021, párr. 6).

Luego, en la Sala de lo Constitucional: sentencia de Amparo 142-2012 del 14 de agosto de 2013, definió el concepto del derecho a la autodeterminación al señalar que «la persona adquiere una situación que le permite: (i) definir la intensidad con que desea que se conozcan y circulen tanto su identidad como otras circunstancias y datos personales; (ii) combatir las inexactitudes o falsedades que las alteren; y (iii) defenderse de cualquier utilización abusiva, arbitraria, desleal o ilegal que pretenda hacerse de esos datos» (Hernández, 2021, párr. 4).

Después de múltiples consultas con abogados, tanques de pensamiento, la academia, instituciones del sector privado, entre otras, se aprobó mediante Decreto Legislativo No 875 la Ley de Protección de Datos Personales, el 28 de abril de 2021, la cual se esperaba que tuviera como objeto «la protección de los datos personales de las personas naturales o jurídicas de carácter privado o público, con la finalidad de regular su tratamiento legítimo e informado, para garantizar el derecho a la intimidad y el derecho a la autodeterminación informativa de las personas naturales» (Asamblea Legislativa, 2021).

Sin embargo, esta Ley se vetó el 7 de mayo de 2021 debido a las siguientes inconveniencias:

A. Por «Falta de armonía con el marco legal salvadoreño e inadecuado diseño de mecanismos jurisdiccionales y no jurisdiccionales para la protección de datos personales».

En este numeral destaca que si bien se tomaron en cuenta las recomendaciones de organismos internacionales, estas no fueron adaptadas a «las instituciones jurídicas del Derecho salvadoreño», como son «la Ley de Firma Electrónica, Ley de Supervisión y Regulación del Sistema Financiero, Código de Trabajo, Ley de Bancos, Ley Orgánica del Registro Nacional de Personas Naturales y las regulaciones relacionadas con la información de carácter tributario y aduanero», así como la jurisprudencia establecida según el Amparo 934-2007 y el Amparo 142-2012 sobre el derecho constitucional a la autodeterminación informativa (presentados anteriormente). Además, señala que no se «atribución alguna para la autoridad nacional que se crearía» para cumplir con esta ley y hay faltas de concordancia que podrían causar confusión o arbitrariedades en el ejercicio de esta normativa.

B. Falta de idoneidad y experticia técnica en la conformación de la Autoridad Nacional de Protección de Datos Personales.

En este sentido, se señaló que los tres miembros propuestos para conformar esta instancia, Corte Suprema de Justicia, Procuraduría de Defensa de los Derechos Humanos y la Universidad de El Salvador «en conjunto con las universidades privadas acreditadas por el Ministerio de Educación, Ciencia y Tecnología, no tienen competencias relacionadas con la materia a regular», por lo que resulta incoherente con las funciones y atribuciones que se les ha asignado.

C. Falta de planificación presupuestaria para la implementación de la ley.

En esta Ley se previó que la entidad a cargo del cumplimiento de esta normativa tendría «personalidad jurídica y patrimonio propia, autónoma en lo administrativo y financiero», lo cual afectaría al presupuesto. Sin embargo, en el proceso de formulación de esta Ley, la Asamblea Legislativa no solicitó opinión al Ministerio de Hacienda para conocer la factibilidad financiera de la nueva entidad.

En la conclusión del veto presidencial a la Ley de Protección de Datos Personales reiteró que la Presidencia de la República considera necesario «contar con un marco jurídico relacionado con la protección de datos personales», pero que dado las inconsistencias antes mencionadas «el proyecto aprobado no es adecuado ni pertinente para dicho fin... por lo que se plantea la necesidad de abordar dicha temática con desde una óptica diferente y con un adecuado diseño, tanto en los aspectos técnicos como jurídicos... previa una adecuada planificación técnica y financiera.». Dado que este concepto regulatorio no se continuó, El Salvador no tiene una ley de protección de datos al cierre del primer trimestre de 2024.

Por otra parte, al revisar las leyes, políticas y agendas relacionadas con el progreso tecnológico se tiene que en El Salvador hay 14 medidas entre políticas, leyes, creación de instituciones generados entre diciembre de 2010 y abril de 2023:

1. Conectándonos al Futuro de El Salvador presentada en 1999.
2. Política Nacional de Informática, presentada el 21 de julio de 2000.
3. Creación de la Comisión Nacional para la Sociedad de la Información el 23 de diciembre de 2004.
4. Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador fue concebida en 2010.
5. Ley de acceso a la información pública del 2 de diciembre de 2010.
6. Ley de Desarrollo Científico y Tecnológico del 15 de febrero de 2013.
7. Política Nacional de Computadora presentada en 2015.
8. Ley especial contra los delitos informáticos y conexos del 4 de febrero de 2016.
9. Política Nacional de Datos Abiertos de mayo de 2017.
10. Política Nacional de Innovación, Ciencia y Tecnología presentada en mayo de 2018.
11. Secretaría de Innovación creada en junio 2019.
12. Agenda Digital El Salvador 2020-2030 de enero de 2020.
13. Ley Bitcoin del 8 de junio de 2021
14. Ley de emisión de activos digitales del 11 de enero de 2023.
15. Ley de fomento a la innovación y manufactura de tecnologías del 18 de abril de 2023.

1. *Conectándonos al Futuro de El Salvador* una iniciativa del gobierno implementada en 1999, con el apoyo del Banco Mundial, con el objetivo de definir una estrategia de desarrollo de país construida basada en la creación y el uso productivo y participativo de la información y el conocimiento. En este contexto nacieron los Infocentros, concebidos como un modelo alternativo para el aprendizaje, uso y desarrollo de las aplicaciones utilizadas en internet, para facilitar el intercambio de información y fomentar la creación de nuevas empresas.

2. *La Política Nacional de Informática*, presentada el 21 de julio de 2000, fijó como objetivo «Establecer las disposiciones para implementar, operar, controlar, revisar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI) documentado... para asegurar los controles de seguridad suficientes que protejan los activos de información y brinden confianza a las partes interesadas».

3. *La Comisión Nacional para la Sociedad de la Información* se creó, el 23 de diciembre de 2004, para servir como órgano consultivo y asesor del Presidente de la República para el desarrollo y consolidación de la sociedad de la información en el país. Luego, mediante Decreto Ejecutivo del 29 de octubre de 2018 se creó la *Comisión Presidencial de Gobierno Digital* como entidad colegiada, especializada y técnica, adscrita a la Presidencia de la República, a la que se le otorgaron facultades para la formulación, dirección y ejecución de políticas públicas relacionadas con el gobierno digital dentro del Órgano Ejecutivo. Ante estas responsabilidades, se le fijó como objetivo institucional construir fortalecer las acciones encaminadas a la modernización del Estado; coordinar el trabajo en esta área entre las instituciones del Órgano Ejecutivo y con otros órganos del Estado; y, concertar esfuerzos para impulsar una Agenda Digital de país para la creación de una sociedad del conocimiento. Dicho lo anterior, el Gobierno decidió, el 8 noviembre de 2018, derogar el Decreto Ejecutivo que había creado la Comisión Nacional para la Sociedad de la Información.

4. *La Dirección de Innovación Tecnológica e Informática del Gobierno de El Salvador* se concibió, en 2010, para apoyar a la Presidencia de la República y sus dependencias, mediante «acciones para simplificar y estandarizar la gestión gubernamental; promover el uso innovador, eficiente y eficaz de las (TIC), como medio para mejorar y modernizar la gestión pública y asegurar la integridad y disponibilidad de la información». En adición, se espera que promueva el desarrollo del gobierno electrónico, formule propuestas «para promover la innovación TIC» en Órgano Ejecutivo, mejorar «el acceso de la información a la población» por medios tecnológicos, estimule «la creación de redes de cooperación tecnológica entre las instituciones del Órgano Ejecutivo, e impulse el desarrollo y adopción de las TIC (Tecnologías de la Información y las comunicaciones) procurando la eficiencia, eficacia, modernización y transparencia».

5. *Ley de acceso a la información pública*, del 2 de diciembre de 2010, tiene como objeto «garantizar el derecho de acceso de toda persona a la información pública, a fin de contribuir con la transparencia de las actuaciones de las instituciones del Estado (Artículo 1)», de modo que «Toda persona tiene derecho a solicitar y recibir información generada, administrada o en poder de las instituciones públicas y demás entes obligados de manera oportuna y veraz, sin sustentar interés o motivación alguna» (Artículo 2).

6. *Ley de Desarrollo Científico y Tecnológico*, del 15 de febrero de 2013, tiene por objeto «establecer las directrices para el desarrollo de la ciencia y la tecnología, mediante la definición de los instrumentos y mecanismos institucionales y operativos fundamentales para la implementación de una Política Nacional de Innovación, Ciencia y Tecnología, a través de la ejecución de un Plan Nacional de Ciencia y Tecnología, el cual constituye el marco de referencia de la Agenda Nacional de Investigación».

7. El Gobierno de El Salvador concibió la *Política Nacional de Computadora*, mediante la cual se promovió el programa *Una niña, un niño, una computadora,* iniciativa que se comenzó a materializar el 23 de abril de 2015 con la entrega de las primeras 6,479 computadoras personales *Lempitas,* en 346 centros educativos, donde estudiaban más de 84 mil niños/as. Fue el inicio de una estrategia para mejorar las capacidades de los estudiantes para enfrentar un mundo cada vez más digital e interconectado. Entre abril de 2015 y enero de 2019 se entregaron más de 98,500 computadoras en 4,000 centros educativos públicos, donde estudian alrededor de 950,000 niños/as y trabajan más de 33,300 docentes (Diario Colatino, 2019).

Sin embargo, en realidad no se entregaron laptops a los estudiantes, sino que se colocaron mayoritariamente computadoras de escritorio y portátiles en centros escolares públicos. Según datos del Ministerio de Educación, hasta enero de 2019, se habían entregado 75,574 computadoras en 2,983 escuelas que atienden a 865,749 estudiantes y cuentan con 29,653 docentes (Joma y Vides, 2020).

En febrero de 2021 el Gobierno de El Salvador inició la entrega de computadoras portátiles o una *tablet* a alrededor de 1.3 millones de estudiantes, por lo que «Vamos a ser el único país en toda Latinoamérica donde todos nuestros estudiantes van a tener una computadora con internet gratis y todas las herramientas necesarias», expresó el Presidente Nayib Bukele (Gobierno de El Salvador, 2021). De esta manera, se espera reducir la brecha digital, algo que no se logró anteriormente.

8. Ley Especial Contra los Delitos Informáticos y Conexos (Decreto No 260), del 4 de febrero de 2016 señala que «tiene por objeto proteger los bienes jurídicos de aquellas conductas delictivas cometidas por medio de las Tecnologías de la Información y la Comunicación, así como la prevención y sanción de los delitos cometidos en perjuicio de los datos almacenados, procesados o transferidos... o los cometidos mediante el uso de dichas tecnologías que afecten intereses asociados a la identidad, propiedad, intimidad e imagen de las personas naturales o jurídicas en los términos aplicables y previstos en la presente Ley». Por ser una Ley de que se promulgó en 2016, no contempló los delitos que se pueden cometer mediante el uso de la IA, pero constituyó un primer

paso muy importante, por lo que debería modificarse para incluir los aspectos propios del desarrollo y uso de la IA, así como tener consistencia jurídica con una propuesta de Ley de IA.

9. En la *Política Nacional de Datos Abiertos* presentada, en mayo de 2017, se fijó como finalidad «garantizar el acceso expedito, abierto y sin restricciones de uso del conjunto de datos que producen las entidades del Órgano Ejecutivo en formatos estructurados que permitan su uso y reutilización automática» (Capítulo VII). Luego, como objetivo se definió «Establecer los estándares, procedimientos y mecanismos a utilizar para que los datos abiertos estén a disposición de las mismas instituciones de gobierno y de la población de forma proactiva...» (Capítulo VIII).

En este sentido, se visualizó el establecimiento de una política activa de innovación, ciencia y tecnología para establecer «un modelo educativo, de formación y especialización científica, tecnológica y productiva... que permita capitalizar las oportunidades que las capacidades presentes y futuras brindan». Lamentablemente, no hubo mayores avances

11. La Secretaría de Innovación fue creada por el presidente Nayib Bukele, en junio 2019, al tomar posesión de su cargo. Como objetivo principal se fijó «la transformación digital del país» como «una vía de escape a la situación (del país), caracterizada por la pobreza, la exclusión y, sobre todo, el poco desarrollo tecnológico». La Secretaría fue la que diseñó y lanzó la Agenda Digital El Salvador 2020-2030.

12. La Agenda Digital El Salvador 2020-2030, presentada en enero de 2020, se concibió como el primer paso para «iniciar la transformación digital del país», para lo cual se establecieron cuatro componentes para lograrlo de manera exitosa: (1) identidad digital, (2) innovación, educación y competitividad, (3) modernización del estado, y (4) gobernanza digital. Con esta iniciativa, se busca que el Estado se convierta en un «facilitador» para que «los diferentes actores de la sociedad (puedan) adoptar, impulsar y propagar nuevas formas y herramientas de innovación» en sus respectivas áreas de especialidad, utilizando las Tecnologías de la Información y las comunicaciones (TIC) para «así permitir una interacción efectiva y segura para la entrega de servicios públicos y privados, con garantías legales para todos los involucrados en las transacciones internas y externas con el resto del mundo» (p. 7).

13. La Ley Bitcoin, se aprobó el 8 de junio del 2021, y se le fijó como su objeto «la regulación del bitcoin como moneda de curso legal, irrestricto con poder liberatorio, ilimitado en cualquier transacción y a cualquier título que las personas naturales o jurídicas públicas o privadas requieran realizar (Artículo 1). Si bien esta Ley establece que «El tipo de cambio entre el bitcoin y el dólar de

los Estados Unidos de América... será establecido libremente por el mercado (Artículo 2)», que «Todo precio podrá ser expresado en bitcoin» (Artículo 3), que «Todas las contribuciones tributarias podrán ser pagadas en bitcoin» (Artículo 4), no fue incluida como medio a utilizar en la contabilidad de las personas naturales ni jurídicas, al señalar que «Para fines contables, se utilizará el dólar como moneda de referencia» (Artículo 6), esto es, el dólar se mantuvo como la única moneda de referencia. Además, establece que «Todo agente económico deberá aceptar Bitcoin, como forma de pago cuando así le sea ofrecido por quien adquiere un bien o servicio» (Artículo 7).

14. La *Ley de emisión de activos digitales* se promulgó el 11 de enero de 2023, a la cual se le estableció como objeto «establecer el marco legal que otorgue certeza jurídica a las operaciones de transferencia a cualquier título de activos digitales que se utilicen en las emisiones de ofertas públicas realizadas en... El Salvador; así como regular los requisitos y obligaciones de los emisores, proveedores de servicios de activos digitales, y demás participantes que operen en el proceso de ofertas públicas, con el objetivo de promover el desarrollo eficiente del mercado de activos digitales y proteger los intereses de los adquirentes» (Artículo 1). El Artículo 6 señala la creación de la *Comisión Nacional de Activos Digitales*, «como una institución de derecho público con personalidad jurídica y patrimonio propio, de carácter técnico, con autonomía económica, financiera y administrativa», adscrita al Ministerio de Economía. Se estableció que esta comisión es la encargada de la aplicación de las normativas de esta Ley, sus reglamentos y demás reglas de ofertas públicas de activos digitales (Artículo 7), así como «asegurar la integridad del mercado y la provisión de la debida información a los adquirentes» (Artículo 8).

15. La *Ley de fomento a la innovación y manufactura* de tecnologías del 18 de abril de 2023 tiene por objeto «contribuir al crecimiento económico y el desarrollo sostenible del país mediante el fortalecimiento de la competitividad a través del fomento de la innovación y de la manufactura de tecnología desarrollada en el territorio nacional», como medio para promover el «crecimiento de la fuerza laboral capacitada» en estos trabajos, «para el desarrollo de la industria tecnológica a nivel global».

Esta Ley incluye incentivos fiscales para las empresas que califiquen: «(a) Exención total del Impuesto sobre la Renta respecto de las actividades incentivadas; (b) Exención de todo tipo de retenciones del Impuesto sobre la Renta respecto de las actividades incentivadas; (c) Exención total de impuestos municipales sobre el activo neto declarado por los beneficiarios; (d) Exención del pago de la Ganancia de Capital (artículos 14 y 42 de la Ley de Impuesto sobre la Renta); (e) Exención total del pago de los Derechos Arancelarios a la Importación e impuestos que graven la importación de los bienes, insumos, maquinarias, equipos y herramientas necesarios para el desarrollo de las actividades incentivadas» (Artículo 7).

La información antes presentada muestra que se retomó con mayor fuerza y se le ha dado sentido y dirección a la gobernanza digital en El Salvador y, como lo señala la *Agenda Digital El Salvador 2020-2030*, sería necesario fortalecerla mediante la eliminación de «competencias duplicadas, asignar recursos, y crear mecanismos de seguimiento permanente». Ahora, considerando algunos avances innovadores y determinantes en el mundo digital, el proceso para fortalecer la gobernanza de esta área tecnológica se puede realizar en el momento de la formulación de una Ley de Inteligencia Artificial de El Salvador y una Ley de Protección de Datos. En este proceso, será determinante mantener una visión integral pública y privada para que el país cuente con un marco legal y regulatorio basado en soluciones técnicas comunes y estandarizadas, donde la ética y las buenas prácticas constituyan sus fundamentos.

Si bien el marco normativo integral que establezca El Salvador debe incluir controles y sanciones para responder a las amenazas cibernéticas, al uso indebido, abusivo, dañino, excluyente y violatorio de los derechos humanos, también, se debe mantener principios y condiciones que no entorpezcan o limiten el desarrollo innovador de las TIC, especialmente, de la IA. En resumen, como se señala la Agenda Digital El Salvador 2020-2030, que haya un equilibro para que exista un ambiente colaborativo y «protocolos para prevenir, detectar y responder a las amenazas cibernéticas a las que se ve expuesta la información ciudadana, empresarial y la infraestructura crítica del Estado» (p. 12).

IV. Propuesta de Ley de IA para El Salvador

Ante el vertiginoso e innovador avance de la IA, y su cada vez mayor uso en todo el mundo, los países miembros de la ONU adoptaron, el 21 de marzo de 2024, una resolución con el propósito de establecer una regulación a nivel mundial. El objetivo principal de esta medida es garantizar la seguridad y confiabilidad en el uso de la IA, así como reducir las disparidades existentes entre naciones.

Esta propuesta se presenta como una primera respuesta de El Salvador a la resolución de la ONU que para alinearse, con una regulación global, han tomado como referencias la Ley de Inteligencia Artificial de la UE del 18 de marzo de 2024, la legislación China adoptada entre julio de 2021 y abril de 2023, el marco legal del Reino Unido, la Ley de IA de Perú del 13 de junio de 2023, así como las propuestas de Ley de Brasil y de Chile para regular la IA y la propuesta para normar la robótica y las tecnologías conexas, las cuales se encuentran en proceso de aprobación a inicios de abril de 2024. Además, se tomaron en cuenta la Constitución de la República de El Salvador y diversas leyes que deberán ser revisadas o reformadas para que, como lo especifica la Agenda Digital El Salvador 2020-2030, se eliminen «competencias duplicadas, asignar recursos, y crear mecanismos de seguimiento permanente».

Es de destacar que esta propuesta de Ley de IA debe consultarse con diversos sectores de la sociedad salvadoreña para recibir comentarios y solicitudes de ajustes, eliminaciones y nuevos conceptos a incluir. Este debe ser un paso irrenunciable y cumplirlo como se ha hecho en los países que han formulado y aprobado este tipo de ley de IA. En adición, se debe resaltar que esta propuesta de Ley, alineada con los principios fundamentales necesarios para una legislación global, puede servir de base sustancial para todo país que esté considerando la formulación de una Ley de IA.

ANTEPROYECTO DE LEY DE INTELIGENCIA ARTIFICIAL

DECRETO No NN
LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR
CONSIDERANDO:

I. Que el Artículo 1 de la Constitución "reconoce a la persona humana como el origen y el fin de la actividad del Estado", por lo que su obligación es "asegurar a todos los habitantes de la República, el goce de la libertad, la salud, la cultura, el bienestar económico y la justicia social", todo lo cual está amenazado por el uso indebido o manipulaciones de las herramientas de Inteligencia Artificial.

II. Que el avance de las tecnologías de la Información y las Comunicaciones, en general, y de la Inteligencia Artificial, en particular, se han convertido en herramientas de uso diario por la gran mayoría de la población, empresas, organizaciones sin fines de lucro e instituciones del Estado, y han generado condiciones que permiten potenciar el progreso socioeconómico, combatir la delincuencia y proveer mayor seguridad interna en El Salvador.

III. Que la Resolución de fecha 21 de marzo de 2024, de la Organizaciones de las Naciones Unidas, promueve que los sistemas deben seguros y fiables beneficiando el desarrollo sostenible para todos, y que los derechos humanos puedan ejercerse tanto fuera de línea como dentro de ella.

IV. Que el uso de inteligencia artificial también conlleva serios riesgos y consecuencias negativas por el mal uso de la información y la falta de ética en su desarrollo y aplicación, como son la propagación de información falsa que genera desinformación a gran escala, los *deep fakes* maliciosos y pornográficos, el riesgo de causar daño mental y físico a niños, niñas y adolescentes, quienes están expuestos a ataques directos, así como a las demás personas, empresas e instituciones públicas y de la sociedad civil con adversos efectos socioeconómicos, educativos, culturales, jurídicos y políticos.

V. Que antes los riesgos señalados, es necesario contar con leyes y reglamentos efectivos para supervisar y garantizar aspectos como la transparencia en los algoritmos y la toma de decisiones, la protección de la privacidad y la seguridad de los datos, así como la responsabilidad y rendición de cuentas de los desarrolladores y usuarios de Inteligencia Artificial.

VI. Que El Salvador cuenta con varias leyes, institucionalidad y una agenda digital como con la:

1. Ley de Desarrollo Científico y Tecnológico del 15 de febrero de 2013, que tiene por objeto establecer las directrices para el desarrollo de la ciencia y la tecnología.

2. La Secretaría de Innovación, institución creada en junio 2019, cuyo objetivo es "la transformación digital del país" como "una vía de escape" a la situación de pobreza, exclusión y de poco desarrollo tecnológico.

3. La Agenda Digital El Salvador 2020-2030 presentada en enero de 2020 por la Secretaría de Innovación, que presenta una visión estratégica para "iniciar la transformación digital del país".

4. La Ley de Emisión de Activos Digitales del 11 de enero de 2023, que tiene como objeto "establecer el marco legal que otorgue certeza jurídica a las operaciones de transferencia a cualquier título de activos digitales que se utilicen en las emisiones de ofertas públicas" en El Salvador y regular las actividades de los emisores y proveedores de estos servicios, promover el desarrollo eficiente del mercado y proteger los intereses de los adquirentes. Que, mediante esta Ley se creó la Comisión Nacional de Activos Digitales, como la encargada de la aplicación de las normativas de esta Ley, sus reglamentos y demás reglas de ofertas públicas de activos digitales.

5. La Ley de fomento a la innovación y manufactura de tecnologías del 18 de abril de 2023 que tiene por objeto "contribuir al crecimiento económico y el desarrollo sostenible del país mediante el fortalecimiento de la competitividad a través del fomento de la innovación y de la manufactura de tecnología desarrollada en el territorio nacional".

VII. Que dada la información presentada en el Considerando IV, y de acuerdo a lo señalado en la *Agenda Digital El Salvador 2020-2030*, en el sentido que sería necesario fortalecer la gobernanza digital en el país mediante la eliminación de "competencias duplicadas, asignar recursos, y crear mecanismos de seguimiento permanente", se requiere incluir en esta Ley un Capítulo especial sobre la Protección de Datos, para contar con una normativa basada en soluciones técnicas de aplicación y aceptación universal, donde la ética y las buenas prácticas constituyan sus fundamentos.

VIII. Que es fundamental que en el marco normativo El Salvador se establezca que debe ser integral, incluir controles y sanciones para responder a las amenazas cibernéticas, por el posible uso indebido, abusivo, dañino, excluyente y violatorio de los derechos humanos, también se deben mantener principios de libre mercado y condiciones tecnológicas para no entorpecer o limitar el desarrollo innovador de las TIC, especialmente de la Inteligencia Artificial.

IX. Que hay continuos desarrollos tecnológicos innovadores y disruptivos, además es necesario normar tanto los sistemas de inteligencia artificial como la robótica y las tecnologías conexas en sus ámbitos de aplicación, esta legislación debe ser revisada y actualizada a lo menos cada 12 meses o cuando se presente una situación innovadora que requiera un ajuste a esta Ley.

POR TANTO: en uso de sus facultades constitucionales y a iniciativa del presidente de la República, por medio del Ministro de Economía,

DECRETA, la siguiente:

LEY DE INTELIGENCIA ARTIFICIAL DE LA REPÚBLICA DE EL SALVADOR

TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
OBJETO, FIN Y DEFINICIONES

Objeto
Art. 1. Esta Ley tiene por objeto promover el uso ético y responsable de la Inteligencia Artificial en la era digital, donde toda actividad tecnológica se centre y privilegie a la persona humana, que sea confiable, respete los derechos humanos y potencie el desarrollo económico, social, jurídico, político y ambiental para mitigar y recuperar el daño que causan los seres humanos, mediante la conformación de un entorno seguro y confiable que garantice su uso sostenible, transparente, replicable y responsable.

Finalidad
Art. 2. Esta Ley tiene como finalidad establecer un marco jurídico integral para regular y supervisar el desarrollo, comercialización, distribución y utilización de los sistemas de Inteligencia Artificial, garantizando la protección de los derechos fundamentales consagrados en la Constitución de la República de El Salvador.

Inteligencia Artificial

Art. 3. Para la aplicación de esta Ley, se establecen las siguientes definiciones:

1. Inteligencia Artificial: es una disciplina tecnológica que combina datos, algoritmos y capacidad informática para crear sistemas que imitan la inteligencia humana, mediante los cuales aprenden de la información y adaptan su comportamiento sin necesidad de programación específica para cada tarea, utilizando algoritmos y modelos matemáticos para procesar grandes volúmenes de datos y mejorar con el tiempo mediante el aprendizaje automático. Para tales efectos, cuando la normativa, se refiera a este concepto, se abreviará IA.

2. Acuerdo anticompetitivo: es una situación donde un grupo de empresas impiden o restringen la competencia o intentan desplazar a los competidores mediante acuerdos, pactos, carteles o convenios de colusión para manipular el mercado, fijar precios u otras condiciones de compraventa y repartirse el mercado, lo que está sancionado en la Ley de Competencia de El Salvador.

3. Agentes de inteligencia artificial: son los proveedores y operadores de sistemas de IA.

4. Algoritmos de recomendación: son aplicaciones que utilizan IA y aprendizaje automático para analizar el comportamiento y preferencias de los usuarios para sugerirles o recomendarles bienes y servicios de su interés, así como para satisfacer sus necesidades y potenciar la fidelización.

5. Archivo, registro o base de datos: es el conjunto organizado de datos personales sujetos a tratamiento o procesamiento, ya sea de forma electrónica o no, sin distinguir la modalidad de su formación, almacenamiento, organización o acceso.

6. Autodeterminación informativa: es la facultad que tiene toda persona para ejercer los derechos y utilizar los mecanismos establecidos en esta Ley sobre la información personal que le concierne, contenida en registros públicos o privados, especialmente los almacenados mediante medios digitales e informáticos.

7. Bloqueo de datos: es la restricción temporal de cualquier acceso o tratamiento de los datos almacenados.

8. Ciberresiliencia o resiliencia cibernética: es la capacidad de un sistema u organización para resistir y/o recuperarse cuando sufre ataques o incidentes cibernéticos.

9. Ciberseguridad: abarca todas las actividades necesarias para proteger las redes y sistemas de información de los usuarios contra ciberamenazas y ciberataques, evitando que sean afectados por estos eventos.

10. Consentimiento: es la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los datos cuando no exista otro fundamento legal para su tratamiento.

11. Datos biométricos: son los datos personales obtenidos a partir de un tratamiento técnico específico, que precisa las características físicas, fisiológicas o conductuales de una persona natural, que pueden utilizarse para identificarla o confirmar su identificación única en formato digital, como son imágenes faciales o datos dactiloscópicos.

12. Datos de entrada: son los datos proporcionados a un sistema de IA u obtenidos directamente por él de una o diversas fuentes, a partir de los cuales produce la información de salida, en busca de producir resultados útiles, confiables y precisos.

13. Datos personales: es la información privada de una persona identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico y otra análoga.

14. Datos sensibles: son aquellos datos personales que afectan a la esfera más íntima de su titular y cuya utilización indebida pueda causar discriminación, afectar el derecho al honor, a la intimidad personal y familiar y a su propia imagen. Estos datos suelen revelar aspectos como el credo, religión, origen étnico, afiliación o ideologías políticas, afiliación sindical, preferencias sexuales salud física y mental, información

biométrica, genética, situación moral y familiar y cualquier otra información de naturaleza íntima similar.

15. Desarrollador: es toda persona natural o jurídica que desarrolle un sistema de IA mediante procesos para la creación, diseño, despliegue y compatibilidad de softwares relacionados con sistemas de IA.

16. Discriminación: es toda acción o señalamiento que resulte en un trato desfavorable o injusto hacia una persona o grupo, vulnerando su dignidad, derechos humanos y libertades debido a características especiales como origen geográfico, raza, color o etnia, género, nivel de ingresos, condiciones socioeconómicas, edad, discapacidad, religión o política, que potencialmente puedan causar una exclusión, restricción o rechazo, restringir o alterar su reconocimiento, el goce o ejercicio de igualdad o de cualquier derecho previsto en el sistema jurídico de El Salvador.

17. Discriminación indirecta: es la discriminación que se genera cuando la práctica, criterio o uso pareciera ser aparentemente neutral pero potencialmente tiene la capacidad de causar desventajas a las personas que pertenecen a un grupo específico, o colocarlos en desventaja, excepto cuando ella tiene una justificación objetiva, razonable y legítima de acuerdo con los derechos previstos en el sistema jurídico de El Salvador.

18. Disociación o Anonimización: es un procedimiento irreversible de gestión de datos mediante el cual se reemplaza la información personal de un individuo por identificadores artificiales para que dichos datos no puedan ser utilizados para identificar a ninguna persona.

19. Encargado del tratamiento: es la persona natural o jurídica, pública o privada que, ya sea sola o en conjunto con otros, trate datos personales por cuenta del responsable.

20. Fuentes accesibles al público: son las bases de datos personales de administración pública o privada, cuya consulta puede ser realizada por cualquier persona o medio, salvo que está prohibido por una norma o sujeto al abono de una contraprestación.

21. Desarrollador: es toda persona natural o jurídica que desarrolle un sistema de IA mediante procesos para la creación, diseño, despliegue y compatibilidad de softwares relacionados con sistemas de IA.

22. Incidente: es cualquier evento que tenga efectos adversos en la seguridad de las redes y sistemas de información.

23. Minería de textos y de datos: es el proceso que transforma textos no estructurados mediante la extracción y análisis de grandes cantidades de datos o extractos parciales para convertirlos en un formato estructurado que sirve para identificar patrones significativos y nueva información para el desarrollo o uso de sistemas de IA.

24. Monopolio: es una situación del mercado donde un productor o un vendedor es el único que ofrece o explota un bien o un servicio, lo que le permite fijar a su conveniencia su producción u oferta, determinar el precio de su bien o servicio y restringir la entrada de competidores.

25. Oligopolio: es una situación donde unas pocas empresas tienen la capacidad de influir en el mercado, y así, influir en la determinación del precio del bien o los o servicios que ofrece.

26. Operador del sistema de IA: es toda persona natural o jurídica que emplee o utilice, en su nombre o beneficio, sistema de IA, salvo que lo realice para una actividad personal no profesional.

27. Proveedor: es toda persona natural o jurídica que inicie procesos o se dedique a comercializar o distribuir un sistema de IA, a cambio de un cobro o de manera gratuita, estén establecidos en El Salvador o en otro país.

28. Responsable del tratamiento de datos: es la persona natural o jurídica, pública o privada, propietaria de la base de datos o que decide sobre la finalidad y medios del tratamiento.

29. Sandboxes Regulatorios o Banco de Pruebas Regulatorios: son un espacio virtual que brinda un espacio controlado y delimitado por el supervisor, el cual permite reducir la incertidumbre en el desarrollo de un proyecto o de un nuevo producto o de nuevos modelos de negocio, aplicaciones

o procesos, para que haya una mejor comprensión de la transformación digital en un ambiente seguro para impulsar la innovación.

30. Seudonimización: es el proceso de cambiar la denominación de los datos personales por seudónimos, de modo que no puedan asociarse directamente con el titular sin información adicional. Sin embargo, aunque se oculta la identidad de la persona, no se elimina el vínculo entre los datos y la persona, por lo que es un procedimiento reversible que permite volver a identificar al titular.

31. Sistema de identificación biométrica remota: es un sistema de IA diseñado para identificar a personas físicas sin su participación directa, mediante el cual se comparan sus datos biométricos con los que hay en una base de datos de referencia, los que permite identificar a múltiples personas o su comportamiento de manera simultánea, sin requerir la participación activa de ellas.

32. Sistemas de IA: son programas informáticos o *softwares* diseñados para realizar tareas que normalmente requieren inteligencia humana, como el aprendizaje automático supervisado y no supervisado, percepción, razonamiento y toma de decisiones. Estos sistemas pueden utilizar técnicas como el procesamiento del lenguaje natural, motores de inferencia y deducción, estrategias estadísticas, visión por computadora y la robótica para realizar funciones de forma autónoma o con asistencia humana.

33. Sistemas de IA de alto riesgo: son los que son utilizados según lo establecido en el artículo 31 de esta Ley.

34. Sistemas de IA de riesgo inaceptable son:

a. Los que emplean técnicas subliminales que trascienden la conciencia de una persona y que son utilizadas para alterar de manera sustancial su comportamiento y llegar a provocar o potencialmente provocando daños físicos o psicológicos tanto en la persona expuesta como en otras personas.

b. Las técnicas que aprovechan alguna vulnerabilidad de un grupo de personas, como la edad o discapacidad física o mental, para alterar sustancialmente el comportamiento de personas dentro de ese grupo, potencialmente causando daños físicos o psicológicos tanto en la persona expuesta como en otras personas.

c. Los sistemas y técnicas empleados por autoridades públicas o sus representantes para evaluar y clasificar la fiabilidad de personas naturales basándose en su conducta social, personalidad o características previamente obtenidas y que le puedan causar un trato perjudicial o desfavorable a ella o a un grupo o a colectivos sociales: (i) cuando no tengan relación con el contexto donde se generó o fue recabada originalmente la información; y (ii) cuando resulte en una decisión injustificada o desproporcionada respecto a su comportamiento social o la gravedad de éste.

35. Titular: es toda persona natural cuyos datos sean objeto del tratamiento al que se refiere la presente Ley.

36. Transferencia de datos personales: es toda entrega total o parcial de datos personales para ser trabajados por un tercero que actuará como encargado del tratamiento o como nuevo responsable. Se excluyen las entregas de datos personales para el almacenamiento de información por terceros o fuera del país por entidades públicas o privadas a cualquier persona distinta al titular de datos, mediante el uso de medios físicos o electrónicos o cualquier otra tecnología que lo permita.

37. Trazabilidad de datos: es la capacidad de seguir el rastro de los datos desde su punto de origen, uso, recorrido, localización y destino final, lo que permite registrar su tratamiento y resultados, así como para tomar medidas preventivas o correctivas.

38. Tratamiento de datos: es una operación o conjunto de operaciones que se realizan mediante procedimientos automatizados o manuales de datos personales, como son los procesos de recolección, registro, organización, conservación, modificación, extracción, consulta, uso, comunicación por transmisión, difusión, distribución o cualquier otra forma que facilite el acceso, cotejo, interconexión, bloqueo, supresión o destrucción de ella, entre otros.

39. Usuario: es toda persona natural o jurídica que utilice un sistema de IA.

CAPÍTULO II
PRINCIPIOS

Principios

Art. 4. El desarrollo, ejecución y uso de sistemas de IA en El Salvador deben considerar, aplicar y ajustarse en total conformidad con los siguientes principios:

1. Respeto a la propiedad intelectual de los sistemas de IA actuales y los por crearse en el futuro.
2. No generar discriminación sino crecimiento incluyente, equitativo y mayor bienestar socioeconómico.
3. Respeto de la justicia, equidad e inclusión socioeconómica.
4. Aportar al progreso sostenible y de respeto del medioambiente.
5. Libertad de decisión y de elección.
6. Prevención, precaución y mitigación de potenciales riesgos sistémicos por usos indebidos intencionales o no intencionales.
7. Sistemas tecnológicos transparentes, explicables, integrales y auditables.
8. Confiabilidad, calidad, veracidad de la información que se utilice o que se genere.
9. Rendición de cuentas y reparación integral de daños.
10. Alta seguridad cibernética.
11. Trazabilidad de las decisiones durante todo el ciclo de vida de los sistemas de IA como medio de rendición de cuentas y atribución de responsabilidades a una persona natural o jurídica.
12. Abiertos al debido proceso legal, impugnabilidad y el principio de contradicción o derecho a confrontar las pruebas que se presenten en contra de una persona natural o jurídica durante un juicio.

TÍTULO II
DERECHOS, DEBERES Y OBLIGACIONES DE LOS USARIOS DE INTELIGENCIA ARTIFICIAL

CAPÍTULO
LOS DERECHOS DE LAS PERSONAS

Derecho a recibir información sobre sistemas de IA
Art. 5. Toda persona que desee utilizar sistemas de IA, especialmente cuando pertenezca a grupos vulnerables como niños, adolescentes, personas mayores y personas con discapacidad, tiene el derecho a recibir información gratuita, clara, precisa y con un lenguaje de fácil comprensión, incluyendo el posible uso de íconos o símbolos de fácil reconocimiento, antes de contratar o utilizar el sistema.

Esta información debe abordar los siguientes aspectos:

1. Cómo la naturaleza automatizada de la interacción y la toma de decisiones en los procesos o productos puede afectar a la persona que los utiliza.
2. Descripción general del sistema, los tipos de decisiones, recomendaciones o predicciones que se pretende o pueden hacer y las consecuencias que puede tener su uso para la persona.
3. Identificación de los operadores del sistema de IA, los protocolos de gobernanza y ética que tienen y cómo son utilizados en el proceso de desarrollo y en el uso del sistema por parte de su o sus creadores.
4. Descripción de cómo el sistema de IA trabaja y de todas las personas que estuvieron involucrados en el proceso de toma de decisiones, predicción o recomendación.
5. Categorías de datos personales utilizados en el contexto de la operación del sistema de IA.
6. Presentación y descripción de las medidas de seguridad, de las que evitan discriminación y las de protección y confiabilidad adoptadas, incluyendo exactitud, precisión y cobertura.
7. Descripción detallada sobre los posibles riesgos asociados al uso de los sistemas de IA, así como la metodología y medios para remediar problemas o mal funcionamiento, asegurando la protección de los derechos de los usuarios en caso de incidentes

Derecho de respuesta oportuna y efectiva
Art. 6. La persona afectada por un sistema de IA tiene derecho a solicitar una explicación y recibir una respuesta gratuita, en un plazo máximo de 10 días hábiles, sobre las decisiones, predicciones o recomendaciones, incluyendo información sobre los criterios y procedimientos utilizados, así como los principales factores que afectan dicha predicción o decisión específica. Esta información debe incluir:

1. La racionalidad y lógica del sistema, su significado y las potenciales consecuencias que puede tener tal decisión para la persona afectada.
2. El grado y nivel de contribución del sistema de IA a la toma de decisiones.
3. Los datos que han sido procesados, su fuente y los criterios para la toma de decisiones y, cuando corresponda, su ponderación, ante la situación del afectado;
4. Los mecanismos que pueden ser utilizados por la persona que desee impugnar la decisión.
5. La posibilidad de tener un contacto personal por parte de la persona o personas afectadas.

Derechos de Protección
Art. 7. Toda persona que sea o haya sido afectada por sistemas de IA tiene los siguientes derechos de protección:

1. Derecho a la privacidad y protección de datos personales, de acuerdo con los derechos previstos en el sistema jurídico de El Salvador.
2. Derecho a tener información previa relativa a sus interacciones con sistemas de IA.
3. Derecho a solicitar y recibir una explicación sobre toda decisión, recomendación o previsión realizada por sistemas de IA.
4. Derecho a objetar decisiones o previsiones realizadas por sistemas de IA que puedan causar efectos jurídicos o que incidan significativamente en los intereses de la persona afectada.
5. Derecho a la determinación y a la participación de personas en el desarrollo y de las decisiones relativas a los sistemas de IA de acuerdo con el avance e innovaciones tecnológicas.

6. Derecho a la no discriminación y a la corrección de sesgos, de discriminación directa e indirecta, ilegal o abusiva.

Derechos de Oposición
Art. 8. Toda persona que sea o haya sido afectada por sistemas de IA tiene los derechos de oposición siguientes:

1. Impugnar y solicitar la revisión de las decisiones, recomendaciones o pronósticos generados el sistema cuando estos produzcan efectos jurídicos relevantes o impacten significativamente sus intereses.
2. Solicitar la corrección de sus datos cuando estos sean incompletos, inexactos o desactualizados, o estén basados en inferencias discriminatorias, irrazonables o que menoscaben la buena fe objetiva por ser datos inadecuados o abusivos procesados con métodos imprecisos o estadísticos incorrectos y que estén en uso por sistemas de IA.
3. Solicitar y tener anonimato, el bloqueo o la eliminación de datos innecesarios o excesivos.

CAPÍTULO II
DEBERES Y OBLIGACIONES DE LOS USUARIOS DE IA

Obligación Legal de los usuarios
Art. 9. Los usuarios de la IA podrán utilizar los sistemas o programas de IA, resguardando que su uso sea exclusivamente para actos, contratos o declaraciones lícitas, de cualquier índole.

Ética en el uso de la información
Art. 10. Los usuarios de la IA que utilicen sistemas o programas con IA, para múltiples actividades, acciones, labores o tareas, al obtener la información requerida, resguardarán los valores éticos en el tratamiento de la información, teniendo la debida diligencia de no ocasionar conflictos legales o penales, referentes al plagio, o violaciones a los derechos de autor.

TÍTULO III
ENTIDADES REGULADORAS, PROCEDIMIENTO Y ORGANIZACIÓN

CAPÍTULO I
ENTIDAD REGULADORA

Institución Encargada

Art. 11. La Secretaría de Innovación de la Presidencia de la República, de aquí en adelante Secretaría de Innovación, como responsable de la transformación digital de El Salvador, es la autoridad técnica y normativa encargada de dirigir, evaluar y supervisar el uso y la promoción del desarrollo de la IA y de tecnologías innovadoras. Así mismo, tiene la responsabilidad de garantizar el libre acceso y competencia de mercado, para alcanzar los objetivos de país en todo lo relacionado con la transformación digital y los objetivos de desarrollo sostenible. Por tanto, la Secretaría de Innovación desarrollará y coordinará medidas y acciones para promover y potenciar:

1. El desarrollo de la IA y su adopción como una herramienta que impulse el desarrollo económico, social, político, jurídico y ambiental del país, para mejorar la calidad de vida de toda su población.
2. El establecimiento de normas para mejorar sistemáticamente la regulación y supervisión de los sistemas de IA, así como garantizar el libre acceso y la competencia en el mercado para prevenir la formación de cualquier tipo de monopolio, oligopolio o acuerdo anticompetitivo.
3. La creación y mantenimiento actualizado del registro de sistema de IA.
4. La formación de profesionales con competencias para aprovechar, desarrollar y utilizar la IA.
5. La creación y el fortalecimiento de la infraestructura digital como medio que potencie el desarrollo de la IA.
6. El desarrollo de una infraestructura de datos que proporcione datos públicos de alta calidad, confiables, reutilizables y accesibles a los usuarios.
7. La adopción de lineamientos éticos para un uso sostenible, transparente y replicable de la IA.

8. El correcto uso de algoritmos de recomendación para garantizar a los usuarios inclusión, privacidad y transparencia en el funcionamiento del algoritmo, así como brindar los medios para que los usuarios controlen y comprendan cómo se utilizan sus datos para generar recomendaciones.
9. Las capacidades para pronunciarse sobre los incidentes graves o defectos de funcionamiento y aplicar sanciones según lo estipulado en esta Ley y otras leyes de El Salvador.
10. Un ecosistema de colaboración de IA a nivel nacional e internacional.

Entorno regulatorio para fomentar la innovación
Art. 12. La Secretaría de Innovación podrá autorizar el funcionamiento de un entorno regulatorio experimental para fomentar la innovación en IA (*sandbox* regulatorio) para las organizaciones que lo soliciten y cumplan con los requisitos especificados en esta Ley y en su reglamentación.

Solicitudes de autorización de sandboxes
Art. 13. Las solicitudes de autorización de *sandboxes* regulatorios se presentarán ante la Secretaría de Innovación a través de un proyecto que incluya, como mínimo, lo siguiente:

1. Descripción de la innovación que se tendrá en el uso de una tecnología o del uso alternativo de tecnologías existentes.
2. Descripción y respaldo técnico sobre las mejoras y sus aportes para mejorar la eficiencia, reducir costos, aumentar la seguridad, mitigar riesgos y maximizar los beneficios para la sociedad, en general, y los consumidores, en particular.
3. Incluir un plan de discontinuidad que describa las medidas a tomar para garantizar la viabilidad operativa del proyecto una vez finalizado el período de autorización del sandbox regulatorio.

Procedimientos para solicitar funcionamiento de *sandboxes*
Art. 14. La Secretaría de Innovación reglamentará los procedimientos para solicitar y autorizar el funcionamiento de los *sandboxes* regulatorios. Además, tendrá la facultad para limitar o interrumpir su funcionamiento y emitir recomendaciones considerando, entre otros aspectos, la preservación de los derechos fundamentales de los usuarios, la protección de sus datos personales y su seguridad, que puedan ser adversamente afectadas.

Responsabilidades de los participantes en un sandbox
Art. 15. Los participantes en un *sandbox* regulatorio de IA siguen siendo responsables por cualquier daño que le causen a terceros como resultado de la experimentación que están realizando en el banco de pruebas.

Procesos de minería de datos
Art. 16. El uso automatizado de obras, como extracción, reproducción, almacenamiento y transformación, en procesos de minería de datos y textos en sistemas de IA, en actividades que realizan instituciones de educación y de investigación, periodismo, museos y bibliotecas, no constituye un delito contra los derechos de autor, siempre que:

1. Se realice con fines educativos, de investigación, informativos o culturales, y se cite adecuadamente la fuente original de la obra utilizada conforme a las normas habitualmente empleadas.
2. No está destinado a la simple reproducción, exhibición o difusión de la obra original.
3. No causar daños injustificados a los intereses económicos de los autores originales.
4. No competir con el uso legítimo y correcto de las obras.

Base de datos de alto riesgo y de acceso público de IA
Art. 17. Corresponde a la Secretaría de Innovación la creación, la regulación y el mantenimiento de una base de datos de IA de alto riesgo y de acceso público de documentos de evaluación de impacto, asegurando el pleno respeto y la confidencialidad de los secretos comerciales e industriales.

Desarrollo de los sistemas IA
Art. 18. El desarrollo, ejecución y uso de sistemas de IA en El Salvador deben considerar, aplicar y ajustarse en total conformidad con los siguientes fundamentos conceptuales:

1. La persona y el respeto de los derechos humanos debe ser siempre el centro y razón de ser de todo trabajo en todas las áreas tecnológicas.
2. Todo desarrollo y uso de cualquier medio innovador y disruptivo de tecnología debe respetar la privacidad de las personas, proteger sus datos y utilizarlos con la debida autorización de conformidad con la Ley de Protección de Datos Personales.

3. Se deben respetar los principios de libre empresa, de libre competencia y de defensa del consumidor.
4. Pleno respeto al sistema de libertades y los principios democráticos republicanos.
5. El Estado debe crear y mantener condiciones que promuevan la investigación y desarrollo de los sectores productivos, especialmente de los relacionados con el desarrollo tecnológico innovador y disruptivo.
6. El Estado debe crear y mantener condiciones que promuevan la creación de información y su acceso en la educación, en todos sus niveles, mediante el uso de todos los medios tecnológicos innovadores y de IA disponibles y por existir en el futuro, así como son las plataformas educativas digitales, el uso de sistemas de tutoría virtual basados en IA o el acceso a recursos educativos en línea.
7. El Estado debe crear y mantener condiciones que promuevan y protejan la equidad la no discriminación, la pluralidad y el pleno respeto a los derechos laborales.
8. Todo desarrollo y uso de cualquier medio innovador y disruptivo de tecnología debe contribuir a la protección, recuperación y sostenibilidad del medio ambiente.

Notificación de incidentes graves de seguridad
Art. 19. Los agentes de IA informarán de inmediato a la Secretaría de Innovación cuando ocurra un incidente grave de seguridad, especialmente cuando exista algún riesgo de violación grave de los derechos humanos de las personas, de la vida e integridad física de una persona o grupo de personas, que pueda causar u ocurrir una interrupción de las operaciones de infraestructura crítica, causar daños graves a la propiedad o al medio ambiente, de acuerdo con lo establecido en esta Ley.

CAPÍTULO II
SOLICITUDES Y AUTORIZACIONES A DESARROLLADORES, PROVEEDORES Y USUARIOS DE SISTEMAS DE IA

Requisitos de la solicitud
Art. 20. Todo desarrollador, proveedor y usuario de sistemas de IA, deberá presentar una solicitud que contendrá los siguientes requisitos:

1. Tener un plan de gestión y prevención de riesgos que incluya medidas que permitan eliminar o reducir los riesgos mediante un diseño y desarrollo adecuados, y establecer medidas de mitigación y control cuando sea necesario.
2. Contar con un plan de gestión de datos de entrada que incluya la evaluación exhaustiva de posibles sesgos y deficiencias en los datos, así como tener claros y efectivos procedimientos para corregir cualquier problema identificado.
3. Garantizar que los datos de entrada proporcionados por cualquier desarrollador, proveedor o usuario sean pertinentes para la finalidad prevista del sistema de IA.
4. Contar con un sistema de registro automático de eventos mientras el sistema de IA está en funcionamiento.
5. Contar con un sistema de gestión de calidad para garantizar el cumplimiento de los requisitos establecidos en la presente Ley.
6. Contar con instrucciones de uso clara y fáciles de comprender, que deben incluir:
    a. Los datos de contacto del proveedor.
    b. Las características, capacidades y limitaciones del funcionamiento, especialmente cuando el sistema de IA es de alto riesgo.
    c. Los métodos y procedimientos para la vigilancia humana.
    d. La vida útil estimada, así como las medidas de mantenimiento y cuidados necesarias para garantizar el correcto funcionamiento del sistema de IA.
7. Contar con medidas que permitan una vigilancia efectiva por parte de los usuarios de sistemas de IA y tener una interfaz humano-máquina adecuada y un botón específico para iniciar, interrumpir y apagar el funcionamiento del sistema.
8. Demostrar un nivel adecuado de precisión, solidez y ciberseguridad en el sistema de IA.
9. Demostrar y garantizar la resistencia del sistema de IA a intentos de alteración de su uso o funcionamiento por parte de terceros no autorizados.

Autorización Previa

Art. 21. Todo desarrollador, proveedor y usuario de sistemas de IA deberá solicitar autorización previa a la Secretaría de Innovación a iniciar el desarrollo, comercialización, distribución y utilización de estos medios en El Salvador. Además, deberá certificar que se trata de una creación propia como medio para asegurar el cumplimiento del principio de respeto a la propiedad intelectual.

Plazo de resolución
Art. 22. La solicitud, también deberá incluir toda la documentación técnica necesaria para que la Secretaría de Innovación evalúe los posibles riesgos del sistema de IA a desarrollarse. La evaluación la deberá realizar en un plazo de 60 días calendario a partir del momento en que se presente la solicitud.

Examen de la solicitud por la Secretaría
Art. 23. La Secretaría de Innovación la podrá aprobar, rechazar o hacer observaciones a la solicitud. En caso de observaciones, el solicitante tendrá 30 días calendario para responder, y la Secretaría de Innovación deberá emitir una respuesta en un plazo adicional de 30 días calendario.

Una vez concedida la autorización, la Secretaría de Innovación entregará un certificado de autorización válido por 5 años, el cual deberá someterse a un nuevo proceso de autorización para su renovación. En caso de modificaciones sustanciales en un sistema de IA, el desarrollador, proveedor y usuario deben presentar una nueva solicitud de autorización.

Evaluación de los sistemas de IA
Art. 24. Para evaluar la solicitud de autorización, la Secretaría de Innovación podrá someter a los sistemas de IA a pruebas, tales como la entrega de datos de entrada y someterlos a situaciones especiales. Los desarrolladores, proveedores y usuarios deben proporcionar toda la información solicitada a la Secretaría de Innovación para que evalúe el sistema de IA.

Todas las partes involucradas en el proceso de autorización deben respetar la confidencialidad de la información y de los datos obtenidos y respetar los derechos de propiedad intelectual y la confidencialidad de la información empresarial

Declaración de Inaceptabilidad por riesgo inaceptable
Art. 25. La Secretaría de Innovación no autorizará el desarrollo, distribución, comercialización ni utilización de sistemas de IA cuando el riesgo sea calificado como inaceptable.

Observaciones y prevenciones a la solicitud
Art. 26. Después de calificar un sistema de IA como de alto riesgo, la Secretaría de Innovación realizará las observaciones pertinentes, y solicitará a todos los desarrolladores, proveedores y usuarios que cumplan los requisitos del Art. 20 de esta ley.

Garantías
Art. 27 Independientemente del nivel de riesgo, los desarrolladores, proveedores y usuarios de sistemas de IA destinados a interactuar con personas deben garantizar que están diseñados y desarrollados de manera que las personas puedan saber de inmediato que están interactuando con un sistema de IA.

Además, quienes trabajen con sistemas de IA que generen o manipulen contenido multimedia, como imagen, sonido o vídeos, que se asemeje notablemente a personas, objetos, lugares u otras entidades o eventos existentes, y que pueda inducir erróneamente a una persona a pensar que son auténticos o reales, deben informar a quienes accedan a dicho contenido que ha sido generado de forma artificial o manipulado por un sistema de IA.

Procedimiento en caso de Incidentes
Art. 28. Los desarrolladores, proveedores y usuarios de sistemas de IA deben notificar a la Secretaría de Innovación cuando se presente un incidente grave o un defecto de funcionamiento.

Una vez notificada, la Secretaría de Innovación deberá informar a todos los desarrolladores, proveedores y usuarios la suspensión temporal del desarrollo, distribución, comercialización y utilización del sistema de IA afectado. La Secretaría de Innovación tendrá un plazo de 15 días calendario para evaluar el incidente notificado y pronunciarse sobre él, pudiendo retirar la autorización conferida a los desarrolladores, proveedores y usuarios o levantar la suspensión temporal.

Sistema de acceso al público
Art. 29. La Secretaría de Innovación deberá contar con un sistema de acceso público para recibir solicitudes de autorización para el desarrollo, distribución, comercialización y utilización de sistemas de IA, así como para notificar incidentes graves o defectos de funcionamiento.

Registro Público
Art. 30. La Secretaría de Innovación deberá contar con un registro público de:

1. Las solicitudes de autorización para el desarrollo, distribución, comercialización y utilización de sistemas de IA, informando claramente si fueron autorizadas o rechazadas por la Secretaría de Innovación.

2. Los incidentes graves y defectos de funcionamiento notificados por desarrolladores, proveedores y usuarios, así como las decisiones que haya adoptado la Secretaría de Innovación en respuesta a dichas notificaciones.

Sanción
Art. 31. El incumplimiento de las normas contenidas en la presente Ley por parte de un desarrollador, proveedor y usuario será sancionado con cuarenta y cinco (45) salarios mínimos del Sector de Comercio y Servicios, que deberá ser pagado en la Dirección General de Tesorería del Ministerio de Hacienda.

En el caso de que la sanción sea consecuencia de no haber notificado un incidente grave o haber presentado información inexacta, incompleta o engañosa, el monto de las sanciones se duplicará. Además, la Secretaría de Innovación podrá retirar la autorización de distribución, comercialización o uso, según corresponda.

Desobediencia
Art. 32. El desarrollo, distribución, comercialización o uso de sistemas de IA de riesgo inaceptable serán sancionados con prisión entre tres (3) años y 5 años de prisión, será aplicable en estos casos la Ley Especial contra los delitos informáticos y conexos; y el Código Penal en los casos de que se hayan cometido concurso real o ideal de delitos, o delitos contra con colectivos vulnerados.

CAPÍTULO III
CLASIFICACIÓN DE RIESGOS

Evaluación de Riesgos
Art. 33. Antes de ofrecer y comercializar un sistema de IA, el proveedor deberá realizar una evaluación de riesgos y clasificar el sistema de acuerdo con los criterios establecidos en esta Ley, incluyendo una evaluación preliminar de los fines o aplicaciones del sistema, así como el registro de los procesos y la documentación que la respalda para determinar responsabilidades y solicitar rendición de cuentas.

En caso que el sistema no sea clasificado como de alto riesgo, la Secretaría de Innovación podrá notificar y exigir la reclasificación del sistema de IA, así como requerir una evaluación de impacto algorítmico cuando sea necesario realizar una investigación.

Sistemas de Alto Riesgo

Art. 34. Son sistemas de IA de alto riesgo los que son utilizados para los siguientes fines:

1. Como dispositivos de seguridad en la gestión y funcionamiento de infraestructuras críticas, como control de tráfico aéreo, marítimo y terrestre, y redes suministro de agua y electricidad.
2. En educación y formación profesional, incluidos los sistemas y procesos utilizados para determinar el acceso a instituciones educación o de formación profesional, así como para la evaluación y seguimiento de los estudiantes.
3. En reclutamiento, selección, filtrado y evaluación de candidatos, así como para tomar decisiones sobre ascensos o finalización de contratos laborales, división de tareas, control y evaluación del desempeño y comportamiento de las personas afectadas por dichas aplicaciones de IA utilizadas en las áreas de empleo, gestión de los trabajadores y el acceso al empleo por cuenta propia.
4. Evaluación de criterios para el acceso, elegibilidad, revisión, disminución o revocación de servicios públicos y privados esenciales, incluidos los de asistencia pública y servicios de seguridad.
5. En la evaluación de la capacidad de endeudamiento de las personas naturales o jurídicas y los métodos y criterios para definir su calificación crediticia.
6. Para establecer prioridades para los servicios de emergencias como asistencia médica, policía y seguridad pública y bomberos.
7. En la administración de justicia, como son los sistemas que ayudan a las autoridades judiciales en la investigación de posibles delitos y en la aplicación de la ley.
8. En vehículos autónomos, cuando su uso pueda crear riesgos para la integridad física de las personas.
9. En aplicaciones utilizadas en el sector de la salud, incluidas aquellas que se utilicen como auxiliar en diagnósticos y procedimientos médicos.
10. Los sistemas de identificación biométrica.
11. En la investigación criminal y la seguridad pública, cuando se utiliza para evaluar riesgos individuales y determinar el riesgo potencial que una persona cometa infracciones, delitos o sea reincidente, así como para identificar posibles víctimas o para evaluar rasgos de personalidad, características o registro de comportamiento criminal de personas o grupos.

12. En estudios y análisis de delitos contra las personas obtenidos de grandes y complejas bases de datos obtenidas de diferentes fuentes y formatos para identificar patrones desconocidos y descubrir relaciones ocultas, por parte de las autoridades policiales, de investigación y de justicia.
13. En procesos de gestión de migraciones y control de fronteras.

Incorporación y Actualización por nuevas aplicaciones

Art. 35. La Secretaría de Innovación será la responsable de actualizar la lista de sistemas de IA de alto riesgo cuando surjan nuevas aplicaciones, considerando al menos uno de los siguientes criterios:

1. Que la implementación del sistema sea a gran escala, considerando el número de personas afectadas, su duración y frecuencia.
2. Que el sistema pueda violar derechos y libertades o la utilización de un servicio.
3. Que el sistema tenga un alto potencial de dañar material o moralmente o crear discriminación.
4. Que el sistema afecte a personas de un grupo vulnerable específico.
5. Que los posibles resultados nocivos del sistema sean irreversibles o difíciles de revertir.
6. Que un sistema similar de IA haya causado previamente daño material o moral.
7. Que por el bajo grado de transparencia, explicabilidad y auditabilidad del sistema de IA se dificulte su control y supervisión.
8. Cuando exista un alto nivel de identificabilidad de los usuarios, incluyendo el procesamiento de datos genéticos y biométricos para identificar con total certeza a una persona, especialmente cuando el proceso incluye posibilidades de combinar, cotejar o comparar datos de diferentes fuentes.
9. Cuando existan expectativas razonables de afectar a una persona o grupo de personas mediante el uso de sus datos en el sistema de IA, especialmente en lo relacionado con la confidencialidad, como en el procesamiento de datos confidenciales o sensibles.

CAPÍTULO IV
LA GOBERNANZA DE LOS SISTEMA DE INTELIGENCIA ARTIFICIAL

Seguridad de los Sistemas
Art. 36. Los agentes de IA deben establecer protocolos de gobernanza y ética y aplicarlos en los procesos internos para de garantizar la seguridad de los sistemas y el cumplimiento de todos los derechos de las personas según esta Ley y las leyes relacionadas, los que deben incluir, al menos, las siguientes medidas:

1. De transparencia con relación al uso de sistemas de IA en la interacción con personas naturales.
2. De transparencia en la comunicación e información relativa a las medidas de gobernanza y ética utilizadas en el desarrollo y uso del sistema de IA de la empresa o del agente o de los agentes.
3. De gestión de datos para reducir y prevenir potenciales sesgos discriminatorios.
4. Para la legitimación del tratamiento, protección de datos y respeto a la privacidad desde el diseño, desarrollo y adopción de técnicas que minimicen el uso de datos personales.
5. Adopción de parámetros adecuados y éticos para separar y organizar datos para entrenamiento, prueba y validación de resultados del sistema.
6. Para dar la mayor seguridad posible a la información utilizada desde la concepción hasta la operación del sistema.

Estas medidas de gobernanza y ética de los sistemas de IA se deben aplicar durante todo su ciclo de vida, desde la concepción hasta la discontinuación o el cierre de sus actividades

Medidas de Gobernanza y Ética
Art. 37. En el caso de sistemas de IA de alto riesgo, los agentes de IA deben adoptar y cumplir las siguientes medidas de gobernanza y ética en todos los procesos internos:

1. Tener la documentación que sustenta el proceso de desarrollo y la tecnología utilizada para el funcionamiento del sistema y las decisiones que se tomaron en su construcción, y uso, considerando todas las etapas relevantes en el ciclo de vida del sistema, como son diseño, desarrollo, evaluación, operación e interrupción del sistema.

2. Contar con herramientas de registro automático para el funcionamiento del sistema, para poder realizar una evaluación sobre su precisión, robustez y ética, así como determinar su potencial discriminatorio, conocer las medidas adoptadas para mitigar riesgos y los posibles efectos adversos.
3. Realizar pruebas para evaluar e identificar si se tienen adecuados niveles de fiabilidad, considerando el tipo de aplicación del sistema de IA, incluidas las pruebas de robustez, exactitud, precisión y cobertura.
4. Tener definidas y aplicar medidas técnicas que garanticen la explicabilidad de los resultados de los sistemas de IA. Estas medidas deben estar disponibles para los operadores y posibles afectados por el funcionamiento y uso del sistema, y deben explicar tanto la lógica como los criterios relevantes para producir resultados y para su interpretación. Esto debe hacerse respetando el secreto industrial y comercial.
5. Informar de manera inmediata a la Secretaría de Innovación cuando tengan conocimiento de uno o más riesgos inesperados que tengan el potencial de violar los derechos de las personas.

Evaluación del Impacto Algorítmico

Art. 38. Cuando un sistema de IA sea clasificado como de alto riesgo según la evaluación preliminar, el proveedor debe hacer una evaluación del impacto algorítmico. Esta evaluación debe ser realizada por profesionales externos al proveedor, quienes deben contar con amplios y demostrados conocimientos técnicos, científicos y legales relacionados con esta área tecnológica. Dichos profesionales deben elaborar un informe de resultados y recomendaciones de manera independiente.

Publicaciones de información sensible

Art. 39. Queda estrictamente prohibida a personas naturales y jurídicas la publicación de bases de datos que contengan información financiera, especialmente las que están relacionadas con transacciones en monedas digitales o criptoactivos, ya sea de manera electrónica o física. Además, queda prohibido el uso, manipulación o venta de códigos de acceso o cualquier información sensible sin la autorización expresa de cada uno de los usuarios propietarios de dicha información.

Metodología
Art. 40. La metodología de evaluación de impacto algorítmico debe incluir, al menos los siguientes componentes:

1. Los conceptos y fundamentos utilizados para la preparación de la evaluación.
2. La identificación y consideración de los riesgos conocidos y los previsibles desde el desarrollo hasta la implementación y uso del sistema de IA.
3. Propuestas concretas que aseguren la reducción de los riesgos identificados.
4. Un proceso seguimiento claro y bien definido, que incluya pruebas de control de calidad, evaluaciones y medidas para mitigar los riesgos, así como programas para capacitar y sensibilizar sobre los riesgos y beneficios asociados con el sistema de IA.

La Secretaría de Innovación podrá establecer cualquier otro criterio, metodología y factores necesarios para preparar una evaluación de impacto, regular la frecuencia de las actualizaciones en concordancia con el ciclo de vida de los sistemas de IA de alto riesgo, tanto en las áreas de aplicación existentes como en las que puedan surgir en el futuro.

TÍTULO IV
RESPONSABILIDADES, PRECEPTOS DE BUENAS PRÁCTICAS

CAPÍTULO I
RESPONSABILIDADES

Reparación del daño
Art. 41. El proveedor u operador de un sistema de IA, especialmente de aquellos sasos clasificados como de alto riesgo o riesgo excesivo, deberá reparar íntegramente cualquier daño material o moral causado a una persona o grupo de personas, en directa proporción a su grado de participación en dicho daño.

En el caso de comprobarse que un proveedor u operador de un sistema de IA ha causado un daño a una persona o grupo de personas, la Secretaría de Innovación impondrá una sanción que oscilará entre veinte (20) y cincuenta (50) salarios mínimos del Sector de Comercio y Servicios.

Agentes
Art. 42. Los agentes de inteligencia artificial no serán responsable cuando:

1. Demuestren que no pusieron en circulación, emplearon o se aprovecharon del sistema de IA.
2. Comprueben que el daño es efectivamente propio de la víctima o de un tercero o que es un caso fortuito externo.

CAPÍTULO II
PRECEPTOS DE BUENAS PRÁCTICAS, ÉTICA Y GOBERNANZA

Buenas Prácticas
Art. 43. Los agentes de IA podrán, ya sea individualmente o a través de asociaciones, establecer sus propios criterios o códigos de buenas prácticas, ética y gobernanza, los cuales deben señalar de manera clara y precisa:

1. Las características de la organización, las normas éticas que aplican, el régimen de funcionamiento y coordinación y los métodos y procedimientos que utilizan.
2. Los medios que tienen para que las personas afectadas puedan realizar denuncias.
3. Los estándares de seguridad, las normas técnicas y obligaciones para la implementación del sistema.
4. Los programas para capacitar a los trabajadores y educar e informar a los usuarios.
5. Los mecanismos internos de supervisión y mitigación de riesgos y las medidas técnicas y organizativas de seguridad para la gestión de los riesgos.

Gobernanza
Art. 44. Los programas de gobernanza deben como mínimo mostrar:

1. El compromiso de cumplir fielmente los procesos y políticas internas, así como los preceptos o códigos de buenas prácticas, ética y gobernanza para no causar daños a personas o grupos de personas y asegurar la proporcionalidad entre los métodos utilizados y los fines determinados y legítimos de los sistemas de IA.

2. Que existe una relación entre la estructura, escala y volumen de sus operaciones, incluso identificando su potencial para causar daños.
3. Que para establecer una relación de confianza con las personas que utilicen el sistema de IA, hay libre acceso a información y a un actuar transparente que asegure mecanismos de consulta y participación.
4. Medios para garantizar que se tienen procesos integrados de gobernanza y ética por la estructura de la organización y de supervisión interna y externa.
5. Que se cuenta con planes de respuesta para revertir los posibles resultados dañino que pueda causar sistema de IA.
6. Que se cuenta con métodos y procesos para actualizar sistemáticamente los programas de gobernanza y ética mediante el uso de la información que se obtenga del seguimiento continuo y de las evaluaciones periódicas.

La Secretaría de Innovación podrá establecer, modificar o derogar procedimientos para analizar la compatibilidad del código de conducta y ética en consistencia con los resultados de las actualizaciones periódicas y la legislación vigente.

TÍTULO V
ORGANISMO DE CONTRALORÍA SOCIAL Y SEGURIDAD DIGITAL

CAPÍTULO I
NORMAS SOBRE RECOMENDACIÓN ALGORÍTMICA

Supervisión de los servicios de recomendación algorítmica

Art. 89. Los proveedores de servicios de recomendación algorítmica deben:

1. Contar con procesos que garanticen la seguridad de sus servicios de recomendación algorítmica.
2. Establecer y completar sistemas de gestión y medidas técnicas para revisar, evaluar, monitorear y verificar:
    a. Los mecanismos algorítmicos
    b. La gobernanza y ética tecnológica para no causar daños a los usuarios.
    c. El registro de usuarios.
    d. Los medios que tienen para la verificación de los procesos de difusión de información.
    e. Los sistemas de ciberseguridad y de gestión de incidentes de seguridad.

f. Los medios para informar y dar respuesta a las consultas de los usuarios.

3. Contar con sistemas que garanticen:
    a. La total seguridad de los datos.
    b. La debida protección de la información personal.
    c. La prevención de cualquier tipo de fraude.
4. Tener claramente definidas las normas que rigen el servicio de recomendación algorítmica y los medios que tienen para informar a los usuarios de manera clara y precisa.
5. Tener personal especializado y el soporte técnico necesario de acuerdo con la escala de los servicios de recomendación algorítmica que ofrece.

Verificación y evaluación

Art. 90. Los proveedores de servicios de recomendación algorítmica deben examinar, verificar y evaluar sistemáticamente los sistemas, modelos, datos y aplicaciones algorítmicas, entre otras, para garantizar el cumplimiento de lo dispuesto en esta Ley sobre ética y moral.

Deber de los proveedores

Art. 91. Los proveedores de servicios de recomendación algorítmica deben fortalecer sus sistemas para garantizar la seguridad de la información y establecer bases de datos completas con características que les permitan identificar información ilegal y dañina. Además, deben implementar estándares, normas y procesos para la entrada de bases de datos de alta calidad. En caso de que la información generada algorítmicamente carezca de un indicador, se debe marcar con uno para poder continuar con la difusión.

Tan pronto se identifique que hay información ilegal, el proveedor de servicios de recomendación algorítmica debe detener su difusión de forma inmediata, adoptar medidas para eliminarla, conservar los registros pertinentes e informar detalladamente a la Secretaría de Innovación sobre el incidente en cuestión.

Fortalecimiento de los sistemas

Art. 92. Los proveedores de servicios de recomendación algorítmica deben fortalecer sistemáticamente sus modelos y la gestión de etiquetado de usuarios, así como actualizar y mejorar sistemáticamente las normas para registrar los intereses en los modelos de usuario y las de gestión de etiquetado de usuarios.

Queda prohibida la introducción de información ilegal o dañina, así como convertirlas en etiquetas de usuario para utilizarlas como base para recomendar contenido informativo.

Fortalecimiento de la visualización del servicio
Art. 93. Los proveedores de servicios de recomendación algorítmica deben fortalecer la visualización del servicio de recomendación algorítmica o la gestión ecológica de la página, establecer y perfeccionar mecanismos para la intervención manual y la elección autónoma del usuario, y presentarán vigorosamente información conforme a las orientaciones de valores convencionales en segmentos clave como las portadas y las pantallas principales. términos de búsqueda populares, temas seleccionados, listas de temas, ventanas emergentes, entre otros.

Utilización de recursos técnicos
Art. 94. Los proveedores de servicios de recomendación algorítmica deben utilizar recursos técnicos de manera integral para garantizar un alto grado de transparencia, facilitar la comprensión de la búsqueda, así como la clasificación, selección, notificación automática y visualización del contenido, para evitar la generación de influencias nocivas y reducir posibles controversias o disputas con los usuarios.

Art. 95. Se prohíbe a los proveedores de servicios de recomendación algorítmica utilizar algoritmos para registrar usuarios falsos, intercambiar o manipular cuentas ilegales de usuarios o aprobaciones (likes), comentarios y acciones compartidas que sean falsas o realizar acciones que influyan en la opinión pública.

Prohibición de imposición de restricciones a proveedores
Art. 96. Se prohíbe a los proveedores de servicios de recomendación algorítmica utilizar algoritmos para imponer restricciones a otros proveedores que atenten contra el libre mercado, obstruir o dañar el normal funcionamiento de estos servicios de información, realizar actos para establecer un monopolio, oligopolio o un acuerdo anticompetitivo.

Protección de los derechos de los usuarios de servicios de recomendación algorítmica
Art. 97. Los proveedores de servicios de recomendación algorítmica deberán informar y notificar de manera sistemática y clara a los usuarios sobre los servicios que ofrecen, incluyendo los

principios básicos, propósitos y motivos, así como los principales mecanismos operativos, en un formato de fácil comprensión.

Desactivación de servicios
Art. 98. Los proveedores de servicios de recomendación algorítmica deberán brindar a los usuarios la opción de no utilizar sus características personales y darles una opción para desactivar los servicios, ante lo cual dejará de prestar los servicios relacionados de inmediato. Asimismo, proporcionarán a los usuarios la opción para elegir o eliminar etiquetas de usuario utilizadas para servicios de recomendación algorítmica basados en sus características personales.

Cuando los proveedores de servicios de recomendación algorítmica utilicen algoritmos de manera que generen una influencia que vulnere los derechos o los intereses de los usuarios, deberán dar una explicación detallada y asumir la responsabilidad correspondiente de acuerdo con lo establecido en esta Ley y en aquellas que tengan una relación con el caso.

Derechos de Protección de las niñas, niños y adolescentes
Art. 99.- Cuando los proveedores de servicios de recomendación algorítmica brinden servicios a niños, niñas y adolescentes, deberán cumplir con el Principio del Interés superior, y los derechos de protección, conforme a esta Ley y aquellas que tengan relación con los derechos de los niños, niñas y adolescentes, y evitar proporcionarles información que dañe su salud física y mental, mediante el desarrollo de modelos adecuados para su uso por parte de la niñez y adolescencia.

Se prohíbe a los proveedores de servicios de recomendación algorítmica difundir información a niños, niñas y adolescentes, que pueda incitarlos a imitar conductas inseguras o actos que vulneren la ética y la moral social, adoptar tendencias dañinas o que puedan influir en su salud física y mental o causarles una adicción al uso de algunas bebidas y otros productos que se sabe que generan daños en el cuerpo de las personas, se aplicará la Ley Crecer Juntos para la Protección Integral de la Primera Infancia, niñez y adolescencia.

Protección de Derechos Fundamentales
Art. 100.- Cuando los proveedores de servicios de recomendación algorítmica brinden sus servicios a personas mayores de edad, deberán respetar sus derechos conforme a esta Ley y aquellas que tengan relación con sus derechos personales. Además, deberán considerar sus diversas necesidades y dificultades para salir, desplazarse, someterse a tratamientos médicos, consumir y evitar fraudes. Para cumplir con estos requisitos, los proveedores de servicios de recomendación algorítmica deberán proporcionar servicios inteligentes diseñados para personas mayores de edad, que garanticen un acceso amigable y seguro y para que tengan respuestas de fácil comprensión en el uso de estos servicios.

Facilitación del servicio
Art. 101.- Los operadores de servicios de recomendación algorítmica deberán proporcionar medios de acceso fáciles y eficientes para que los usuarios puedan presentar sus quejas de manera abierta y pública, para conocer los flujos de trabajo y los tiempos de respuestas a las demandas y quejas de los usuarios.

CAPÍTULO II
NORMAS SOBRE CIBERSEGURIDAD

Objeto
Art. 45. El objeto de las normas sobre ciberseguridad es garantizar el correcto funcionamiento de los sistemas de información, redes y servicios de comunicaciones electrónicas que son fundamentales para las actividades diarias de la sociedad y el desarrollo económico y social, político, jurídico y ambiental de El Salvador; así como alcanzar un alto nivel de ciberseguridad, ciber resiliencia y confianza, en los productos, servicios y procesos tecnológicos; y contar con sólidas defensas ante las ciber amenazas y los ciberataques.

Entidad Supervisora
Art. 46. La Secretaría de Innovación es la instancia responsable de supervisar los sistemas digitales y el uso de IA para fortalecer la ciberseguridad en El Salvador, para que sea un lugar más seguro para vivir y hacer negocios en línea para las personas como para las empresas. Por tanto, la Secretaría de Innovación debe desarrollar las capacidades necesarias para asesorar y dar capacitaciones especializadas en ciberseguridad a las instituciones del sector público y a las empresas que operan productos, servicios y procesos tecnológicos.

Estrategia de Ciberseguridad
Art. 47. La Secretaría de Innovación formulará la Estrategia de Ciberseguridad de El Salvador, la cual revisará y, como mínimo, la actualizará anualmente para prevenir nuevas amenazas de ataques cibernéticos.

Sistemas de Alto Riesgo
Art. 48.- Se consideran como sistemas de IA de alto riesgo los que se crean para ser utilizados en:

1. La identificación biométrica remota en tiempo real o diferido de personas en espacios privados.
2. La gestión del suministro de agua y electricidad.
3. La asignación y determinación del acceso a establecimientos de educación, así como para la evaluación de estudiantes.
4. La selección y contratación de personas en trabajos.
5. La asignación de tareas y el seguimiento y evaluación del rendimiento y la conducta de trabajadores.
6. La evaluación de personas para acceder a prestaciones y servicios de asistencia pública.
7. La evaluación de la solvencia o establecer la calificación crediticia de personas.
8. Situaciones de emergencia y desastre, especialmente en la asignación de recursos o el establecimiento de prioridades para el envío de servicios de intervención, como bomberos, ambulancias, personal militar y de la policía.
9. La determinación del riesgo que personas cometan infracciones penales o ser reincidentes, así como la identificación y prevención del riesgo para las potenciales víctimas de delitos.
10. Cualquier etapa de una investigación y en la interpretación de hechos que puedan constituir un delito en el contexto de un juicio.
11. La gestión de situaciones de migración, asilo y control fronterizo.
12. Procesos que puedan causar un perjuicio a la salud y la seguridad de las personas o violar sus derechos constitucionales.

Apoyo y Promoción de la Ciberseguridad
Art. 49. La Secretaría de Innovación dará apoyo y promocionará la ciberseguridad mediante programas para que las empresas del sector privado, las instituciones del sector público, organizaciones de la sociedad civil y la sociedad tengan información y adecuados conocimientos teóricos y prácticos sobre ciberseguridad, especialmente en aspectos relativos a ciber higiene y ciber alfabetización, así como para mejorar la prevención, detección, análisis y capacidad de respuesta a ciber amenazas e incidentes.

Programa de Certificación de Sistemas
Art. 50. La Secretaría de Innovación establecerá una normativa para que las empresas que se especializan en brindar productos, servicios y procesos de tecnologías de la información y las comunicaciones puedan obtener transparentemente una certificación que sus sistemas tienen programas que garantizan un alto nivel de ciberseguridad de acuerdo con los estándares internacionales.

El diseño del programa de certificación de la ciberseguridad deberá cumplir al menos los siguientes objetivos de seguridad:

1. Proteger los datos almacenados, transmitidos o tratados de otra manera para que estén resguardados frente a cualquier tipo de almacenamiento, tratamiento, acceso o revelación accidental o no autorizada durante todo el ciclo de vida del producto, servicio o proceso.
2. Proteger los datos almacenados, transmitidos o tratados contra la destrucción accidental o no autorizada, la pérdida o la alteración o la falta de disponibilidad durante todo el ciclo de vida del producto, servicio o proceso.
3. Garantizar que únicamente las personas, programas o máquinas autorizadas puedan acceder a los datos, servicios o funciones que han sido autorizadas por la Secretaría de Innovación.
4. Demostrar capacidades para detectar y documentar las vulnerabilidades que se conocen o puedan generarse.
5. Demostrar capacidades para identificar, registrar y comprobar los datos, servicios o funciones que han sido objeto de acceso, uso u otro tratamiento, mostrando el momento y persona responsable.
6. Garantizar que los productos, servicios y procesos no contengan vulnerabilidades conocidas.

7. Demostrar capacidades para restaurar rápidamente la disponibilidad y el acceso a los datos, servicios y funciones en caso de incidente físico o tecnológico.
8. Garantizar que los productos, servicios y procesos tecnológicos sean seguros desde el diseño.
9. Garantizar que los productos, servicios y procesos tecnológicos se entreguen mediante programas y equipos informáticos actualizados, libres de vulnerabilidades conocidas públicamente y con medios para efectuar actualizaciones de seguridad.

Informes periódicos

Art. 51. La Secretaría de Innovación deberá preparar periódicamente cada tres meses y compartir dicha información en los medios electrónicos pertinentes:

1. Análisis y evaluación de impacto de las tecnologías emergentes, así como los efectos esperados de tipo social, jurídico, económico y normativo de las innovaciones tecnológicas sobre la ciberseguridad.
2. Análisis estratégicos a largo plazo de las ciberamenazas e incidentes, para detectar e informar sobre las tendencias emergentes y contribuir a su prevención.
3. Orientaciones sobre las mejores prácticas para la seguridad de las redes y los sistemas de información, con especial énfasis en la seguridad de las infraestructuras críticas.
4. Información sobre la ciberseguridad en su sitio web, en un espacio especialmente asignado para este propósito.
5. Análisis e informes sobre incidentes significativos, que estarán a libre disposición de instituciones del sector privado, del sector público, organizaciones de la sociedad civil y la sociedad, en general.
6. Sin perjuicio de lo dispuesto en numeral 5 anterior, la Secretaría de Innovación no divulgará a terceros la información que trate o reciba mediante una solicitud de tratamiento confidencial.
7.

Programas de Ciberseguridad

Art. 52. La Secretaría de Innovación deberá tener programas para:

1. Sensibilizar y orientar al público sobre los riesgos relacionados con la ciberseguridad y sobre las buenas prácticas que recomienda seguir a todo usuario, especialmente en cuanto a ciber higiene y ciber alfabetización, información que debe

estar disponible en su sitio web en un espacio especialmente asignado para este propósito.
2. Realizar periódicamente campañas de divulgación de información para aumentar el conocimiento y la conciencia sobre ciberseguridad.

Objetivos de la Ciberseguridad

Art. 53. La Secretaría de Innovación deberá establecer programas de certificación de ciberseguridad para cumplir, al menos, los siguientes objetivos de seguridad:

1. Proteger los datos almacenados, transmitidos o procesados de manera accidental o no autorizada durante todo el ciclo de vida del producto, servicio o proceso tecnológico.
2. Proteger los datos almacenados, transmitidos o procesados contra accesos o revelaciones accidentales o no autorizados durante todo el ciclo de vida del producto, servicio o proceso tecnológico.
3. Asegurar que solo las personas, programas o máquinas autorizadas puedan acceder a los datos, servicios o funciones correspondientes a su derecho de acceso.
4. Detectar y documentar las dependencias y vulnerabilidades conocidas, así como registrar los datos, servicios o funciones relacionados con el acceso, uso u otro tratamiento de los datos, incluyendo el momento en que se produjo el incidente y el nombre de la persona responsable.
5. Disponer de medios para verificar los datos, servicios o funciones que fueron objeto de acceso, uso u otro tratamiento, así como registrar el momento en que se produjo el incidente y el nombre de la persona involucrada.
6. Verificar la ausencia de vulnerabilidades conocidas en los productos, servicios y procesos tecnológicos.
7. Restaurar la disponibilidad y el acceso a los datos, servicios y funciones de forma rápida en caso de incidente físico o técnico.
8. Asegurar que los productos, servicios y procesos tecnológicos sean seguros contra defectos desde su diseño.
9. Asegurar que los productos, servicios y procesos de tecnologías de la información y las comunicaciones se entreguen siempre con programas y equipos informáticos actualizados y seguros, que no contengan vulnerabilidades conocidas y que dispongan de mecanismos para efectuar actualizaciones de seguridad.

Certificación de Ciberseguridad

Art. 54. La Secretaría de Innovación establecerá los requisitos que el fabricante o el proveedor de productos, servicios o procesos tecnológicos deben cumplir para obtener la certificación de ciberseguridad. Estos requisitos deben incluir, al menos, los siguientes:

1. El objeto y alcance del esquema de certificación, incluido el tipo o categoría de productos, servicios y procesos tecnológicos que se deben tener
2. Una clara descripción de los requisitos a cumplir, su finalidad y los métodos de evaluación y los niveles de garantía considerados de acuerdo con las necesidades de los potenciales usuarios.
3. Referencias a las normas internacionales o de El Salvador que se aplicarán para hacer la evaluación para la certificación de la ciberseguridad.
4. Toda la información necesaria para la certificación que el solicitante debe facilitar a la Secretaría de Innovación, incluyendo el tiempo que debe estar disponible.
5. Las condiciones para poder utilizar marcas o etiquetas cuando el modelo de trabajo prevea marcas o etiquetas.
6. Los métodos para controlar el cumplimiento de los productos, servicios y procesos tecnológicos, incluidos los mecanismos para demostrar el cumplimiento sistemático de los requisitos de ciberseguridad especificados.
7. Las condiciones para la expedición, mantenimiento, continuación y renovación de un certificado de ciberseguridad, así como condiciones para la ampliación o la reducción del alcance de la certificación.
8. Las consecuencias para los productos, servicios y procesos tecnológicos cuando dejan de cumplir con los requisitos establecidos.
9. Las normas sobre cómo se deben notificar y tramitarse las vulnerabilidades de ciberseguridad previamente no detectadas en productos, servicios y procesos tecnológicos.
10. El contenido y formato de los certificados de ciberseguridad que serán entregados, su período de validez y la política de divulgación de la información.

Estándares de ciberseguridad
Art. 55. La Secretaría de Innovación revisará y actualizará sistemáticamente las normas y requisitos para una gestión segura de la ciberseguridad, teniendo en cuenta los estándares y las mejores prácticas que son internacionalmente aceptados. Estas actualizaciones se aplicarán tanto a los productos, servicios y sistemas de operaciones en red del sector público como del sector privado.

Apoyo y coordinación
Art. 56. La Secretaría de Innovación apoyará a las empresas y programas innovadores de tecnología de ciberseguridad, así como al desarrollo, aplicación y la divulgación masiva de tecnologías de ciberseguridad, que contribuyan a brindar productos y servicios de red seguros y confiables. Además, velará por proteger los derechos de propiedad intelectual de las tecnologías de red y apoyará a las instituciones que realizan investigaciones y desarrollo relacionadas con la ciberseguridad, incluyendo las instituciones de educación superior.

Certificación
Art. 58. Los productos digitales solo podrán ser comercializados en El Salvador una vez que la Secretaría de Innovación haya certificado que sus fabricantes o desarrolladores cumplen con los requisitos esenciales establecidos en esta Ley para garantizar la ciberseguridad. Esta certificación se otorgará únicamente a aquellos productos que demuestren mantener estos estándares en uso, para prevenir, contrarrestar y eliminar riesgos o ataques cibernéticos.

Seguridad de las operaciones de red
Art. 59. La Secretaría de Innovación les requerirá a los operadores de red cumplir con requisitos para la protección de la seguridad que sean compatibles con un sistema de protección multinivel de ciberseguridad para garantizar que la red esté libre de interferencias, daños o acceso no autorizado, así como para evitar fugas, robo o falsificación de datos de la red. Por tanto, los operadores de red deberán:

1. Formular sistemas de gestión de seguridad interna y reglas operativas, determinar las personas responsables de la ciberseguridad y definir claramente el personal que tiene la responsabilidad de protección y cumplimiento con los requisitos de la ciberseguridad.

2. Adoptar medidas técnicas para prevenir virus informáticos, ciberataques, intrusiones en la red y otras acciones que pongan en peligro la ciberseguridad;
3. Adoptar medidas técnicas para monitorear y registrar los estados operativos de la red, así como los incidentes de ciberseguridad como está determinado en esta Ley.
4. Implementar medidas para la clasificación de datos y definir niveles de acceso y manejo de información según su sensibilidad y mantener una copia de seguridad encriptada de los datos críticos.

Prohibición de instalación de programas maliciosos
Art. 60. Se prohíbe a los proveedores de productos y servicios de red instalar programas maliciosos. En el momento de descubrir que cualquiera de sus productos y servicios tienen fallas o vulnerabilidades de seguridad, informarán inmediatamente a la Secretaría de Innovación e implementarán medidas correctivas e informarán internamente a los trabajadores de la organización y a los usuarios.

Mantenimiento de seguridad
Art. 61. Los proveedores de productos y servicios de red deberán proporcionar mantenimiento de seguridad para todos sus productos y servicios. Este mantenimiento se llevará a cabo según los términos y períodos acordados con los clientes.

Consentimiento del titular
Art. 62. Cuando un producto o servicio de red tenga como función recabar información personal del usuario, el proveedor deberá indicarlo claramente y obtener el consentimiento del titular de acuerdo con lo dispuesto en esta ley y otras leyes relacionadas con la protección de datos personales.

Respuesta de emergencias
Art. 63. Los operadores de redes deberán tener planes de respuesta de emergencia para incidentes de ciberseguridad y abordar con prontitud las vulnerabilidades de los sistemas, virus informáticos, ciberataques, intrusiones en la red y otros riesgos de ciberseguridad similares. Cuando se produzcan cualquiera de estos tipos de incidentes de ciberseguridad, los operadores de redes deben aplicar de inmediatamente un plan de respuesta de emergencia, adoptar las medidas correctivas necesarias e informar a las instancias internas de conformidad con las disposiciones establecidas.

Prohibición en violaciones de Derechos de las partes
Art. 64. Queda prohibido que las empresas, su personal y personas naturales participar o involucrarse en intromisiones en las redes de otras partes, de manera que violen los dispuesto en esta Ley, así como interrumpir el funcionamiento normal de las redes de otras partes, ni robar datos de la red ni participar en otras actividades que pongan en peligro la ciberseguridad. Tampoco deben proporcionar programas o herramientas que pueden ser utilizados para interrumpir cualquier tipo de funciones de la red y las medidas de protección, ni deben participar en cualquier acción que conlleve el robo datos de la red o participar en otros actos que pongan en peligro la ciberseguridad.

Además, queda prohibido a las empresas, su personal o personas naturales brindar ayuda, soporte técnico, publicidad, promoción o pago de gastos cuando tengan un conocimiento claro y comprobable de las organizaciones o personas que participan en acciones que ponen en peligro la ciberseguridad.

Apoyo Interinstitucional
Art. 65. Los operadores de redes brindarán apoyo y asistencia técnica a los órganos de seguridad pública y al Ministerio de Defensa encargados de salvaguardar la seguridad nacional, así como a los que realicen investigaciones de actividades delictivas de conformidad con esta ley y otras leyes relacionadas con aspectos tecnológicos y de IA.

Cooperación entre operadores
Art. 66. La Secretaría de Innovación, así como todas las dependencias del Estado deben apoyar, estimular y potenciar la cooperación entre los operadores de redes en áreas como recopilación, análisis, notificación y manejo de situaciones de emergencia por incidentes de ciberseguridad, para aumentar la capacidad de salvaguarda de la seguridad de los operadores de redes.

Sistema de coordinación y apoyo
Art. 67. Las empresas privadas y todas las dependencias del Estado deben establecer y aplicar métodos y sistemas para la estandarización y coordinación de la ciberseguridad en sus organizaciones, así como fortalecer las capacidades para el análisis y evaluación de la ciberseguridad y para brindar sistemáticamente apoyo, dar advertencias y coordinar respuestas ante los riesgos de ciberseguridad que se identifiquen.

Utilización de la información
Art. 68. La información obtenida por los departamentos de ciberseguridad e informatización que desempeñan funciones de protección de la ciberseguridad solo puede utilizarse para este fin.

Seguridad de las operaciones para la infraestructura de información crítica
Art. 69. La Secretaría de Innovación debe implementar medidas para proteger las operaciones de las infraestructuras críticas, como control de tráfico aéreo, marítimo y terrestre, y redes suministro de agua y electricidad, así como finanzas, redes de comunicaciones y gobierno electrónico con un concepto de protección multinivel de ciberseguridad para enfrentar situaciones que interrumpan la función central que desarrollan o cuando experimenten una fuga de datos, para evitar poner en peligro la seguridad nacional, el bienestar del país o el interés público.

Evaluación anual
Art. 70. Los operadores de infraestructura de información crítica deberán, al menos una vez cada año, realizar un análisis de situación que incluya una evaluación de la seguridad de sus redes y los riesgos que pueda haber, el método utilizado, las medidas de mejora que se proponen o que se modifican, y las medidas que se tienen para garantizar una efectiva protección de la seguridad de la infraestructura de información crítica.

Obligación de informar metodología
Art. 71. Para garantizar la protección de la seguridad de la infraestructura de información crítica, la Secretaría de Innovación solicitará a los operadores informar metodología y tiempos para:

1. Identificar los posibles riesgos de seguridad que pueden afectar a la infraestructura de información crítica.
2. Implementar medidas de mejora y demostrar capacidades para realizar pruebas y evaluaciones de los riesgos de ciberseguridad.
3. Realizar simulacros de respuesta de emergencia en ciberseguridad para garantizar un trabajo coordinado y la capacidad de respuesta efectiva a incidentes de ciberseguridad.
4. Promover el intercambio de información sobre ciberseguridad entre los operadores de infraestructuras de información crítica y de instituciones de investigación y organizaciones de servicios de ciberseguridad.

5. Proporcionar soporte técnico y asistencia para la gestión y recuperación de emergencias de ciberseguridad.

Seguridad de la información de la red
Art. 72. Los operadores de redes mantendrán estrictamente la confidencialidad de la información de los usuarios que recopilen y usarán sistemas de protección de la información de los usuarios.

Aplicación supletoria
Art. 73. Los operadores de redes que recopilen y utilicen información personal deberán cumplir con todos los requisitos establecidos en esta Ley u otras leyes relacionadas aspectos tecnológicos, y de protección de la información confidencial y de IA y tener el consentimiento de los titulares cuyos datos se recopilen.

Prohibición de destrucción de información
Art. 74. Los operadores de redes no deben divulgar, alterar ni destruir la información personal que recopilan. Cuando no tengan el consentimiento del titular cuya información fue recopilada, no deben proporcionarla a otros operadores. Esto último no aplica cuando después de procesar la información no se puede identificar a la persona y no se puede recuperar su identidad.

Sanción a violación a la intimidad
Art. 75. Cuando un titular descubra que el operador de red ha violado disposiciones establecidas en esta Ley y otras leyes relacionadas aspectos tecnológicos, y de protección de la información confidencial y de IA o acuerdos entre las partes para recopilar o utilizar su información personal, tiene derecho a exigir al operador que elimine su información personal. Además, cuando un titular descubra que la información personal recopilada o almacenada por el operador de red tiene errores, puede exigir que el operador haga de inmediato la corrección.

Prohibición de obtención de información ilegal
Art. 76. Los operadores de redes no deben utilizar métodos ilegales para adquirir información personal, ni vender ni proporcionar ilegalmente información personal a terceros. Además, deberán proteger la información personal y los datos comerciales confidenciales que conozcan en el desempeño de sus funciones, y no podrán filtrarla, venderla o proporcionarla ilegalmente a terceros.

Suspensión de publicaciones ilícitas
Art. 77. Cuando los operadores de red descubran que una publicación o transmisión está prohibida por esta Ley, suspenderán de inmediato la transmisión de esa información, procederán a eliminarla y evitarán que se difunda, aunque deben guardar los registros de esa información.

Implementación del Sistema de Quejas
Art. 78. Los operadores de redes deberán establecer sistemas que tengan una clara y simple metodología para presentar quejas y la forma cómo se procesarán y tiempos para dar respuesta.

Monitoreo, alerta temprana y respuesta a Emergencias
Art. 79. La Secretaría de Innovación creará un sistema de monitoreo, alerta temprana y respuestas a ataques e incidentes que pongan en riesgo los sistemas de ciberseguridad. El objetivo de este sistema es potenciar sistemáticamente los esfuerzos de recopilación, análisis y presentación de informes de ciberseguridad.

Planes de respuesta a incidentes de ciberseguridad
Art. 80. Los planes de respuesta a ataques e incidentes de ciberseguridad se clasificarán considerando factores como la magnitud del daño que se ha causado y su alcance, así como la calidad técnica y operacional de las medidas para dar respuesta a cualquier situación de emergencia.

Ataques cibernéticos
Art. 81. Cuando ocurra un ataque o incidente al sistema de ciberseguridad, los operadores de red deberán activar de inmediato el plan de respuesta de emergencia, para eliminar el daño, prevenir su expansión y minimizar sus efectos. Además, deberán hacer una evaluación y valoración exhaustiva del incidente ocurrido, identificando los peligros ocultos y de los posibles nuevos riesgos de seguridad y publicarán las advertencias relevantes de manera pública en sus sitios web.

Sanciones por causar daños a la ciberseguridad
Art. 82. Cuando los operadores de red o los proveedores de productos o servicios de red no cumplan las funciones de protección de la ciberseguridad previstas en esta Ley, no realicen las correcciones o causen daños a la ciberseguridad, a la persona natural responsable se le impondrá una multa equivalente a diez (10) salarios mínimos del Sector de Comercio y Servicios.

Para personas jurídicas la multa será de veinte (20) salarios mínimos del Sector de Comercio y Servicios. En caso de reincidencia calificada por la Secretaría de Innovación como falta grave, la multa será de hasta el uno por ciento (1 %) de sus ingresos anuales del último año fiscal, antes de impuestos.

Sanción por no exigir identidad real
Art. 83. Los operadores de red o los proveedores de productos o servicios de red que no exijan a los usuarios que proporcionen información de identidad real y verificable, o que continúen proporcionando servicios relevantes a los usuarios que no proporcionen información de identidad real y verificables, y no realicen los ajustes correspondientes se les impondrá una multa de veinte (20) salarios mínimos del Sector de Comercio y Servicios. En caso de reincidencia calificada por la Secretaría de Innovación como falta grave, la multa será de hasta el uno por ciento (1 %) de sus ingresos anuales del último año fiscal, antes de impuestos.

Nota de Advertencia
Art. 84.- Si los operadores de red o los proveedores de productos o servicios de red no cumplen con los requisitos establecidos en esta Ley para realizar evaluaciones de riesgos de ciberseguridad y publicar información relacionada con la ciberseguridad, la Secretaría de Innovación les enviará una nota de advertencia al operador de red, para que tome las medidas correctivas necesarias para corregir y el plazo para ejecutarlas.

En caso de que el operador de red o el proveedor de productos o servicios de red no cumpla con lo indicado en la nota de advertencia, se le impondrá una multa de veinte (20) salarios mínimos del Sector de Comercio y Servicios. Además, dependiendo de la gravedad del incumplimiento, la Secretaría de Innovación podrá imponer una multa de hasta el uno por ciento (1 %) de sus ingresos anuales del último año fiscal, antes de impuestos, suspender sus operaciones hasta que se realicen las correcciones, el cierre de sus sitios web, la revocación de permisos de operación, o la cancelación de sus licencias comerciales

Aviso y Sanciones
Art. 85.- Cuando en el desarrollo de su trabajo un operador de red o un proveedor de productos o servicios de red participe en actividades que dañen la ciberseguridad, o si proporciona un software o herramientas que se utilizan en actividades que dañan o ponen en riesgo la ciberseguridad, o proporciona soporte técnico a otro operador de red que realice este tipo de actividades, la Secretaría de Innovación podrá imponerle una multa de veinte (20) salarios mínimos del Sector de Comercio y Servicios. Además, dependiendo de la gravedad del incumplimiento, la Secretaría de Innovación podrá imponer una multa de hasta el uno por ciento (1 %) de sus ingresos anuales del último año fiscal, antes de impuestos, suspender sus operaciones, cerrar sus sitios web, la revocación de permisos de operación, o la cancelación de sus licencias comerciales.

A través del Instituto del Proceso de Extinción de Dominio y de la Administración de los Bienes de Origen o Destinación Ilícita, se confiscará las ganancias obtenidas ilícitamente y se dará aviso a la Fiscalía General de la República, que inicie la investigación y los trámites judiciales correspondientes para la detención de los responsables.

Consecuencias por infracciones muy graves
Art. 86. Los operadores de red y los proveedores de productos o servicios de red que hayan recibido sanciones por infracciones muy graves, como las establecidas en la sección segunda del Título VI, no podrán desempeñar cargos de gestión en materia de ciberseguridad ni en operaciones clave de redes durante cinco (5) años. Los operadores de red que hayan recibido sanciones penales no podrán trabajar en puestos clave de gestión de seguridad cibernética y en operaciones de red de por vida.

Remisión
Art. 87.- Cuando los operadores de red y los proveedores de productos o servicios de red almacenen o procesen cualquier tipo de información relacionada con la seguridad nacional o calificada como secreto nacional sin aplicar los métodos y normas establecidos en esta Ley o sin la autorización oficial del Estado, la secretaría de Innovación remitirá al Ministerio de la Defensa Nacional toda la información relacionada con el incidente para que proceda de acuerdo a las leyes que aplican en el ámbito de la Defensa Nacional.

CAPÍTULO III
CONTRALORÍA SOCIAL

De la autoridad competente
Art. 88. Para lograr la transformación digital de El Salvador, la Secretaría de Innovación ejecutará la Agenda Digital El Salvador 2020-2030, para convertir al Estado en un facilitador que fomente la adopción, impulse y difunda nuevas formas y herramientas de innovación. entre los diversos actores de la sociedad.

En este contexto, la Secretaría de Innovación deberá supervisar el cumplimiento de lo establecido en esta Ley y en aquellas que tengan relación con cualquier caso relacionado con el uso de sistemas de IA. Además, deberá:

1. Promover y preparar estudios, investigaciones y análisis sobre buenas prácticas, códigos de conducta, gobernanza y ética aplicables a todo el proceso de desarrollo y uso de estos sistemas de IA.
2. Promover acciones de cooperación con autoridades nacionales, internacionales y transnacionales, así como acuerdos para proteger y fomentar el desarrollo y uso de sistemas de IA. Estas acciones se harán en consulta o en coordinación con el Ministerio de Relaciones Exteriores de El Salvador.
3. Preparar el reglamento de esta Ley, el cual debe incluir:
    a. Los procedimientos asociados para garantizar el pleno cumplimiento los derechos previstos en esta Ley.
    b. Los procedimientos, métodos y requisitos básicos para investigar y preparar las evaluaciones de impacto algorítmico.
    c. Definir la forma y requisitos de la información a publicar sobre el uso de sistemas de IA.
4. Supervisar los servicios de recomendación algorítmica para garantizar el pleno cumplimiento de esta Ley y otras leyes pertinentes de El Salvador, así como de todos los principios establecidos en el Art. 5.
5. Coordinar con las autoridades públicas encargadas de supervisar y regular los sectores económicos e instancias gubernamentales que hacen uso de tecnologías de última generación, especialmente de IA.

6. Establecer un sistema para monitorear, ya sea de manera independiente o en colaboración con otras autoridades públicas, el desarrollo y uso de sistemas de IA, así como la divulgación de información personal o de grupos de personas, con el fin de prevenir violaciones de sus derechos.
7. Establecer un sistema para enfrentar casos de incumplimiento de esta Ley, incluyendo los procesos administrativos para garantizar el principio de contradicción o derecho a confrontar las pruebas que se presenten en contra, la defensa amplia y el derecho de apelación.
8. Establecer un sistema para atender cualquier petición verificada contra un operador de un sistema de IA, que no haya respondido dentro del plazo establecido en esta Ley.

TÍTULO VI
INFRACCIONES Y SANCIONES

CAPÍTULO I
INFRACCIONES

Tipos de infracciones
Art. 102. Las infracciones establecidas en esta Ley de Inteligencia Artificial se clasifican en tres tipos de infracciones: leves, graves y muy graves. Esta clasificación se fundamenta en las prácticas de IA y en los riesgos que puedan representar para los usuarios, ya sea individualmente o como grupo, en cuanto a la seguridad y protección de los derechos fundamentales establecidos en la Constitución de El Salvador, sus leyes y en esta Ley.

Infracciones leves
Art. 103. Son infracciones leves:

A. El incumplimiento de deberes y obligaciones establecidas en esta Ley que no estén tipificadas como infracciones graves o muy graves.
B. El incumplimiento del mandato de mantener registros actualizados del sistema de IA.
C. El incumplimiento de las condiciones esenciales establecidas al otorgar o renovar la licencia para utilizar tecnologías innovadoras, incluyendo IA.
D. No atender o responder adecuadamente, o retrasar sin justificación un requerimiento de información solicitado por la Secretaría de Innovación de acuerdo con lo dispuesto en esta Ley.

E. El incumplimiento del mandato de mantener registros actualizados del sistema de IA. En caso que esto se reitere por segunda vez se considerará infracción grave; y en una tercera o más ocasiones constituirá infracción muy grave y le aplicarán las sanciones establecidas para cada una de estas dos últimas categorías.

Infracciones graves
Art. 104. Son infracciones graves:

A. El incumplimiento de las normas establecidas en esta Ley y su Reglamento, así como las instrucciones y decisiones que adopte la Secretaría de Innovación por parte de los agentes de IA.
B. Violar los derechos, garantías y principios establecidos en la Constitución de El Salvador, en esta Ley y los establecidos por la Defensoría del Consumidor y acciones y medidas que hayan causado un daño irreparable a los titulares.
C. Violar el derecho de toda persona a recibir información gratuita, clara y precisa, como lo establece esta Ley, especialmente al emitir contenidos perjudiciales dirigidos a usuarios pertenecientes a grupos vulnerables como niños, adolescentes, personas mayores y personas con discapacidad. En caso de reincidencia, por segunda vez o más veces, se clasificará como una infracción muy grave, aplicándose las sanciones correspondientes a esta categoría.
D. Que un agente o grupo de agentes de inteligencia artificial, en el desarrollo y aplicación de su trabajo:

1. Entorpezcan el desarrollo económico, social, político, jurídico y ambiental del país o limiten o entorpezcan el progreso nacional o afecten adversamente la calidad de vida de sus habitantes.
2. Impidan o limiten el libre acceso y la competencia en el mercado de IA con el objetivo o intención de establecer cualquier tipo de monopolio, oligopolio o acuerdo anticompetitivo.
3. No mantener una base de datos de IA de alto riesgo de acceso público que permitan evaluar el impacto de su uso y se haya irrespetado la confidencialidad de los secretos comerciales e industriales.
4. No contar con protocolos de gobernanza y ética o no aplicarlos debidamente en los procesos internos para de garantizar la seguridad de los sistemas y el cumplimiento de todos los derechos de las personas según esta Ley y las leyes relacionadas.

5. Incumplan el mandato de formar, capacitar, crear competencias o actualizar conocimientos en los profesionales que trabajan en la organización y utilizar los avances innovadores y disruptivos en IA.
6. No cumplan los fundamentos conceptuales para el desarrollo, ejecución y uso de sistemas de IA establecidos en el Art. 4 de esta Ley.
7. No crear, actualizar o fortalecer la infraestructura digital como medio para potenciar el desarrollo y actualización de la IA.
8. No contar con una infraestructura de datos que proporcione información pública de alta calidad, confiable, reutilizable y accesible a los usuarios.
9. No haber establecido ni estar aplicando lineamientos éticos que garanticen un uso sostenible, transparente y replicable de la IA.
10. No tener condiciones para el correcto uso de algoritmos de recomendación que sirvan para garantizar a los usuarios inclusión, privacidad y transparencia en el funcionamiento del algoritmo, ni contar con los medios para que los usuarios controlen y comprendan cómo se utilizan sus datos para generar recomendaciones utilizando la IA.
11. No dar a conocer los incidentes graves o defectos de funcionamiento ni aplicar las sanciones según lo estipulado en esta Ley y otras leyes de El Salvador.
12. Incumplir los procedimientos requeridos por la Secretaría de Invasión para solicitar y autorizar el funcionamiento de los *sandboxes* regulatorios, así como limitar o interrumpir su funcionamiento y no presentar recomendaciones para la preservación de los derechos fundamentales de los usuarios, la protección de sus datos personales y su seguridad.
13. Extraer y utilizar información automatizada de obras, textos y datos para reproducirlos, almacenarlos y transformarlos mediante sistemas de IA, sin autorización constituyendo un delito contra los derechos de autor, salvo en los casos excluidos en esta Ley.

Infracciones muy graves

Art. 105. La acumulación de cuatro infracciones graves en un mismo año calendario constituirán una infracción muy grave.

CAPÍTULO II
SANCIONES
SECCIÓN PRIMERA
DISPOSICIONES SANCIONATORIAS

Sanciones
Art. 106. Por infracciones cometidas contra lo establecido en esta Ley, los agentes de IA están sujetos a las siguientes sanciones administrativas aplicables por la Secretaría de Innovación:

1. Advertencia: en casos de infracciones leves y no reincidentes, se enviará una nota de advertencia sobre las posibles consecuencias si no se corrige según las instrucciones enviadas.
2. Multa simple: En el caso de una persona jurídica, la infracción conlleva una multa equivalente a veintiocho (28) salarios mínimos del Sector de Comercio y Servicios. Para grupos o conglomerados de El Salvador o residentes en el país, la multa será de hasta el dos por ciento (2 %) de sus ingresos anuales del último año fiscal, antes de impuestos.
3. Multa simple: en el caso de una persona jurídica, la infracción conlleva una multa equivalente a veintiocho (28) salarios mínimos del Sector de Comercio y Servicios.
4. Hacer pública la infracción después de que su ocurrencia haya sido debidamente investigada y confirmada.
5. Prohibición o restricción de participar en el régimen de sandbox regulatorio establecido en esta Ley, hasta por cinco años.
6. Suspensión parcial o total, temporal o definitiva, del desarrollo, suministro u operación del sistema de IA.
7. Prohibición de procesar las bases de datos que se señalen.

Las sanciones se aplicarán después del procedimiento administrativo, en el cual el infractor tendrá la oportunidad de presentar una defensa de acuerdo con las características del caso.
8.
Prohibición de Publicación de Archivos
Art. 107. Queda estrictamente prohibida la publicación de archivos privados con información financiera que hagan uso de monedas digitales o criptoactivos en cualquier medio, ya sea electrónico o físico. Asimismo, se prohíbe el uso o venta de códigos de acceso u otra información sensible sin la autorización expresa de cada uno de los usuarios propietarios de dicha información.

Esta falta de autorización constituye una violación muy grave. En el caso de personas naturales, la sanción será de cincuenta (50) salarios mínimos del Sector de Comercio y Servicios. Para las personas jurídicas, la multa podrá alcanzar hasta un tres por ciento (3 %) de sus ingresos anuales del último año fiscal, antes de impuestos."

Advertencia
Art. 108. Cuando los proveedores de servicios de recomendación algorítmica violen las disposiciones establecidas en esta Ley y otras leyes pertinentes de manera leve y no reincidente, la Secretaría de Innovación enviará una nota de advertencia sobre las posibles consecuencias si no se corrige según las instrucciones enviadas y ordenarán una rectificación que se deberá cumplir en un plazo máximo de 30 días calendario.

Si las instrucciones de correcciones no son cumplidas dentro del plazo señalado, al igual que los casos de infracciones graves, la Secretaría de Innovación ordenará a los proveedores la suspensión del servicio de recomendación algorítmica hasta que cumplan satisfactoriamente las rectificaciones señaladas. Además, podrá imponer una multa entre catorce (14) y veintiocho (28) salarios mínimos del Sector de Comercio y Servicios.

Cooperación Interinstitucional
Art. 109. En el caso que la Secretaría de Innovación descubra que se ha creado y existe cualquier tipo de monopolio, oligopolio o acuerdo anticompetitivo, coordinará con la Superintendencia de Competencia, para aplicar las sanciones que corresponden por prácticas anticompetitivas e infracciones a la Ley de Competencia.

El agente económico que haya recibido una sanción puede interponer recurso de revisión. Una vez que la resolución se mantiene firme, si corresponde una sanción pecuniaria, debe pagarla en la Dirección General de Tesorería del Ministerio de Hacienda dentro del plazo establecido por la Ley, y luego presentar el comprobante de su cancelación a la secretaria de Innovación y a la Superintendencia de Competencia en el término de tres días.

En el caso de que el agente económico no realice el pago, se remitirá la información pertinente a la Fiscalía General de la República, para que inicie las acciones correspondientes, para que los pagos se hagan efectivos por la vía de ejecución.

Ejecución de la Ley
Art. 110. La Secretaría de Innovación definirá en el Reglamento de esta Ley el procedimiento de investigación y los criterios para la aplicación de las sanciones administrativas y de las leyes pertinentes que se puedan aplicar en el proceso en el proceso en curso.

SECCIÓN SEGUNDA
CLASIFICACIÓN DE LAS SANCIONES

Sanciones por Infracciones Leves
Art. 111. En el caso de infracciones leves, la Secretaría de Innovación podrá enviar una advertencia sobre la infracción cometida y demandar una corrección en el plazo que considere adecuado. Además, podrá imponer una sanción pecuniaria a micro o medianas empresas, así como a personas naturales, entre tres (3) y diez (10) salarios mínimos del Sector de Comercio y Servicios. Esta sanción se deberá pagar en la Dirección General de Tesorería del Ministerio de Hacienda.

Para las grandes empresas, la sanción pecuniaria será de veinte (20) salarios mínimos del Sector de Comercio y Servicios, también a ser pagada en la Dirección General de Tesorería del Ministerio de Hacienda.

Art. 107. En caso de infracciones leves, la Secretaría de Innovación podrá enviar una advertencia y exigir una corrección en el plazo adecuado. Asimismo, podrá imponer una sanción pecuniaria a micro o medianas empresas, así como a personas naturales, entre tres (3) y diez (10) salarios mínimos del Sector de Comercio y Servicios. Esta sanción se deberá pagar en la Dirección General de Tesorería del Ministerio de Hacienda.

En el caso de grandes empresas, la multa será de veinte (20) salarios mínimos del Sector de Comercio y Servicios, que también se deberá pagar en la Dirección General de Tesorería del Ministerio de Hacienda.

Sanciones por Infracciones graves
Art. 112. En el caso de infracciones graves, la Secretaría de Innovación aplicará una sanción pecuniaria a micro o medianas empresas, así como a personas naturales, entre once (11) y veinte (20) salarios mínimos del Sector de Comercio y Servicios. Esta sanción se deberá pagar en la Dirección General de Tesorería del Ministerio de Hacienda.

Para las grandes empresas, la multa será de veinticinco (25) salarios mínimos del Sector de Comercio y Servicios, que también se deberá pagar en la Dirección General de Tesorería del Ministerio de Hacienda.

Sanciones por Infracciones muy graves
Art. 113. En el caso de infracciones muy graves, la Secretaría de Innovación aplicará una sanción pecuniaria a micro o medianas empresas, así como a personas naturales, entre veinticinco (25) y treinta y cinco (35) salarios mínimos del Sector de Comercio y Servicios. Esta sanción se deberá pagar en la Dirección General de Tesorería del Ministerio de Hacienda.

Para las grandes empresas, la Secretaría de Innovación podrá aplicar una sanción pecuniaria entre cincuenta (50) y sesenta (60) salarios mínimos del Sector de Comercio y Servicios, que también se deberá pagar en la Dirección General de Tesorería del Ministerio de Hacienda.

En caso de reincidencia, la Secretaría de Innovación podrá aplicar una sanción de hasta ochenta (80) salarios mínimos del Sector de Comercio y Servicios, o un cuatro por ciento (4.0%) de su última facturación anual antes de impuestos.

Otras Sanciones
Art. 114.- Los profesionales, funcionarios o empleados públicos que cometan infracciones graves o muy graves a la presente ley, serán inhabilitados para el ejercicio de su profesión o función, y podrán ser despedidos o destituidos, según la gravedad de la infracción.

Asimismo, se aplicarán las demás sanciones previstas en la presente ley u otras leyes relacionadas.

TÍTULO VII
DISPOSICIONES FINALES

Aplicación Supletoria
Art. 115.- Los derechos y principios expresados en esta Ley no excluyen la aplicación de otras leyes o de tratados internacionales que El Salvador haya firmado.

Vigencia
Art. 116.- La presente ley entrará en vigor ciento ochenta días después de su publicación.

DADO EN EL SALÓN AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los N días del mes de HHHHHH del año dos mil XXXX.

VI. Propuesta de Ley de protección de datos para El Salvador

En una revisión de la legislación de El Salvador que realizó Alfredo Chirino, en 2015, destacó que no había una definición de protección de datos personales, ni siquiera en la Ley de Acceso a la Información Pública. Sin embargo, señaló que había una aproximación de lo que podría ser una definición cuando se refiere a «que se trataría de un derecho de la persona, directamente o a través de su representante... (cuando) se están procesando sus datos personales; a conseguir una reproducción inteligible de ellos sin demora; a obtener las rectificaciones o supresiones que correspondan cuando los registros sean injustificados o inexactos y a conocer los destinatarios cuando esta información sea transmitida, permitiéndole conocer las razones que motivaron su petición» (p. 45).

Para sustentar este argumento, Chirino citó el Art. 31 de la referida Ley, que dice:

> Art. 31.- Toda persona, directamente o a través de su representante, tendrá derecho a saber si se están procesando sus datos personales; a conseguir una reproducción inteligible de ella sin demora; a obtener las rectificaciones o supresiones que correspondan cuando los registros sean injustificados o inexactos y a conocer los destinatarios cuando esta información sea transmitida, permitiéndole conocer las razones que motivaron su petición, en los términos de esta ley. El acceso a los datos personales es exclusivo de su titular o su representante.

Además, Chirino resaltó que esta Ley «tomó en consideración la importancia de que las personas tengan a su alcance mecanismos para conocer la información que de ellas obra en los archivos de cualquier ente público», lo cual le permite al titular «ejercer los derechos de acceso, rectificación, oposición y eliminación de sus datos personales» (p. 46).

Sin embargo, el concepto jurídico de protección de datos o autodeterminación informativa se reconoció como derecho fundamental de los salvadoreños mediante una sentencia de la Corte Suprema de Justicia, del 4 de marzo de 2011; después de un proceso de amparo constitucio-nal que la Asociación Salvadoreña para la Protección de Datos e Internet (INDATA), presentara una demanda contra la empresa Equifax Centroamérica— en ese momento conocida como DICOM— por haber recopilado y comercializado cuatro millones de datos personales de salvadoreños sin su conocimiento ni consentimiento (Legal Corp., Amparo 934-2007). De esta manera, la Corte Suprema de Justicia, a través de la Sala de lo Constitucional, estableció el derecho de acceso a la información personal o a la autodeterminación informativa, Habeas Data,

acción legal que puede iniciar toda persona natural o jurídica para ejercer su derecho a solicitar y obtener la información existente sobre su persona, y solicitar su eliminación o corrección si fuera parcial, inexacta, incompleta, fraccionada, falsa o estuviera desactualizada.

En su sentencia, los magistrados definieron el derecho a la autodeterminación informativa como «la necesidad de las personas de preservar su identidad ante la revelación y el uso de los datos que les conciernen y (la protección) frente a la ilimitada capacidad de archivarlos, relacionarlos y transmitirlos» (La Prensa Gráfica, 2014. párr. 1). Además, le ordenaron a la empresa demandada «abstenerse de utilizar, transferir y comercializar, a cualquier título y destino, la información de las personas que conste en su base de datos, a menos que en cada caso individual cuente con el consentimiento expreso de sus titulares» (Ibidem, párr. 2).

No obstante, dado los avances en tecnología, en general, y de la IA, en particular, es necesario incluir el impacto que ellos tendrán en el manejo y uso de los datos personales, así como la posible vulneración de los derechos de las personas y/o grupos de personas, para evitar su uso indebido y daños.

ANTEPROYECTO DE LEY DE PROTECCIÓN DE DATOS

DECRETO No NN
LA ASAMBLEA LEGISLATIVA DE LA REPÚBLICA DE EL SALVADOR
CONSIDERANDO:

I. Que el Artículo 1 de la Constitución "reconoce a la persona humana como el origen y el fin de la actividad del Estado, que está organizado para la consecución de la justicia, de la seguridad jurídica" para todos sus habitantes.

II. Que el Artículo 2 de la Constitución señala que el Estado debe garantizar "el derecho al honor, a la intimidad personal y familiar y a la propia imagen", todo lo cual puede estar en riesgo con el uso indebido o manipulaciones de los datos personales y el mal uso de las herramientas de Inteligencia Artificial.

III. Que las tecnologías de la información y las comunicaciones, en general, y de la Inteligencia Artificial, en particular, se han convertido en herramientas de uso diario por gran parte de la población, empresas, organizaciones sin fines de lucro e instituciones del Estado, creando condiciones que pueden potenciar el progreso socioeconómico de El Salvador.

IV. Que las mejores prácticas deben incluir programas de capacitación continua para distintos niveles de usuarios; capacitar sobre políticas y prácticas de gestión de riesgo aplicadas a la IA generativas de texto; el papel de las personas en la validación y verificación de los textos generados por IA; establecer equipos multidisciplinarios de consulta para que puedan abordar el estudio de casos de uso complejos, así como tener técnicas e información para que los usuarios conozcan los mecanismos de anonimización o disociación de datos para garantizar la protección de la información de la organización y terceros.

V. Que el uso de inteligencia artificial también conlleva serios riesgos y amenazas a personas naturales y jurídicas por el mal uso de la información y la falta de ética en su desarrollo y aplicación, por lo que es necesario contar con una ley y reglamentos efectivos para supervisar y garantizar la protección de la privacidad y la seguridad de los datos personales.

VI. Que ante los riesgos y amenazas de la IA es necesario fortalecer la gobernanza digital, lo cual se requiere contar con una Ley de Protección de Datos, basada en soluciones técnicas de aplicación y aceptación universal, donde la ética y las buenas prácticas constituyan sus fundamentos.

VII. Que en la medida que la IA utiliza o se nutre de grandes cantidades de datos personales es fundamental tener una ley que garantice que esta información se recopile y utilice cumpliendo los principios de ética y pleno cumplimiento con las leyes. Esto implica garantizar a los titulares su consentimiento para compartir sus datos, y que se protejan adecuadamente contra posibles violaciones o ataques.

VIII. Que en la medida que evoluciona la IA y se ponen a disposición del público nuevas e innovadoras tecnologías, que ejecutarán decisiones automatizadas de mayor profundidad, es relevante asegurar que estas decisiones no se basen en prejuicios o causen perjuicios o discriminen a ciertos a una o a un grupo de personas.

IX. Que hay continuos desarrollos tecnológicos innovadores y disruptivos que pueden afectar la protección de los datos personales, este tipo de legislación debe ser revisada y actualizada tan pronto como surge una tecnología innovadora que muestre la necesidad de ajustar esta Ley.

IX. Que hay continuos desarrollos tecnológicos innovadores y disruptivos que pueden afectar la protección de los datos personales, este tipo de legislación debe ser revisada y actualizada tan pronto como surge una tecnología innovadora que muestre la necesidad de ajustar esta Ley.

X. Que esta Ley debe tener estrechos vínculos con la Ley de Inteligencia Artificial como instrumentos legales destinados a proteger los datos personales de los titulares para evitar daños de todo tipo a sus titulares.

POR TANTO: en uso de sus facultades constitucionales y a iniciativa del Presidente de la República, por medio del Ministro de Economía,

DECRETA, la siguiente:

LEY DE PROTECCIÓN DE DATOS
TÍTULO I
DISPOSICIONES GENERALES

CAPÍTULO I
OBJETO Y CAMPO DE APLICACIÓN

Objeto
Art. 1. La presente Ley tiene por objeto garantizar el derecho al honor, a la intimidad personal y familiar, y a la propia imagen mediante el buen uso y ético tratamiento de los datos personales, para que estos sean confiables, veraces y actualizados. Además, tiene como objeto la protección integral de los datos personales, cuando se encuentren en posesión de particulares o de personas jurídicas o entidades públicas y privadas, o cualquier otro tipo de entidad sin personalidad jurídica, con la finalidad de regular su tratamiento legítimo, seguro, transparente e informado, garantizar la privacidad y el derecho a la autodeterminación informativa de las personas naturales y establecer las normas relativas a la libre circulación de tales datos.

Campo de Aplicación
Art. 2. Esta Ley aplicará a los datos personales almacenados en bases de datos, ya sea en físico como en formatos total o parcialmente automatizados, que surta efectos en el territorio nacional.

Se regirá por esta Ley todo tratamiento de datos de personas naturales que sea efectuado en El Salvador, con excepción de:

1. El tratamiento de datos de historial crediticio que realicen los sujetos obligados en según la Ley de Regulación de los Servicios de Información sobre el Historial de Créditos de las Personas.
2. El tratamiento realizado por personas naturales que recopilen y almacenen datos personales exclusivamente para uso interno, personal o doméstico, sin fines de divulgación, uso comercial o venta.
3. El tratamiento de la información obtenida mediante un proceso previo de disociación o anonimización, de manera que el resultado no pueda asociarse al titular.
4. Los tratamientos relacionados con la seguridad pública, la Defensa Nacional, la seguridad del Estado y sus actividades en materia penal, investigación y represión del delito.
5. Los tratamientos de datos realizados en el ejercicio de la libertad de prensa y de expresión.

Comité Técnico Ejecutivo
Art. 3. La Secretaría de Innovación de la Presidencia de la República, en adelante Secretaría de Innovación, la Defensoría del Consumidor, el Instituto de Acceso a la Información Pública y toda institución del Estado que recolecte, transforme y utilice datos personales deberán coordinar sus actividades para garantizar el cumplimiento de lo estipulado en esta Ley y de sus respectivas leyes. Para cumplir este mandato, crearán un Comité Técnico-Ejecutivo que se deberá reunir al menos trimestralmente y producir informes sobre los resultados y acciones tomadas para garantizar la protección, así como el buen y ético uso de los datos personales.

Coordinación de la Información Interinstitucional
Art. 4. La Secretaría de Innovación normará los procesos para la captación para evitar la recopilación excesiva de datos personales, que quitan tiempo a los titulares, recargan los sistemas y pueden causar inconsistencias, se aplicará la Ley de Procedimientos Administrativos para prevenir trámites burocráticos.

Definiciones
Art. 5. Para la aplicación de esta Ley, se utilizarán las siguientes definiciones:

1. Archivo, registro o base de datos: es el conjunto organizado de datos personales sujetos a tratamiento o procesamiento, independientemente de su forma, electrónica o no, sin distinguir la modalidad de su formación, almacenamiento, organización o acceso.
2. Autodeterminación informativa: es la facultad que tiene toda persona para ejercer los derechos y utilizar los mecanismos establecidos en esta Ley sobre la información personal que le atañe, contenida en registros públicos o privados, especialmente los almacenados mediante medios digitales e informáticos.
3. Ciberseguridad: abarca todas las actividades necesarias para proteger las redes y sistemas de información de los usuarios contra ciberamenazas y ciberataques, evitando que estos eventos los afecten.
4. Consentimiento: es la manifestación de la voluntad del titular de los datos mediante la cual se efectúa el tratamiento de los datos cuando no exista otro fundamento legal para su tratamiento.
5. Datos biométricos: son los datos personales obtenidos a partir de un tratamiento técnico específico, que precisa las características físicas, fisiológicas o conductuales de una persona natural, que pueden utilizarse para identificarla o confirmar su identificación única en formato digital, como son imágenes faciales o datos dactiloscópicos.
6. Datos personales: es la información privada de una persona identificada o identificable, relativa a su nacionalidad, domicilio, patrimonio, dirección electrónica, número telefónico y otra análoga.
7. Datos sensibles: son aquellos datos personales que afectan a la esfera más íntima de su titular y cuya utilización indebida pueda causar discriminación, afectar el derecho al honor, a la intimidad personal y familiar, así como a su propia imagen. Estos datos suelen revelar aspectos como el credo, religión, origen étnico, afiliación o ideologías políticas, membresía sindical, preferencias sexuales, estado de salud física y mental, información biométrica, genética, situación moral y familiar, y cualquier otra información de naturaleza íntima similar.
8. Discriminación: es toda acción o señalamiento que resulte en un trato desfavorable o injusto hacia una persona o grupo, que vulnere su dignidad, derechos humanos y libertades debido a características especiales como origen geográfico, raza, color o

etnia, género, nivel de ingresos, condiciones socioeconómicas, edad, discapacidad, religión o política, que potencialmente puedan causar una exclusión, restricción o rechazo, restringir o alterar su reconocimiento, el goce o ejercicio de igualdad o de cualquier derecho previsto en el sistema jurídico de El Salvador.

9. Disociación o anonimización: es un procedimiento irreversible de gestión de datos mediante el cual se reemplaza la información personal de un individuo por identificadores artificiales para que dichos datos no puedan ser utilizados para identificar a ninguna persona.
10. Encargado del tratamiento: es la persona natural o jurídica, pública o privada que, ya sea sola o en conjunto con otros, trata datos personales por cuenta del responsable.
11. Habeas Data: es la acción legal que puede iniciar toda persona natural o jurídica para ejercer su derecho a solicitar y obtener la información existente sobre su persona, y solicitar su eliminación o corrección si fuera parcial, inexacta, incompleta, fraccionada, falsa o estuviera desactualizada.
12. Incidente: es cualquier evento que tenga efectos adversos en la seguridad de las redes y sistemas de información.
13. Intimidad informática: es el derecho que tiene un titular de tener control sobre sus datos personales desde la autorización del uso de su información en medios digitales y a través de todos los procesos: acceso, uso, actualización, rectificación y cancelación.
14. Proveedor: es toda persona natural o jurídica que inicie procesos o se dedique a comercializar o distribuir un sistema de IA.
15. Responsable del tratamiento: de los datos es la persona natural o jurídica, pública o privada, propietaria de la base de datos o que decide sobre la finalidad y medios del tratamiento.
16. Seudonimización: es el proceso de cambiar la denominación de los datos personales por seudónimos, de modo que no puedan asociarse directamente con el titular sin información adicional. Sin embargo, aunque se oculta la identidad de la persona, no se elimina el vínculo entre los datos y esta, por lo que es un procedimiento reversible que permite volver a identificar al titular.
17. Suplantación de identidad o *phishing:* es un proceso que se utiliza para engañar y así robar información personal confidencial de los usuarios que reciben las solicitudes. Normalmente, para engañar utilizan correos electrónicos con apariencia de ser legales y con el uso de nombres afines.

18. Titular: es toda persona natural cuyos datos sean objeto del tratamiento al que se refiere la presente Ley.
19. Transferencia de datos personales: es toda entrega total o parcial de datos personales para ser trabajados por un tercero que actuará como encargado del tratamiento o como nuevo responsable. Se excluyen las entregas de datos personales para el almacenamiento de información por terceros o fuera del país por entidades públicas o privadas a cualquier persona distinta al titular de datos, mediante el uso de medios físicos o electrónicos o cualquier otra tecnología que lo permita.
20. Tratamiento de datos: es una operación o conjunto de operaciones que se realizan mediante procedimientos automatizados o manuales de datos personales, como son los procesos de recolección, registro, organización, conservación, modificación, extracción, consulta, uso, comunicación por transmisión, difusión, distribución o cualquier otra forma que facilite el acceso, cotejo, interconexión, bloqueo, supresión o destrucción de ella, entre otros.
21. Usuario: es toda persona natural o jurídica que utilice un sistema de IA.

TÍTULO II
DERECHOS DEBERES Y OBLIGACIONES DE LOS TITULARES EN PROTECCIÓN DE DATOS

CAPÍTULO II
DERECHOS DE LAS PERSONAS

Derecho de uso de TIC

Art. 6. Toda persona tiene el derecho a utilizar sistemas tecnológicos, en general, y de IA, en particular. Cuando el usuario pertenezca a grupos vulnerables como niños, adolescentes, personas mayores y personas con discapacidad, tiene el derecho a recibir información gratuita, clara, precisa y con un lenguaje de fácil comprensión, incluyendo el posible uso de íconos o símbolos de fácil reconocimiento, antes de contratar o utilizar el sistema. Esta información debe abordar los siguientes aspectos:

1. Cómo la naturaleza automatizada de la interacción y la toma de decisiones en los procesos o productos puede afectar a la persona que los utiliza.

2. Descripción general del sistema, los tipos de decisiones, recomendaciones o predicciones que se pretende o pueden hacer y las consecuencias que puede tener su uso para la persona.
3. Identificación de los operadores del sistema de IA, los protocolos de gobernanza y ética que tienen y cómo son utilizados en el proceso de desarrollo y en el uso del sistema por parte de su o sus creadores.
4. Descripción de cómo el sistema de IA trabaja y de todas las personas que estuvieron involucrados en el proceso de toma de decisiones, predicción o recomendación.
5. Categorías de datos personales utilizados en el contexto de la operación del sistema de IA.
6. Presentación y descripción de las medidas de seguridad, de las que evitan discriminación y las de protección y confiabilidad adoptadas, incluyendo exactitud, precisión y cobertura.

Derecho a la Intimidad en la virtualidad

Art. 7. Ante el amplio uso de tecnologías de la información y las comunicaciones, en general, y de la IA, en particular, toda persona natural tiene derecho a su propia intimidad informática, el que le confiere al titular el derecho de tener control sobre sus datos personales.

Derecho de respuesta

Art. 8. La persona afectada por un sistema de IA tiene derecho a solicitar una explicación y recibir una respuesta gratuita del responsable del tratamiento de los datos, en un plazo máximo de cinco (5) días hábiles, sobre las decisiones, predicciones o recomendaciones, incluyendo información sobre los criterios y procedimientos utilizados, así como los principales factores que afectan dicha predicción o decisión específica. Esta información debe incluir:

1. Una explicación sobre la racionalidad y lógica del sistema, su significado y las potenciales consecuencias que puede tener para la persona afectada
2. El grado y nivel de contribución del sistema de IA a la toma de decisiones.
3. Los datos que han sido procesados, su fuente y los criterios para la toma de decisiones y, cuando corresponda, su ponderación, ante la situación del afectado.

4. Información sobre los mecanismos disponibles para impugnar la decisión.
5. La posibilidad de establecer un contacto personal por parte de la persona o personas afectadas.

Derecho de acceso y manejo de Información
Art. 9. Toda persona que sea o haya sido afectada por sistemas de IA tiene los siguientes derechos a la información:

1. Derecho a la privacidad y protección de datos personales, así como todos los derechos previstos en el sistema jurídico de El Salvador.
2. Derecho a recibir información previa relativa a sus interacciones con sistemas de IA.
3. Derecho a solicitar y recibir una explicación sobre toda decisión, recomendación o previsión realizada por sistemas de IA.
4. Derecho a objetar decisiones o previsiones realizadas por sistemas de IA que puedan causar efectos jurídicos o que incidan significativamente en los intereses de la persona afectada.
5. Derecho a participar en el desarrollo y en las decisiones relativas a los sistemas de IA de acuerdo con el avance e innovaciones tecnológicas.
6. Derecho a la no discriminación y a la corrección de sesgos, de discriminación directa e indirecta, ilegal o abusiva.

Derechos de Oposición
Art. 10. Toda persona que sea o haya sido afectada por sistemas de IA tiene el derecho de oposición, siguiente:

1. Impugnar y solicitar la revisión de las decisiones, recomendaciones o pronósticos generados el sistema cuando produzcan efectos jurídicos relevantes o que impacten significativamente sus intereses.
2. Solicitar al responsable del tratamiento de los datos la corrección de ellos cuando estos sean incompletos, inexactos o desactualizados o estén basados en inferencias discriminatorias, irrazonables o que menoscaben la buena fe objetiva por ser datos inadecuados o abusivos trabajados con métodos imprecisos o estadísticos incorrectos y que estén en uso por sistemas de IA.

3. Solicitar y tener anonimato, el bloqueo o la eliminación de datos innecesarios, excesivos.

Habeas Data

Art. 11. En cumplimiento con el Derecho de Habeas Data, el encargado del tratamiento de datos personales debe respetar el derecho de los titulares a conocer, actualizar y rectificar toda la información que se haya recogido y que esté almacenada en bancos de datos y archivos de cualquier naturaleza, administrados por personas naturales y/o jurídicas privadas y de entidades públicas. Además, en su uso debe garantizarse a los titulares la preservación de su intimidad, privacidad y honra, mediante la protección de sus derechos a la información y de sus datos personales, los cuales se reconocen como derechos humanos y protegidos por la Constitución de El Salvador y en tratados internacionales.

Derechos Especiales

Art. 12. El titular de los datos personales tendrá los siguientes derechos en el uso de Habeas Data:

1. Conocer, actualizar, rectificar o eliminar sus datos personales que tienen los entes privados o públicos que actúan como encargados del tratamiento de los datos. Este derecho podrá ejercerse cuando se observe que los datos son parciales, inexactos, incompletos, fraccionados, que puedan inducir a error o aquellos que estén prohibidos o no hayan sido autorizados.
2. Solicitar prueba de la autorización otorgada al encargado del tratamiento, salvo en los casos especiales previstos en esta Ley.
3. Ser informado por el encargado del tratamiento y uso de sus datos personales.
4. Presentar quejas ante la Secretaría de Innovación y la Defensoría del Consumidor las quejas por infracciones a lo dispuesto en sus respectivas leyes.
5. Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no respete los principios, derechos y garantías constitucionales y legales.
6. Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

CAPÍTULO II
DEBERES, OBLIGACIONES Y RESPONSABILIDADES

Responsabilidad
Art. 13. El responsable del tratamiento de los datos ya sea por medios manuales o tecnológicos, en general y mediante sistemas de IA, en particular, para garantizar su correcto uso, deberá considerar, aplicar y ajustar todo su trabajo de conformidad con los siguientes principios:

1. Garantizar la seguridad, integridad, disponibilidad y confidencialidad de los datos personales.
2. No adulterar ni tratar datos que no hayan sido autorizados.
3. Respetar el derecho de acceso del titular a su información personal.
4. No generar discriminación sino crecimiento incluyente, equitativo y mayor bienestar socioeconómico.
5. Respeto de la justicia, equidad e inclusión socioeconómica.
6. Aportar al progreso sostenible y de respeto del medioambiente.
7. Libertad de decisión y de elección.
8. Prevención, precaución y mitigación de potenciales riesgos sistémicos por usos indebidos intencionales o no intencionales.
9. Mantener sistemas tecnológicos transparentes, explicables, integrales y auditables.
10. Confiabilidad, calidad, veracidad de la información que se utilice o que se genere.
11. Rendición de cuentas y reparación integral de daños.
12. Alta seguridad cibernética.
13. Trazabilidad de las decisiones durante todo el ciclo de vida de los sistemas de IA como medio de rendición de cuentas y atribución de responsabilidades a una persona natural o jurídica.
14. Abiertos al debido proceso legal, impugnabilidad y el principio de contradicción o derecho a confrontar las pruebas que se presenten en contra durante un juicio.

Vinculación
Art. 14. Todas las actuaciones de los responsables del tratamiento y la transferencia de las bases de datos, tanto públicos como privados, deberán ajustarse a los principios generales citados en esta Ley y otras leyes relacionadas.

Vinculación
Art. 14. Todas las actuaciones de los responsables del tratamiento y la transferencia de las bases de datos, tanto públicos como privados, deberán ajustarse a los principios generales citados en esta Ley y otras leyes relacionadas.

Coordinación legal Interinstitucional
Art. 15. La Secretaría de Innovación en conjunto con la Defensoría del Consumidor dictarán las normas, reglamentos técnicos y lineamientos relacionados con la Protección de Datos, para garantizar su protección.

Obligación de Informar
Art. 16. Cuando se recaben datos personales se deberá informar previamente a sus titulares en forma precisa e inequívoca:

1. La finalidad para la que serán tratados y quiénes podrán ser sus destinatarios o clase de destinatarios.
2. La existencia de la base de datos, electrónica o de cualquier otro tipo, de que se trate y la identidad y domicilio de su responsable.
3. El carácter obligatorio o facultativo de las respuestas al cuestionario que se le proponga, en especial en cuanto a los datos sensibles.
4. Las consecuencias de proporcionar los datos y de la negativa a hacerlo o de su inexactitud.
5. De la identidad y datos de contacto del responsable del tratamiento de ellos o, en su caso, de su representante.
6. La posibilidad de ejercer los derechos de acceso, rectificación, supresión u oposición.
7. Las medidas y mecanismos de protección y seguridad que el responsable del tratamiento de los datos ha implementado y mantiene activas para salvaguardar la información, conforme a lo establecido en esta Ley y otras leyes relacionadas; y sus derechos en casos de que la seguridad sea vulnerada.
8. Las obligaciones del presente artículo pueden satisfacerse mediante la publicación de políticas de privacidad de forma física o electrónica, las que deben ser fácilmente accesibles e identificables.
9. Cuando se proyecte un tratamiento de dato distinto de aquel para el cual se recolectaron, se proporcionará al Titular información sobre esta finalidad ulterior y cualquier otra información adicional pertinente.

Gratuidad del Servicio
Art. 17. Todo titular de datos personales tendrá el derecho de acceso gratuito a toda la información que le concierne y que se encuentre en bases de datos públicas o privadas. Este derecho incluye la posibilidad de conocer el origen de los datos y la finalidad para la cual fueron recabados.

La información debe ser proporcionada en forma clara y detallada utilizando un lenguaje de fácil comprensión, tal como se establece en esta Ley; y debe incluir la totalidad del registro perteneciente al titular, incluso si la solicitud solo aborda un aspecto de los datos personales, a menos que hayan sido objeto de seudonimización o disociación, en cuyo caso se certificarán dichas circunstancias. En ningún caso el informe podrá revelar datos pertenecientes a terceros, incluso si están vinculados con el interesado.

El titular debe poder obtener la información de sus datos personales mediante una consulta sencilla, visualización electrónica u otras tecnologías disponibles, sin la necesidad de utilizar claves o códigos. Este derecho de acceso lo podrá ejercitar el interesado cuando detecte errores, falsedades o desactualizaciones en sus datos. Si este no es el caso, este derecho lo podrán ejercitar precio el pago de una tarifa que no sea mayor que cinco por ciento (5 %) del salario mínimo del Sector de Comercio y Servicios.

Derecho de Modificación de datos confidenciales
Art. 18. Toda persona natural tendrá derecho a solicitar la rectificación, actualización e inclusión en sus datos personales cuando constate errores, falsedades o desactualizaciones.

El responsable de la base de datos o del tratamiento deberá realizar la rectificación, actualización e inclusión en un plazo máximo de quince (15) días hábiles desde que recibe la solicitud por el titular del dato, o informar sobre las razones por las que su solicitud no procede. El responsable de la base de datos o del tratamiento notificará al titular sobre la rectificación, actualización e inclusión realizada

Supresión de Información de datos personales
Art. 19. El titular tendrá derecho a solicitar la supresión de los datos personales cuando los datos personales ya no son necesarios con relación a los fines para los cuales fueron tratados.

Supresión de Información de datos personales
Art. 19. El titular tendrá derecho a solicitar la supresión de los datos personales cuando los datos personales ya no son necesarios con relación a los fines para los cuales fueron tratados.

El ejercicio del derecho de supresión dará lugar al bloqueo de los datos, conservándose únicamente a disposición de la administración pública, jueces y tribunales para la atención de las posibles responsabilidades causadas por el tratamiento de los datos o incumplimiento de los plazos establecidos para su resguardo según esta Ley y otras leyes relacionadas.

Si los datos rectificados o suprimidos fueron previamente comunicados, el responsable del tratamiento de los datos deberá notificar la solicitud correspondiente a los destinatarios de dicha comunicación y, en caso que el tratamiento persista, proceder al bloqueo correspondiente.

Improcedencia
Art. 20. No procede la supresión de los datos personales, en los siguientes casos:

1. Cuando la supresión cause perjuicios a los derechos e intereses legítimos del responsable o terceros.
2. Cuando exista un notorio error o falsedad en la información que acompaña la solicitud.
3. Si contraviene lo establecido por una ley.
4. Cuando sean necesarios para ejercer el derecho a la libertad de expresión y de prensa.
5. Cuando los datos personales hayan sido objeto de seudonimización o disociación.
6. Cuando existan razones de interés público, fines de investigación científica o histórica o estadísticos.

El encargado del tratamiento de la base de datos debe notificar al titular la supresión de sus datos en un lapso no mayor de cinco (5) días hábiles de efectuada la supresión, lo cual deberá hacer sin cargo alguno.

Derecho a Impugnar
Art. 21. Las personas tienen el derecho de impugnar una decisión con efectos jurídicos si esta afecta significativamente sus derechos y se basa exclusivamente en un tratamiento automatizado de

datos destinado a evaluar aspectos específicos de su personalidad.

Este derecho no aplicará si la decisión:

1. Es necesaria para la celebración o ejecución de contratos entre el titular y el responsable.
2. Está autorizada por otras leyes especiales en la materia.
3. Está basada en el consentimiento del titular.

El titular podrá expresar su punto de vista e impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento basado en los numerales 1 y 2, siempre que se base únicamente en un tratamiento automatizado de datos personales que defina sus características o personalidad.

En este caso, titular podrá ejercer sus derechos a obtener información del responsable de la base de datos, incluyendo los criterios de valoración que sustentaron la decisión manifestada en el acto.

TÍTULO III
TRATAMIENTO DE LA INFORMACIÓN CONFIDENCIAL EN EL ÁMBITO PÚBLICO Y PRIVADO

CAPÍTULO I
ENTE REGIDOR Y CONTRALORÍA

Actividades de Promoción y Difusión
Art. 22. La Secretaría de Innovación y la Defensoría del consumidor deberán difundir la información para dar a conocer ampliamente el derecho a la protección de datos personales, promover su ejercicio y ejercer las facultades enfocadas a la vigilancia, supervisión, investigación e inspección de las obligaciones establecidas en esta Ley y otras leyes relacionadas para los sujetos obligados.

Interpretación Dinámica
Art. 23. La Secretaría de Innovación y la Defensoría del consumidor deben velar por la correcta interpretación y aplicación de esta ley y de otros cuerpos normativos relacionados, para garantizar la protección de los datos personales y de los derechos de los titulares.

CAPÍTULO II
AUTORIZACIONES, SOLICITUDES Y TRÁMITES

Solicitud
Art. 24. El titular o su representante podrán solicitar al responsable de la base de datos en los casos establecidos en la presente Ley, acceso, rectificación, actualización, supresión u oposición respecto de los datos personales que le conciernen. Este derecho y las obligaciones establecidas no serán aplicables cuando el responsable sea una persona natural o jurídica clasificada como micro o pequeña empresa, a menos que el tratamiento que realice pueda representar un riesgo significativo al derecho del titular o que se trate de datos personales sensibles o que no sea ocasional.

Formas de presentación de la solicitud
Art. 25. La solicitud de acceso, rectificación, supresión u oposición podrá presentarse tanto de forma física o electrónica y deberá estar acompañada de la documentación correspondiente y cumplir los siguientes requisitos:

1. Dar el nombre completo del titular o del representante, sus generales y, de ser aplicable, la información sobre la personería jurídica.
2. Proporcionar una descripción clara y precisa de los datos personales respecto de los cuales se busca ejercer alguno de los derechos mencionados en esta Ley.
3. Presentar los documentos que acrediten la identidad del titular o, en su caso, la representación de este. En el caso de las solicitudes de rectificación de datos personales, el solicitante o su representante deberá aportar pruebas que respalden las modificaciones señaladas de conformidad con el numeral anterior.
4. Cualquier otro elemento o documento que facilite la localización de los datos personales.
5. Indicar el domicilio del responsable, o de en su defecto, proporcionar un medio electrónico para recibir notificaciones, y los datos generales de la persona encargada de gestionar la solicitud.

Designación
Art. 26. Todo responsable deberá designar una persona natural encargada de tramitar las solicitudes físicas o electrónicas de los titulares, para el ejercicio de los derechos establecidos en la

presente Ley. Esta persona deberá promover la protección de datos personales dentro de la organización y apoyar programas de capacitación en este tema.

Sencillez en la entrega de Información
Art. 27. Ante una solicitud de acceso a los datos personales, el responsable de su tratamiento deberá entregar a su titular o su representante, una copia de la información correspondiente en un formato que sea de fácil comprensión para el solicitante de la información, en un plazo máximo de quince días calendario contados a partir de la fecha en que se recibió la solicitud.

En el caso de solicitudes de rectificación, supresión u oposición, el responsable de su tratamiento deberá entregar al solicitante una resolución que documente las modificaciones realizadas o justifique por qué no se llevaron a cabo, dentro del plazo establecido por la ley. En situaciones excepcionales donde no sea posible entregar la información, realizar la rectificación o supresión u oposición debido a la complejidad de la información u otras circunstancias, se podrá ampliar el plazo en quince (15) días calendario adicionales.

Cumplimiento de la Obligación
Art. 28. La obligación de acceso y entrega de la información se dará por cumplida cuando el responsable de su tratamiento ponga a disposición del titular sus datos personales, ya sea mediante la entrega de copias en formato físico o electrónico.

En el caso que el titular solicite el acceso a los datos a una persona que se presume es la responsable de su tratamiento y esta resulte no serlo, esta deberá comunicarlo de inmediato y proporcionar la información sobre la persona u oficina designada para gestionar dichos trámites, cuando dicha información sea de su conocimiento.

Rechazo
Art. 29. El responsable de su tratamiento podrá negar el ejercicio de los derechos de acceso a los datos personales, o realizar su rectificación, supresión u oposición al tratamiento de ellos en los siguientes casos:

1. Cuando el solicitante no sea el titular de los datos personales, o el representante no esté debidamente acreditado para ello.

2. Cuando en su base de datos no se encuentren los datos personales del solicitante.
3. Cuando se lesionen los derechos de un tercero.
4. Cuando exista un impedimento legal, o la resolución de una autoridad competente que restrinja el acceso a los datos personales, o que impida la rectificación, supresión u oposición de estos.
5. En los demás casos establecidos en esta Ley y otras leyes relacionadas.

La negativa a que se refiere este artículo podrá ser parcial en cuyo caso el responsable efectuará el acceso, rectificación, supresión u oposición que proceda.

En todos los casos anteriores, el responsable del tratamiento de los datos personales deberá informar al titular, o en su caso, al representante, sobre el motivo de su decisión y comunicarla en los plazos establecidos para tal efecto, utilizando el mismo medio por el cual se entregó la solicitud. Además, en caso necesario, deberá acompañar las pruebas pertinentes.

Ejercicio del Derecho de acceso a la solicitud
Art. 30. El acceso a los datos personales, así como la rectificación, supresión o la oposición al tratamiento de ellos lo ejercerá el titular o su representante de manera gratuita. En caso de copias magnéticas o electrónicas, si el interesado aporta el medio de almacenamiento la información, la reproducción también será gratuita.

CAPÍTULO III
DEL PREVIO CONSENTIMIENTO INFORMADO

Prohibición
Art. 31. Los operadores de redes no deben divulgar, alterar ni destruir la información personal que recopilan sin el consentimiento previo del titular, ni deben proporcionarla a otros operadores. Esto último no aplica cuando después de procesar la información no se puede identificar a la persona ni recuperar su identidad. En adición, los operadores de red deberán cumplir con lo establecido en los artículos 70 al 74 de la Ley de Inteligencia Artificial de El Salvador y todos aquellos que tengan alguna relación con los datos personales.

Sistemas de Prevención
Art. 32. Los operadores de redes deberán tener sistemas que permitan detectar la suplantación de identidad o phising para proteger y alertar a los usuarios de engaños y robo de información personal relevante mediante el envío de correos electrónicos que aparentan ser legales y con el uso de nombres afines.

Consentimiento previo
Art. 33. Para el tratamiento de datos sensibles será necesario tener previamente el consentimiento del titular o de su representante, el cual debe darse de manera:

1. Libre: sin mediar error, mala fe, dolo, violencia física o psicológica que puedan afectar la voluntad del titular.
2. Específico: por definir con claridad una o varias finalidades definidas de modo que justifiquen el tratamiento.
3. Informado: que el titular tenga conocimiento previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.
4. Expreso: debe ser inequívoco, de forma tal que pueda demostrarse el otorgamiento del consentimiento, el cual se puede obtener por medios físicos o electrónicos.
5. Individualizado: cada titular debe dar individualmente el consentimiento para el uso de sus datos personales sensibles.

Formas de otorgar el consentimiento
Art. 34. El responsable de recopilar datos personales para su tratamiento deberá obtener el consentimiento del titular, salvo por las excepciones establecidas en esta Ley.

El consentimiento deberá ser otorgado por el titular mediante un documento físico o electrónico, el cual deberá ser resguardado por el responsable de la base de datos.

De igual manera, el documento por medio del cual el titular o su representante extiende su consentimiento para el tratamiento de los datos personales debe ser de fácil comprensión, gratuito y debidamente identificado.

Registro
Art. 35. Para demostrar la obtención del consentimiento o la comunicación de la política de privacidad, la carga de la prueba recaerá, en todos los casos, en el responsable de la base de datos,

conforme a las formas que se establecen en esta Ley.

Revocatoria
Art. 36. El titular podrá revocar su consentimiento para el tratamiento de sus datos personales en cualquier momento, pero sin aplicar un efecto retroactivo, ante lo cual, el responsable deberá establecer mecanismos expeditos, sencillos y gratuitos para revocar el consentimiento.

El retiro del consentimiento no afectará la licitud del tratamiento posterior por el responsable si dicho tratamiento es realizado con base a otras de las causales establecidas en la presente Ley que justifican dicho tratamiento.

Procedimiento
Art. 37. Ante una solicitud de revocación del consentimiento de un titular, el responsable de la base de datos deberá suprimir los datos en un plazo de hasta de cinco (5) días hábiles contados a partir del momento que recibió la solicitud para proceder conforme a la revocación o comunicar su procedencia.

De ser procedente la revocación, el responsable de la base de datos deberá informar en un plazo de hasta cinco (5) días hábiles a aquellas personas naturales o jurídicas a quienes haya transferido los datos, las que, a su vez, deberán eliminar los datos en un plazo de cinco (5) días hábiles a partir de la notificación de suprimirlos. La revocación del consentimiento no tendrá efecto retroactivo.

Confirmación de Revocatoria
Art. 38. Cuando el titular solicite la confirmación de la revocación del tratamiento de sus datos, el responsable de la base de datos deberá responder de forma gratuita dentro de los plazos establecidos en la presente Ley, contados a partir del momento de la presentación de dicha solicitud.

Denuncia
Art. 39. En caso que el responsable de la base de datos se niegue a tramitar la revocación del consentimiento, ya sea de manera expresa o tácita, el titular podrá presentar ante la Secretaría de Innovación y la Defensoría del Consumidor la denuncia correspondiente de conformidad a lo establecido en esta ley.

CAPÍTULO IV
SOBRE LA TRANSFERENCIA DE DATOS

Transferencia
Art. 40. Los datos personales objeto de tratamiento pueden ser transferidos para el cumplimiento de fines lícitos del responsable de la base de datos, siempre y cuando se notifique al titular sobre la política de privacidad de los datos. Esta notificación debe contener la finalidad de la transferencia e identificar al cesionario o proporcionar los elementos que permitan hacerlo.

El consentimiento para la transferencia no será necesario en los siguientes casos:

1. Cuando así se disponga en esta esta Ley y otras leyes relacionadas.
2. Cuando se realice entre dependencias de los órganos del Estado, en cumplimiento de sus respectivas competencias.
3. Cuando Se trate de datos sobre salud personal, de salud pública, emergencia o para la realización de estudios epidemiológicos, siempre y cuando se preserve la identidad de los titulares de los datos mediante mecanismos de seudonimización o disociación adecuados
4. Cuando Consista en intercambio de datos de carácter médico o cuando así lo requiera el tratamiento del afectado por razones de salud o higiene públicas.
5. Cuando se ha aplicado un procedimiento de seudonimización o disociación de la información, de modo que los titulares de los datos sean inidentificables.
6. Cuando Se trate de una transferencia de datos entre filiales de un mismo grupo económico.
7. Cuando se trate de una transferencia de datos a un intermediario tecnológico
8. Cuando se trate de tratamiento de información autorizada por la Ley para fines históricos, estadísticos o científicos.

El cesionario quedará sujeto a las mismas obligaciones legales y reglamentarias que el cedente, y éste último responderá solidaria y conjuntamente por el cumplimiento de estas obligaciones ante la Secretaría de Innovación, la Defensoría del Consumidor y el titular de los datos.

Datos personales de niñas, niños y adolescentes
Art. 41. En todo tratamiento de datos personales de niños, niñas y adolescentes, se debe garantizar el pleno respeto de sus derechos conforme a lo establecido en esta Ley, la Ley Crecer Juntos para la Protección Integral de la Primera Infancia, niñez y adolescencia y la Ley de Inteligencia Artificial, que requieren el cumplimiento del principio del interés superior de las niñas, niños y adolescentes para asegurar su desarrollo integral y el disfrute de sus derechos y garantías.

Queda expresamente prohibido el tratamiento de datos personales de niños, niñas y adolescentes, salvo en los casos, en que la información que sea de naturaleza pública como datos estadísticos. No obstante, incluso en estos casos, se deberán implementar medidas para proteger la identidad de los titulares.

Transferencia de datos con organismos internacionales
Art. 42. La transferencia de datos personales de cualquier tipo está permitida sin requerir consentimiento cuando esta se realiza con países u organismos internacionales que proporcionen niveles adecuados de protección tecnológica, de acuerdo con lo establecido en esta Ley, la Ley de Inteligencia Artificial de El Salvador o del Derecho Internacional. Asimismo, está permitida la transferencia a entidades o intermediarios tecnológicos, siempre y cuando el responsable garantice que cuenta con todos los medios para proteger los datos de acuerdo con esta Ley, mediante contratos, códigos de conducta, ética o estándares internacionalmente aceptados.

Este tipo de transferencia también será permitida cuando se trate de:

1. Cooperación judicial internacional de acuerdo con el respectivo tratado, convenio o acuerdo según las circunstancias del caso.
2. Datos personales relativos a la salud por razones de salud pública, de emergencia o para la realización de estudios epidemiológicos, siempre y cuando se preserve la identidad de los titulares de los datos mediante seudonimización o disociación adecuados.
3. Intercambio de datos de carácter médico, cuando así lo requiera el tratamiento del afectado por razones de salud o higiene públicas.
4. Transferencias bancarias o bursátiles conforme las leyes aplicables.

5. Tratados internacionales sobre protección de datos personales que El Salvador ha firmado.
6. Cooperación internacional entre organismos de inteligencia para la lucha contra el crimen organizado, el terrorismo, el narcotráfico, delitos informáticos y conexos.
7. Transmisiones de datos personales entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable.
8. Transferencia de datos a un intermediario tecnológico.
9. Transferencia de datos entre empresas relacionadas de un mismo grupo económico, aplicando los requisitos establecidos en esta Ley.

También será posible realizar la transferencia internacional de datos personales en las siguientes situaciones:

1. Que el interesado haya dado su consentimiento para la transferencia prevista.
2. Que la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento de los datos, o para la ejecución de actos precontractuales a petición del interesado.
3. Que la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar en interés del interesado, entre el responsable del tratamiento de los datos y un tercero.
4. Que la transferencia sea necesaria o legalmente exigida para la salvaguardia de un interés público importante, o para el reconocimiento, ejercicio o defensa de un derecho en un procedimiento judicial.
5. Que la transferencia sea necesaria para salvaguardar el interés especial del interesado.
6. Que la transferencia se haga desde un registro que, en virtud de disposiciones de esta Ley y otras leyes relacionadas, sirva para facilitar información y esté disponible para consultas por parte del público en general o por cualquier persona que pueda demostrar un interés legítimo, siempre que se cumplan las condiciones establecidas en esta Ley para cada caso particular.

Políticas de Actuación

Art. 43. Las transferencias de datos personales por parte de los responsables estarán supeditadas al fiel cumplimiento de principios y obligaciones establecidas en esta esta Ley, la Ley de Inteligencia

Artificial y otras leyes relacionadas. Las políticas de actuación del responsable deberán estar registradas ante la Defensoría del Consumidor.

Obligación de Probar
Art. 44. Para demostrar que la transferencia de datos personales se realizó conforme a esta Ley y su reglamento técnico, el derecho y deber de probar recaerá en el responsable de la base de datos.

Obligación de contratar
Art. 45. El responsable de la transferencia de datos personales deberá establecer un contrato o convenio con el receptor, en el cual se establezcan al menos las mismas obligaciones y responsabilidades que tiene el sujeto el responsable de la transferencia de dichos datos.

Conservación de la Información
Art. 46. El responsable de la transferencia de datos personales establecerá y documentará los procedimientos para la inclusión, conservación, modificación y supresión de los datos personales, así como las medidas de seguridad en su tratamiento. Además, el responsable de la base de datos debe asegurarse que se cumplen los principios establecidos en la presente Ley, la Ley de Inteligencia Artificial y otras leyes relacionadas especialmente la Ley de Procedimientos Administrativos.

Estas obligaciones no serán aplicables cuando el responsable sea una persona natural o jurídica clasificada como micro o pequeña empresa, a menos que el tratamiento que realice pueda representar un riesgo significativo para los derechos del titular, o que se trate de datos personales sensibles o que no sea ocasional.

De los proveedores
Art. 47. El responsable de la transferencia de datos personales podrá contratar o subcontratar los servicios de un intermediario tecnológico o proveedor de servicios, siempre y cuando haya verificado que dicho intermediario o proveedor cumple con las medidas de seguridad necesarias para garantizar la integridad y seguridad de los datos personales.

Intervención del encargado
Art. 48. El encargado solo podrá intervenir en el tratamiento de las bases de datos personales de acuerdo con lo establecido en el

contrato celebrado con el responsable y siguiendo sus indicaciones.

Obligaciones del encargado
Art. 49. El encargado tendrá las siguientes obligaciones en el tratamiento de las bases de datos personales:

1. Tratar los datos personales únicamente de acuerdo con las instrucciones del responsable de la base de datos.
2. Abstenerse de tratar los datos personales para fines distintos a los indicados por el responsable de la base de datos.
3. Implementar las medidas de seguridad conforme a lo establecido en esta Ley y su reglamento técnico, así como la Ley de Inteligencia Artificial y otras leyes relacionadas.
4. Mantener la confidencialidad de los datos personales tratados.
5. No transferir o difundir los datos personales, salvo instrucciones expresas por parte del responsable de la base de datos.
6. Eliminar los datos personales una vez finalizada la relación jurídica con el responsable de la base de datos o según las instrucciones proporcionadas, siempre y cuando no exista una disposición legal que requiera su conservación.
7. Cumplir con cualquier otra obligación que le atribuya esta Ley, la Ley de Inteligencia Artificial y otras leyes relacionadas.

Política de Gestión
Art. 50. Los responsables de las bases de datos deben elaborar una política de gestión, la cual deberá ser comunicada al encargado para su fiel cumplimiento. Esta política deberá incluir al menos lo siguiente:

1. Las políticas de gestión y los manuales de privacidad y seguridad obligatorios y exigibles dentro de la organización del responsable.
2. Manual de capacitación, actualización y concientización del personal sobre las obligaciones en materia de protección de datos personales.
3. Procedimientos para mantener un estricto control interno para el cumplimiento de las políticas de privacidad.
4. Procedimientos para recibir y responder dudas y quejas de los titulares de los datos personales o sus representantes, con medios tecnológicos ágiles, de fácil acceso y gratuitos, así como para acceder, rectificar, modificar, bloquear o suprimir la información contenida en la base de datos y revocar su consentimiento.

5. Medidas y procedimientos técnicos que permitan mantener un historial de los datos personales durante su tratamiento.
6. Mecanismos mediante los cuales el responsable de la base de datos comunica al encargado las condiciones en las que el titular consintió la recolección, transferencia y tratamiento de sus datos.

Estas medidas, así como sus posteriores modificaciones, deben ser inscritas ante la Secretaría de Innovación y la Defensoría del Consumidor como políticas de gestión.

Contraloría
Art. 51. La Secretaría de Innovación y la Defensoría del Consumidor deberán verificar que los responsables de las bases de datos estén cumpliendo en todo momento con los términos establecidos en la política de gestión.

Medidas de seguridad
Art. 52. El responsable de las bases de datos debe establecer y mantener medidas de seguridad administrativas, físicas y tecnológicas para el control o controles que tienen como objetivo la protección de los datos personales de acuerdo con lo establecido en esta Ley y su reglamento. Además, deberá velar que el encargado de la base de datos y el intermediario tecnológico cumplan con las medidas de seguridad, para el resguardo de la información.

Queda prohibido registrar datos personales en bases que no reúnan las condiciones técnicas de integridad, seguridad, disponibilidad y confidencialidad cuando estas medidas sean de obligatorio cumplimiento para el responsable.

Medidas de Ciberseguridad
Art. 53. El responsable de las bases de datos debe establecer y mantener las medidas de ciberseguridad que trate o almacene, considerando los siguientes factores:

1. La sensibilidad de los datos personales tratados, cuando la ley lo permite.
2. El desarrollo e innovación tecnológica.
3. Las posibles consecuencias de una vulneración para los titulares de sus datos personales.

4. El número de titulares de datos personales.
5. Las vulnerabilidades previas ocurridas en los sistemas de tratamiento o almacenamiento de datos.
6. El riesgo por el valor, cuantitativo o cualitativo, que pueden tener los datos personales.
7. Otros factores que resulten de otras leyes o regulación aplicables al responsable.

Acciones

Art. 54.- Para establecer, mantener y garantizar la seguridad física y tecnológica de los datos personales, el responsable de las bases de datos debe realizar al menos las siguientes acciones:

1. Elaborar una descripción detallada del tipo de datos personales tratados o almacenados.
2. Crear y mantener actualizado un inventario de la infraestructura tecnológica, que incluya equipos, así como programas de cómputo y sus licencias.
3. Definir el tipo de sistema, programa, método o proceso utilizado en el tratamiento o almacenamiento de los datos.
4. Establecer las medidas de seguridad aplicables a los datos personales e identificar aquellas que han sido implementadas.
5. Estas acciones serán verificadas por la Secretaría de Innovación y la Defensoría del Consumidor.

Actualización de las políticas de seguridad

Art. 55. Los responsables de las bases de datos deben actualizar las políticas de seguridad cuando ocurran los siguientes eventos:

1. Se modifiquen las medidas y los procesos tecnológicos de seguridad.
2. Se produzcan modificaciones sustanciales en el tratamiento o almacenamiento, debido a un cambio del nivel de riesgo.
3. Se modifique la plataforma tecnológica.
4. Se vulneren los sistemas de tratamiento o almacenamiento de datos personales de conformidad con lo dispuesto en esta Ley y su reglamento.
5. Exista una afectación a los datos personales, distinta a las mencionadas anteriormente.

Deber de informar

Art. 56. Los responsables de las bases de datos deben informar al titular o su representante legal de forma individual por cualquier

acto que ponga en riesgo la seguridad de sus datos, en un plazo no mayor a cinco (5) días hábiles a partir del momento en que se identificó la vulnerabilidad, para que los titulares afectados puedan tomar las medidas correspondientes. Dentro de este mismo plazo el responsable de la base de datos debe iniciar un proceso de revisión exhaustiva para determinar la magnitud de la afectación y definir y aplicar las medidas correctivas y preventivas que correspondan.

Art. 57. Los responsables de las bases de datos deben informar al titular o su representante legal, así como a la Secretaría de Innovación y la Defensoría del Consumidor, tan pronto como se conozca las posibles vulnerabilidades de seguridad, detallando al menos lo siguiente:

1. La naturaleza del incidente.
2. El tipo de datos comprometidos.
3. Las acciones correctivas realizadas de forma inmediata.
4. Los medios o el lugar tecnológico donde se puede obtener más información sobre lo sucedido.

Prohibición
Art. 58. Ninguna persona puede ser obligada a proporcionar datos sensibles, los cuales solo podrán ser tratados con el consentimiento expreso e inequívoco del titular.

Los datos sensibles solo pueden ser recolectados y tratados con el consentimiento del titular y en situaciones específicas autorizadas por esta Ley cuando existan razones de interés general establecidas por la legislación de El Salvador o cuando el solicitante tenga un mandato legal para hacerlo. Estos datos también podrán ser utilizados con fines estadísticos o científicos siempre que se desvinculen de sus titulares.

En el momento de recabar el consentimiento se debe advertir al titular o a su representante legal acerca de su derecho a no prestarlo.

No obstante, podrán ser objeto de tratamiento los datos de carácter personal relativos a la salud, a tratamientos necesarios para la prevención o para diagnósticos médicos, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios de salud, siempre que el tratamiento de los datos se realice por un

profesional de salud sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto.

Excepción del previo consentimiento
Art. 59. También podrán ser objeto de tratamiento los datos cuando sean necesarios para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento, en este caso se solicitará al secretario de Innovación autorice el tratamiento de los datos, quien tendrá un término de cuarenta y ocho (48) horas para pronunciarse sobre la aprobación o rechazo de la petición.

Los datos personales relativos a la comisión de infracciones penales, civiles o administrativas solo pueden ser objeto de tratamiento por parte de las autoridades públicas competentes. Nada de lo establecido en esta Ley impedirá a las autoridades públicas comunicar o hacer pública la identidad de las personas naturales o jurídicas que estén siendo investigadas por supuestamente haber cometido infracciones a la normativa vigente.

Secreto profesional sobre datos confidenciales
Art. 60. Los establecimientos de salud públicos o privados y los profesionales de la salud pueden recolectar y tratar los datos personales relativos a la salud física o mental de los pacientes que atienden o que estén o hubieren estado bajo tratamiento de ellos, respetando los principios del secreto profesional, la normativa específica y lo establecido en esta Ley.

Protección de datos personales en redes sociales
Art. 61. Los operadores que tengan redes públicas o que presten servicios de comunicaciones electrónicas al público deben garantizar, en el ejercicio de su actividad, la protección de los datos personales conforme a esta Ley, la Ley de Inteligencia Artificial y la de la Defensoría del Consumidor. Para ello, deben adoptar las medidas técnicas, de gestión y ciberseguridad para preservar la seguridad en el uso de su red o en la prestación de sus servicios, garantizando la protección de los datos personales. En caso de que exista un riesgo violación de la ciberseguridad de la red pública de comunicaciones electrónicas, el operador deberá informar a los suscriptores y usuarios sobre dicho riesgo y las medidas que pueden adoptar.

CAPÍTULO V
BASE DE DATOS DE INSTITUCIONES PÚBLICAS

Creación de Registro Público
Art. 62. La creación, modificación o supresión de bases de datos pertenecientes a instituciones públicas deberán registrarse conforme lo previsto en esta Ley y otras leyes relacionadas.

Datos personales sujetos a esta ley
Art. 63. Están sujetos al régimen de la presente ley, los datos personales que, por haber sido almacenado para fines administrativos, deban ser objeto de registro permanente en las bases de datos de la Fuerza Armada, organismos policiales o de inteligencia; así como aquellos relacionados con antecedentes personales que requieran las autoridades administrativas o judiciales en virtud de disposiciones legales

El tratamiento de datos personales con fines de Defensa Nacional o seguridad pública por parte de las Fuerza Armadas, organismos policiales o inteligencia, sin previo consentimiento de los titulares, queda limitado a aquellos necesarios para el estricto cumplimiento de las misiones relacionadas con la Defensa Nacional, la seguridad pública o para la represión de los delitos. Estas bases de datos deben ser específicas y clasificadas por categorías en función de su grado de fiabilidad.

La aplicación de esta disposición dependerá de la clasificación de la información pública de las instituciones mencionadas en los artículos precedentes, para ello, será aplicable la Ley de Acceso a la Información Pública y su reglamento.

Denegación de acceso
Art. 64. Los responsables de las bases de datos que contengan los datos a los que se refiere el artículo anterior podrán denegar el acceso, la rectificación o supresión en función de los peligros que pudieran derivarse para la defensa del Estado o la seguridad pública, la protección de los derechos y libertades de terceros o las necesidades de las investigaciones que se estén realizando.

El titular de los datos que haya denegado total o parcialmente el ejercicio de los derechos establecidos en esta Ley podrá recurrir a la Secretaría de Innovación y/o a la Defensoría del consumidor,

la cual deberá asegurarse de la procedencia o improcedencia de la denegación.

CAPÍTULO VI
BASES DE DATOS DE TITULARIDAD PRIVADA

Inscripción y Registro
Art. 65. Todo responsable de una base de datos deberá estar registrado e incluido en el registro de la Secretaría de Innovación, salvo que sea miembro de una micro o pequeña empresa. Esta exención se aplicará siempre y cuando el tratamiento que realice pueda representar un riesgo significativo a los derechos del titular, que se trate de datos personales sensibles o cuyo tratamiento no sea ocasional.

Tipos de Información por registrar
Art. 66. Los tipos de información incluidos en las bases de datos públicas o privadas destinadas a proporcionar informes deben registrarse tanto en la Secretaría de Innovación como en la Defensoría del Consumidor. Ambas instancias deben coordinarse para garantizar la consistencia de sus registros.

El registro de los datos debe tener como mínimo la siguiente información:

1. Nombre del responsable, número de documento de identidad y domicilio.
2. Características y finalidad de la base de datos.
3. Tipo de datos personales contenidos en cada base.
4. Método de recolección, y en caso de ser aplicable, el procedimiento para su actualización.
5. Finalidad del uso de los datos y la identificación general de las personas naturales o jurídicas con las que pueden ser compartidos
6. Medidas de ciberseguridad utilizadas para garantizar la seguridad de los datos, incluyendo la categoría de las personas con acceso al tratamiento de la información.
7. Período de conservación de los datos.
8. Procedimientos y condiciones para que las personas pueden acceder a sus datos, así como para solicitar su actualización, rectificación o supresión, mediante medios físicos o electrónicos.

Ningún responsable de datos podrá almacenar datos personales que difieran de los declarados en el registro. El incumplimiento de estos requisitos dará lugar a las sanciones previstas en esta Ley.

Datos de uso personal
Art. 67.- Los archivos, registros o bases de datos privados destinados exclusivamente para un uso personal no necesitan registrarse de acuerdo con lo previsto en esta Ley.

Recopilación de datos
Art. 68. La recopilación de datos utilizando medios físicos y electrónicos relacionados con domicilios, reparto de documentos, publicidad o venta directa y otras actividades, se podrá tratar para establecer perfiles determinados con fines promocionales, comerciales o de publicidad. Ellos pueden ser utilizados para establecer hábitos de consumo, siempre y cuando figuren en documentos accesibles al público o hayan sido facilitados por los propios titulares u obtenidos con su consentimiento. El titular de los datos tiene el derecho de acceso a ellos sin cargo alguno.

El titular podrá en cualquier momento solicitar el retiro o bloqueo de su nombre de las bases de datos de forma física o electrónica.

CAPÍTULO VII
BASES DE DATOS PÚBLICAS

Bases de Datos
Art. 69. Las normas sobre creación, modificación o supresión de bases de datos pertenecientes a instituciones públicas deben establecerse mediante Acuerdo Ejecutivo publicado en el Diario Oficial y en el sitio web de la Secretaría de Innovación y en el de la Defensoría del Consumidor.

Estas normas deben indicar:
1. Características y finalidad de la base de datos.
2. La designación genérica de las personas de las cuales se pretende obtener datos y el carácter facultativo u obligatorio de su suministro por parte de los titulares.
3. Los procedimientos para la obtención y actualización de los datos.
4. La estructura básica de la base computarizada y la descripción de la naturaleza de los datos personales que contendrá.

5. Las cesiones o transferencias que se harán de acuerdo con lo establecido en esta Ley.
6. Los nombres de los responsables de la base de datos, incluyendo la dependencia jerárquica.
7. Las oficinas y los sitios web donde se pueden presentar reclamos en ejercicio de los derechos de acceso, rectificación o supresión de datos personales.

En las disposiciones que se dicten para la supresión de los registros se establecerán las medidas y métodos que se utilizarán para su destrucción.

Excepción de Inaplicabilidad
Art. 70. Las normas previstas en esta Ley no se aplicarán a las encuestas de opinión, mediciones y estadísticas resultantes, trabajos de prospección de mercados, investigaciones científicas o médicas y de educación, en la medida que los datos recogidos hayan sido objeto de seudonimización o disociación.

En el caso que durante el proceso de recolección de datos no sea posible mantener el anonimato, se deberá utilizar una técnica de seudonimización o disociación.

CAPÍTULO VIII
NOTIFICACIÓN DE INCIDENTES GRAVES

Obligación de Informar por parte de Agentes IA
Art. 71. Los agentes de IA informarán a la Secretaría de Innovación cada vez que ocurra un incidente grave de seguridad, especialmente cuando exista algún riesgo de violación grave de los derechos humanos de las personas, de la vida e integridad física de una persona o grupo de personas, que pueda causar u ocurrir una interrupción de las operaciones de infraestructura crítica, así como causar daños graves a la propiedad o al medio ambiente, de acuerdo con lo establecido en esta Ley.

TÍTULO IV
DE LAS INFRACCIONES Y SANCIONES

CAPÍTULO I
DE LAS INFRACCIONES

Tipos de Infracciones
Art. 72. Las infracciones establecidas en esta Ley de Protección de Datos Personales se fundamentan en el riesgo y consecuencias que puede tener para los titulares, ya sea de manera particular o como grupo. Las infracciones cometidas por los sujetos de esta ley pueden ser de tres tipos: infracciones leves, infracciones graves e infracciones muy graves.

Infracciones Leves
Art. 73. Son infracciones leves a la Ley de la IA, las siguientes:

A. Las que incumplen el principio de transparencia de la información o el derecho de información del titular, por no facilitar toda la información que exigen esta Ley, ni responder a sus derechos de acceso, rectificación, supresión, limitación del tratamiento o portabilidad de sus datos, ni comunicar estas acciones.
B. Tener el registro de actividades de tratamiento de datos sin incluir toda la información que establece esta Ley.
C.Pedir un pago al interesado para poder acceder a la información o para atender las solicitudes de ejercicio sus derechos según esta Ley.
D. Incumplir con la obligación de notificar la rectificación o supresión de datos personales o limitar del tratamiento que establece esta Ley.
E.No cumplir con la obligación de informar al afectado de los destinatarios a los que se haya comunicado la rectificación, supresión o limitación del tratamiento.
F.Incumplimiento de las obligaciones de los responsables y encargados del tratamiento de los datos.
G. No informar sobre los riesgos efectivos de seguridad a la Secretaría de Innovación en los plazos establecidos en esta Ley y/o hacerlo de forma incompleta.
H. Incumplir las obligaciones establecidas por los organismos de certificación de informar a la Secretaría de Innovación para la expedición, renovación o retirada de una certificación.

Infracciones Graves
Art. 74. Son infracciones graves a la Ley de la IA, las siguientes:

A. Tratar datos de menores de edad sin haber obtenido su consentimiento o de sus padres o tutores.

B. No verificar la validez del consentimiento del menor o de sus padres o tutores.
C. Obstaculizar reiteradamente la solicitud del titular de acceso, rectificación, supresión, limitación del tratamiento o portabilidad de sus datos en los procedimientos y sistemas que no se requieren la identificación del titular.
D. No aplicar las medidas técnicas y de organización que se tiene para garantizar la protección y la seguridad de los datos desde el diseño.
E. No informar sobre las violaciones de los sistemas de seguridad por no haber cumplido don las medidas de seguridad que fueron establecidas e informadas a la Secretaría de Innovación.
F. No responder a la Secretaría de Innovación y/o a la Defensoría del Consumidor en el tiempo establecido a las solicitudes de información o de acciones a seguir para la protección de los datos personales.
G. Contratar un encargado del tratamiento de los datos personales que no ofrezca las garantías necesarias para aplicar las medidas técnicas y de organización necesarias, de acuerdo con lo establecido en esta Ley.
H. Contratar a un tercero para el tratamiento de datos sin haber firmado un contrato que cumpla con los requisitos de las leyes de El Salvador.
I. No tener actualizado el registro de actividades.
J. Incumplir reiteradamente los mandatos establecidos en esta Ley y las leyes respectivas en lo referente a el tratamiento de los datos personales.

Infracciones Muy Graves
Art. 75. Son infracciones muy graves el mantener prácticas de IA de alto riesgo, así como el:

A. Tratamiento de datos los personales de una forma que vulneren los derechos, garantías y principios establecidos en la Constitución de El Salvador, en esta Ley y los establecidos por la Defensoría del Consumidor y que esto haya causado un daño irreparable a los titulares.
B. Tratamiento de los datos personales sin haber comprobado que son legítimos ni haber verificado la validez del consentimiento otorgado por el titular.

C. Utilizar los datos personales obtenidos con una finalidad diferente a la que dio el consentimiento el titular.
D. Tratamiento de los datos personales relativos a sanciones administrativas, condenas, sanciones penales o medidas de seguridad que violen los límites establecidos en esta Ley y las leyes de El Salvador.
E. Omisión reiterada del deber de informar al afectado sobre el tratamiento de sus datos personales y solicitar un pago para dar esta información al titular, lo que se considera en una violación de los derechos de las personas establecidos en esta Ley.
F. Transferencias internacionales de datos personales sin las debidas garantías.
G. Incumplir las resoluciones dictadas por la Secretaría de Innovación.
H. Incumplir con la obligación de bloqueo de datos, entendida como el acto de identificación y reserva de ellos para protegerlos ante consultas o difusiones de cualquier tipo.
I. No facilitar el acceso a la Secretaría de Innovación a los datos personales, información, ubicación física, equipos y medios de tratamiento cuando así lo demande en el transcurso de una investigación.
J. Reversión deliberada de cualquier procedimiento de anonimización para que se pueda volver a identificar a los titulares

CAPÍTULO II
DE LAS SANCIONES

Aplicación de Sanciones
Art. 76. Si se ha incurrido en alguna de las faltas tipificadas en esta Ley, se impondrán sanciones establecidas en esta normativa, sin perjuicio de las sanciones penales que puedan aplicar.

Sanciones para Infracciones leves
Art. 77. La Secretaría de Innovación podrá enviar una advertencia sobre la infracción cometida y demandar una corrección en el tiempo que considere conveniente, así como aplicar una sanción pecuniaria entre tres (3) y diez (10) salarios mínimos del Sector de Comercio y Servicios, cuando sea micro o mediana empresa o como persona natural, la que deberá ser pagado en la Dirección General de Tesorería del Ministerio de Hacienda; impondrá una sanción pecuniaria de veinte (20) salarios mínimos del Sector de

Comercio y Servicios, cuando sea una gran empresa, la que deberá ser pagada en la Dirección General de Tesorería del Ministerio de Hacienda.

Sanciones para Infracciones graves

Art. 78. La Secretaría de Innovación aplicará una sanción pecuniaria entre once (11) y veinte (20) salarios mínimos del Sector de Comercio y Servicios, cuando sea micro o mediana empresa o como persona natural, la que deberá ser pagada en la Dirección General de Tesorería del Ministerio de Hacienda; impondrá una sanción pecuniaria de veinticinco (25) salarios mínimos del Sector de Comercio y Servicios, cuando sea una gran empresa, la que deberá ser pagada en la Dirección General de Tesorería del Ministerio de Hacienda.

Sanciones para Infracciones muy graves

Art. 79. La Secretaría de Innovación aplicará una sanción pecuniaria entre veinticinco (25) y treinta y cinco (35) salarios mínimos del Sector de Comercio y Servicios, cuando sea micro o mediana empresa o como persona natural, la que deberá ser pagada en la Dirección General de Tesorería del Ministerio de Hacienda; impondrá una sanción pecuniaria entre cincuenta (50) y sesenta (60) salarios mínimos del Sector de Comercio y Servicios, cuando sea una gran empresa, la que deberá ser pagada en la Dirección General de Tesorería del Ministerio de Hacienda. En caso de ser uno o más casos reiterados, la Secretaría de Innovación podrá aplicar hasta ochenta (80) salarios mínimos del Sector de Comercio y Servicios o cuatro por ciento (4.0 %) de su última facturación anual antes de impuestos.

Medidas de Protección

Art. 80. Cuando se trate de una infracción muy grave de utilización o cesión ilícita de los datos personales que atente contra los derechos del titular o titulares, tanto la Secretaría de Innovación como la Defensoría del Consumidor podrán requerir a los responsables de los registros de datos personales la cesación de los actos violatorios o cualquier otra medida cautelar que corresponda.

TÍTULO V
DISPOSICIONES FINALES

Aplicación Supletoria Especial
Art. 81. En todo lo que sea aplicable que no se encuentre regulado en esta ley, será aplicable la ley más próxima en materia de información, tal es el caso de la Ley de Acceso a la Información Pública y la Ley de Procedimientos Administrativos, según se el caso, tomando en cuenta sus normas de ejecución, es decir, sus reglamentaciones.

En caso de impugnación de la decisión de la Secretaría de Innovación, se realizará el procedimiento administrativo establecido en la Ley de Procedimientos Administrativos respectivo.

Aplicación Supletoria en caso de conflicto
Art. 82. Las disposiciones de esta ley en lo referente a la protección, gestión y uso de datos personales prevalecerán sobre cualquier otra que la contraríen.
Los agentes de IA deberán informar, en general, en un plazo máximo de 10 días hábiles o en el tiempo que determine la Secretaría de Innovación.

La Secretaría de Innovación será responsable de determinar el grado de gravedad del incidente y podrá, si es necesario, ordenar al agente que adopte medidas y acciones para revertir o reducir los efectos del incidente.

Vigencia
Art. 83. La presente ley entrará en vigor ciento ochenta días después de su publicación.

Decreto Transitorio
Art. 84. Cuando se demande por vía de amparo ante la Sala de lo Constitucional de la Corte Suprema de Justicia, se colocará el tema de Habeas Data, en los conflictos aplicables a esta ley, esta acción se encontrará vigente, hasta que se realicen las reformas a la Constitución y a la Ley de Procedimientos Constitucionales respectivas, para la incorporación del mecanismo de protección de Habeas Data.

DADO EN EL SALÓN AZUL DEL PALACIO LEGISLATIVO: San Salvador, a los N días del mes de HHHHHH del año dos mil XXXX.

VI. CONCLUSIONES

El uso generalizado de la IA promete avances significativos, especialmente, en el ámbito de la salud. Esta tecnología no solo ha contribuido a mejorar las condiciones de vida y aumentar la capacidad para investigar, sino que también a los avances significativos en el tratamiento de enfermedades como el Alzheimer, la obesidad y la anemia falciforme lo que beneficiaría a millones de personas en todo el mundo. Además, se espera que la IA tenga un papel crucial en la gestión de futuras pandemias y el cuidado de embarazos de alto riesgo mediante procesos innovadores de ultrasonidos.

En el campo de la educación, la IA también tiene el potencial de hacer grandes aportes y lograr significativos beneficios, mediante la oferta de tutores personalizados a cada estudiante y el uso de innovadoras herramientas educativas de IA que actualmente se encuentran en desarrollo. Además, puede mejorar la calidad de la educación, en todos los niveles, desde la educación primaria hasta la educación superior, incluyendo la educación continua, o de por vida, para que toda la población conozca sus derechos y deberes en el uso de la IA.

Sin embargo, también, se prevé que la IA tendrá impactos negativos en la vida de las personas naturales y personas jurídicas, generando riesgos significativos y efectos adversos en los ámbitos social, económico, jurídico, político y del medio ambiente. Gran parte del impacto negativo estará asociado con el hermano maligno de ChatGPT y otras amenazas en el dark web por la creación de diversos programas de malware (programa maligno) y sitios web creados para generar una defraudación, estafas sofisticadas, pornografía no consentida, campañas de desinformación, daños mentales y físicos a menores de edad, engaños a personas mayores de edad e incluso dar información para crear armas bioquímicas y de tipo militar.

También, mediante la automatización la IA pondrá en riesgo un alto número de los trabajos repetitivos, lo que causará desempleo y molestar social. En este contexto, la educación continua y la actualización de conocimientos y habilidades serán fundamentales para preservar el empleo y mantener las condiciones de vida alcanzada. Por tanto, la implementación de políticas públicas y empresariales será crucial para establecer medidas que protejan a los trabajadores, asegurando que la IA, además, contribuya al bienestar de los empleados.

Ante las significativas amenazas que presenta la IA, resulta imperativo regular sus procesos de desarrollo, aplicaciones y uso. Dado estos potenciales efectos

adversos derivados de la IA, la UE propuso y aprobó 11 legislaciones, así como la Estrategia sobre Datos, entre 2022 y 2023, con el propósito de regular la transformación digital, garantizar el respeto de los derechos humanos, prevenir todo tipo de discriminaciones y proteger a menores y personas de la tercera edad.

En este mismo sentido, la ONU adoptó, el 21 de marzo de 2024, una resolución para establecer una regulación global con estándares internacionales que garanticen un uso seguro y confiable de la IA, y reducir las desigualdades entre los 193 países miembros. Así mismo, se consideraron las legislaciones de la UE (2024), China (2021-23), Reino Unido, Perú (2023), y proyectos de ley de Brasil y Chile (2021-23). Además, se tomaron en cuenta la Constitución de El Salvador y leyes que deben ser consideradas o reformadas de acuerdo con la Agenda Digital El Salvador 2020-2030.

¿Es posible enseñar ética a las máquinas ante a las amenazas de la IA? Esta pregunta es fundamental, porque se están desarrollando tecnologías que pueden responder afirmativamente. Por lo cual, en la propuesta de Ley de IA, se establece como objetivo promover su uso ético y responsable, donde toda actividad tecnológica se centre en privilegiar a la persona humana, garantizando su confiabilidad, respeto los derechos humanos y fomento del desarrollo económico, social, jurídico, político y ambiental. Este objetivo se logrará mediante la creación de un entorno seguro y confiable que garantice un uso sostenible, transparente, replicable y responsable de la IA.

Con esta propuesta de Ley se pretende establecer un marco jurídico integral para regular y supervisar el desarrollo, comercialización, distribución y utilización de los sistemas de IA, con el objetivo de asegurar la protección de los derechos fundamentales consagrados en la Constitución de El Salvador. Asimismo, pretende garantizar la seguridad, transparencia y rendición de cuentas en el uso de la IA, todo esto, respaldado por claros estándares éticos. Además, la propuesta de Ley incluye medidas destinadas a estimular la inversión y la innovación tecnológica a través de un marco regulatorio claro y predecible.

Finalmente, la Propuesta de Ley de IA de El Salvador puede observarse como un modelo de referencia para otros países que estén en procesos para formular su legislación sobre IA. Esta propuesta debe ser considerada como un paso crucial hacia el futuro de El Salvador, porque demostraría su compromiso con los derechos humanos, la innovación tecnológica y su aspiración de tomar liderazgo en la región.

En la formulación de la propuesta se han tomado en cuenta tanto las legislaciones vigentes como las propuestas de leyes para regular la creación y uso de la IA con el objetivo de ofrecer un modelo que pueda aplicarse en

países que carezcan de esta legislación. No obstante, se enfatiza la necesidad ineludible de realizar consultas con diversos sectores tecnológicos y educativos del sector privado y la sociedad civil para garantizar que la Ley de IA sea fruto de un consenso que regule y controle de manera efectiva el uso de la IA.

Dado que El Salvador no se cuenta con una Ley de Protección de Datos Personales se ha desarrollado una propuesta que complementa la Ley de IA, adaptada al nuevo entorno tecnológico en general y al de la IA en particular. Esta propuesta para la protección de datos personales también puede ser útil para actualizar o reformar leyes similares en países que ya cuentan con legislación en este ámbito.

ANEXOS

Anexo I. Historia de la Inteligencia Artificial

El concepto de la inteligencia artificial (IA) se origina tras la publicación del artículo *A Logical Calculus of Ideas Immanent in Nervous Activity* (Un cálculo lógico de ideas inmanentes a la actividad nerviosa) de Warren McCullochy y Walter Pitts en 1943. En ese trabajo, presentaron el modelo de neuronas artificiales para la creación de una red neuronal, que se considera el primer trabajo del campo de inteligencia artificial, término que aún no se conocía en esos momentos (Sobrino y Barro, 1993).

En 1950, Alan Turing publicó el artículo *Computing Machinery and Intelligence* (Maquinaria computacional e inteligencia), donde introdujo por primera vez al público el concepto de lo que hoy se conoce como el *Test de Turing,* conocido inicialmente como Imitation Game. Este test sigue utilizándose para determinar si en la interacción entre un ser humano y una máquina, la inteligencia de esta última puede considerarse similar o igual a la del ser humano (Santander Universidades, 2023). El *Test de Turing* continúa siendo una prueba objetiva y fiable de la IA. En 1951, Marvin Minsky y Dean Edmonds, estudiantes de la Universidad de Harvard, crearon el primer ordenador de red neuronal, *SNARC* (*Stochastic Neural Analog Reinforcement Calculator* - Calculadora de refuerzo analógico neuronal estocástico).

Luego, en 1952, Arthur Samuel desarrolló un software que podía aprender a jugar ajedrez de forma autónoma. Posteriormente, en 1956, los científicos informáticos Marvin Minsky, John McCarthy y Claude Shannon organizaron a una conferencia en Dartmouth, una de las instituciones académicas más importantes del mundo y miembro de la Ivy League, en la que reunieron a los pioneros involucrados en el emergente campo de la IA. Durante este evento, Minsky, McCarthy y Shannon presentaron la lógica teórica que habían desarrollado, la cual se considera como el primer programa de IA diseñado a resolver problemas de búsqueda heurística (arte o la ciencia del descubrimiento).

Allí también señalaron que «cada aspecto del aprendizaje o cualquier otra característica de la inteligencia puede, en principio, describirse con tanta precisión que se puede hacer una máquina para simularlo» (cita proporcionada por Sarah Romero, 2023). En esta conferencia, que se denominó *Research Project on Artificial Intelligence* (El Proyecto de Investigación sobre Inteligencia Artificial), se concibió como campo de investigación y trabajo la IA, evento

cuando McCarthy utilizó por primera el término inteligencia artificial (Darthmouth Conference, 2014). Luego, en 1957, McCarthy cofundó con Marvin Minsky, el Laboratorio de Inteligencia Artificial del MIT. Entre los primeros proyectos de IA desarrollados en 1959 destacan Logic Theorist, de Allen Newell y Herbert A. Simon y el General Problem Solver, creado por Simon, Shaw y Allen Newell, con el objetivo de crear una máquina capaz de resolver prácticamente cualquier problema complejo, por lo que es considerado el primer programa útil de IA (Romero, 2023).

Pasado algún tiempo, Arthur Samuel acuñó el término *Machine Learning* en IBM, en 1959, al mismo tiempo que John McCarthy y Marvin Minsky fundaron en el *Massachusetts Institute of Technology* (Instituto de Tecnología de Massachusetts) el *MIT Artificial Intelligence Project* (Proyecto de Inteligencia Artificial), donde se condujo la primera investigación coordinada de IA n el Proyecto de Inteligencia Artificial. Luego, John McCarthy también creó el «*AI Lab*» en la Universidad de Stanford posteriormente en 1963 (Romero, 2023).

A fines de la década de los 50, Roger Easton, físico que trabajaba en el Laboratorio de Investigación Naval de Estados Unidos, contribuyó al desarrollo del Sistema de Vigilancia Espacial Naval y el Proyecto *Vanguard* (Vanguardia), que «lanzó el primer satélite con energía solar y creó el primer sistema para detectar y rastrear todo tipo de objetos en la órbita terrestre» (Carsync.com, 2021, párr. 7). Los buenos resultados que logró Easton en el monitoreo de astronaves, navegación y tecnología del tiempo, con la participación de Ivan A. Getting y Bradford Parkinson sentaron las bases de NAVSTAR, dando origen a lo que hoy se conoce como el GPS *(Global Positioning System)* Sistema Global de Posicionamiento.

En los años siguientes, surgieron dudas sobre los avances en la investigación de la traducción automática. En 1966, el gobierno de los EUA ordenó al *National Research Council* (Consejo Nacional de Investigación) realizar un análisis de la situación. Este informe, conocido como AL-PAC (*Automatic Language Processing Advisory Committee*), señaló que había pocos avances en la investigación de la traducción automática, la cual tenía como objetivo traducir simultáneamente el idioma ruso durante la Guerra Fría. Ante la falta de progreso, la recomendación principal fue dejar de invertir tiempo y dinero en el proyecto. Como resultado, muchos otros proyectos relacionados que también recibían financiamiento estatal se cancelaron.

Siete años después, en 1973, el parlamento del Reino Unido solicitó al matemático y profesor Sir James Lighthill una evaluación sobre la situación de la investigación en IA en el país. En su evaluación, conocida como el informe *Lighthill*, señaló el fracaso de la investigación en IA en el Reino Unido y la incapacidad para lograr los grandes objetivos establecidos. De manera similar

a lo ocurrido en EUA, los recortes presupuestarios llevaron a una disminución en el número de proyectos de investigación en IA, lo que dio lugar a lo que se conoce como el «primer invierno de la IA» que se extendió hasta 1980 (Romero, 2023).

Sin embargo, en medio de las dudas sobre los avances en IA, en 1966 Joseph Weizenbaum, del MIT, desarrolló ELIZA, considerado el primer chatbot del mundo. Este innovador programa logró incorporar el procesamiento del lenguaje natural humano con el propósito de enseñar a las computadoras a comunicarse con los seres humanos en su propio lenguaje, sin necesidad de una programación en código. Luego, en 1969, Marvin Misnky, también del MIT escribió el libro *Perceptrones*, que presenta las teorías sobre autómatas, inteligencia artificial y reconocimiento de patrones, e incorpora sus aplicaciones en diversas disciplinas, incluida la psicología. Este trabajo fue fundamental para el desarrollo y análisis de las redes neuronales artificiales (National Geographic, 2020).

El «primer invierno de la IA» terminó con la creación de R1 (posteriormente denominado XCON (abreviatura de *eXpert CONfigurer*) por *Digital Equipment Corporations.* Este sistema de producción basado en reglas, desarrollado por John P. McDermott en 1978, se empleó para gestionar los pedidos de sistemas de computadoras VAX fabricadas por la *Digital Equipment Corporation*, de acuerdo con necesidades específicas de cada cliente. Los excelentes resultados obtenidos generaron un marcado incremento en las inversiones en este campo durante más de una década (Romero, 2023).

En medio de este auge, EUA y Japón realizaron grandes inversiones en la investigación de la IA. En este contexto, las empresas de este sector invirtieron más de US$1,000 millones por año en sistemas expertos. En este contexto, se crearon las máquinas Lisp (*LISt Processor*, Procesamiento de listas) para satisfacer una fuerte demanda, la cual desafortunadamente se desplomó en 1987 debido a la aparición de alternativas más económicas. Este suceso llevó a lo que se conoce como el «segundo invierno de la IA». Nuevamente, los gobiernos de EUA y Japón dejaron de lado los proyectos de investigación en sistemas expertos.

No obstante, en medio del «segundo invierno», en 1979, Hans Moravec presentó el *Stanford Cart*, uno de los primeros vehículos autónomo controlados por computadora. Este vehículo logró atravesar una sala con sillas y circunnavegar el Laboratorio de IA de Stanford (National Geographic, 2020). Por otra parte, es relevante destacar que los sistemas expertos se basaban en IA simbólica. Sin embargo, en la década de los 80 surgió un nuevo enfoque conocido como «conexionismo», el que considera que el comportamiento inteligente puede modelarse para representar una estructura y funcionamiento similares a las

redes neuronales del cerebro. A pesar de que las primeras redes neuronales tenían capacidades limitadas, el progreso logrado permitió que a partir de 1986 se lograra las primeras integraciones de redes de varias capas más complejas, lo que condujo a un renacimiento del interés en la IA (Romero, 2023).

El progreso continuó, pero no fue hasta 1997, cuando se dio un acontecimiento determinante, en la medida que la IA Deep Blue de IBM logró ganarle a Gary Kasparov, el campeón mundial de ajedrez. La máquina le había ganado al hombre, evento que permitió un nuevo resurgimiento de las investigaciones en inteligencia artificial (National Geographic, 2020).

Sin embargo, pasada una década, Google logró grandes avances a partir de 2008 en el reconocimiento de voz y pudo utilizar esa función en sus aplicaciones para smartphones. Cuatro años más tarde, en 2012, Andrew Ng alimentó una red neuronal con 10 millones de vídeos de YouTube, que utilizó como una base de datos de entrenamiento. Gracias al inicio del Deep Learning, esta red neuronal pudo aprender a reconocer un gato sin que se le enseñara lo que es un gato. Este fue el comienzo inicio de una nueva etapa para el Deep Learning (Romero, 2023).

Luego, en 2016, se dio un nuevo triunfo de la IA sobre el ser humano, cuando el sistema AlphaGo de Google *DeepMind* venció a Lee Sedol, el campeón de Go. Así la IA también comenzó a ser parte de los videojuegos, utilizando el *DeepMind AlphaStar*. Además, el uso de *Deep Learning* y el *Machine Learning* también se introdujo en todos los sectores económicos, sociales, políticos, jurídicos, de seguridad y ambientales mediante el uso de un gran número de aplicaciones, acercando el concepto de una IA de uso general a ser cada vez más real (Romero, 2023).

Google también hizo innovadores aportes en este campo al presentar Alexa, en 2016, considerado el primer asistente de voz, al que se sumó como competencia el Google Home, puesto que ambos tienen capacidades para responder a órdenes como elegir música, responder preguntas y controlar dispositivos. También esta empresa lanzó Google Allo, una aplicación de mensajería móvil que permite aprender del usuario y adaptarse a sus costumbres. Por su parte, IBM presentó a Watson, un sistema informático que creó en conjunto con General Motors, el cual es capaz de memorizar las preferencias del conductor, estudiar los datos e identificar patrones en sus preferencias y decisiones (Gestión, 2016).

Y el rápido progreso innovador en el campo de la IA continuó, en 2017, en busca que los ordenadores sean tan inteligentes o más que las personas, con capacidades para pensar y razonar. En este devenir, se tiene que en 2017 la IA cada vez se posiciona más como parte de la vida de los seres humanos y con

ella se generan corrientes de opinión, que luego, al consolidarse en las redes, se transforman en opinión pública. Además, cada vez hay más actividades de riesgo o de alta dificultad que se están realizando con mayor facilidad utilizando IA (Pieczynski, 2017).

Ya en 2018, se amplía y profundiza el uso de IA en áreas como el *blockchain*, Internet de las Cosas (IoT), ciberseguridad, la nube, y la de los asistentes virtuales. También, aumenta el uso de chatbots que utilizan IA para interpretar con mayor claridad lo que una persona desea expresar ya sea por medio telefónico y de un texto en la computadora. Además, hay cada vez más aplicaciones innovadoras contribuyen a mejorar el trabajo que se realiza en áreas como investigación, salud, educación y marketing, entre otras. A esto se suman las nuevas herramientas e instrumentales utilizadas en estudios y aplicaciones de biología molecular, en los ámbitos de metagenómica o la revolución de la ingeniería genética CRISPR-Cas9 que han servido para mejorar la producción agrícola, producir biocombustibles y facilitar la degradación de los compuestos que hay en los plásticos (Europapress.es, 2018).

En 2019 comienzan a ser cada vez más utilizados los asistentes virtuales que son más humanos, en tanto que, además de facilitar diversos trabajos también interactúan con quienes los están utilizando e incluso, les permite establecer una relación de compañía e incluso de amistad. Además, la aplicación del *deep learning* continúa mejorando y permite entrenar a las máquinas para resolver problemas cada vez más difíciles. Por su parte, el uso del blockchain, que se aplicaba fundamentalmente en el ámbito financiero, es cada vez más utilizado en diversas empresas como medio para mejorar la seguridad informática y proteger la información (Treviño, 2023).

Los avances en IA continuaron y en 2019 la empresa OpenAI presentó la mano robot Dactyl, máquina entrenada con aprendizaje por refuerzo, que pudo resolver el cubo de Rubik con rapidez y destreza extraordinarias. Además, en febrero dio a conocer el sistema Generative Pre-Training (GPT) para generar texto sintético sin supervisión y de manera automática, ante lo cual no hubo acceso al público por considerarse muy peligroso para la humanidad. No obstante, en noviembre dieron a conocer el GPT-2 de libre acceso al público. Por su parte, Samsung lanzó un sistema con capacidades para transformar imágenes faciales y, a partir de ellas, crear vídeos falsos, utilizando redes generativas antagónicas o Generative Adversarial Networks (GAN), y que también permiten la creación automática de textos y las falsificaciones de audios de alta calidad. En este contexto toman fuerza el concepto de *DeepFake* (ultra falso) y los debates sobre la ética en el uso de la IA (DAIL, 2019).

En el año 2022 los avances en IA fueron altamente disruptivos, especialmente por el ChatGPT, que se dio a conocer y puesto a disposición del público el

30 de noviembre de ese año, al cual se le puede hacer preguntas o dar una instrucción sobre cualquier tema y tener respuestas altamente acertadas en tiempo real. Esta herramienta ha tenido tres versiones y su cuarta versión se estrenó en 2023 (López, 2022).

Los avances en el campo de la IA continuaron en 2023, entre los que destacan los relacionados con la IA generativa que son técnicas de aprendizaje profundo (deep learning) y el uso de grandes bloques de datos que mejoraron sus capacidades para crear nuevos contenidos en textos, imágenes, vídeos y música, destacando principalmente ChatGPT y Dall E, entre otras. Pero no todo es positivo ante estos avances, porque en torno a ellos se han abierto importantes debates éticos y legales. No es para menos, por ejemplo, el cantante Bad Bunny mostró su molestia porque su voz se imitó con tecnología artificial para interpretar una canción (Velázquez, 2023).

OpenAI con su modelo de IA ChatGPT remeció el mercado. En respuesta, Google presentó aceleradamente a Bard como una alternativa, el cual aún no había sido totalmente desarrollado y que no causó mayor reacción. Google siguió trabajando en este sistema y a inicio de febrero presentó a Gemini como su modelo definitivo, el que está disponible en tanto en la web como para móviles. Por su parte, Microsoft lanzó Copilot en septiembre de 2023 (Limón, 2024).

Al entrar en el sitio web de Google, la invitación para usar Gemini dice al usuario «Potencia tu creatividad y productividad. Chatea para comenzar a escribir, planificar, aprender y mucho más con la IA de Google». Por ahora, Gemini está solo en inglés, luego seguirán los idiomas japonés y coreano y, posteriormente, el español. Gemini no solo busca ser un sustituto del buscador, sino también «un verdadero asistente de inteligencia artificial, conversacional, multimodal y más útil que nunca», según Sissie Hsiao, vicepresidenta de Google (Limón. 2024, párr. 3).

En adición, Open AI dio a conocer *Sora* una herramienta transformadora para crear vídeos que realiza el trabajo solo con darle una descripción de lo que se desea que se reproduzca en la pantalla, utilizando AI para realizarlo. A *Sora* se le puede solicitar el vídeo tal como lo desea el usuario, el que se creará utilizando IA generativa, los cuales se pueden reproducir de manera completa o extenderlos para que tengan mayor duración (Jiménez, 2024).

Sin embargo, las tecnologías de IA siguieron progresando aceleradamente y las nuevas aplicaciones innovadoras siguen irrumpiendo con fuerza en el mercado. El periodista J. Barrera (2024) destaca en su artículo Las 10 apps de inteligencia artificial más populares y fáciles de usar, que ellas están transformando las empresas porque mejoran su eficiencia y capacidades para la toma de decisiones y están revolucionando la forma cómo los usuarios interactúan con ella, en

tanto que son utilizadas a diario en diversas actividades. Ante este avance, Barrera enumera las diez aplicaciones de IA que lideran el mercado y que tiene alta demanda, basado en información publicada en tecnología gitmind.com:

1. Chatgpt: disponible desde fines de 2022, es una aplicación que permite mantener conversaciones enviando un texto y preguntas que responde de manera instantánea, al tiempo que puede hacer recomendaciones y sugerencias y traducir textos.

2. Amazon Alexa: asistente virtual de Amazon que por medio de reconocimiento de voz permite responder a los pedidos de los usuarios. También sirve para reproducir música, establecer alarmas y administrar electrodomésticos del hogar, entre otros. También puede proporcionar información sobre el clima, las noticias y otros temas.

3. GitMind: aplicación con capacidades para crear mapas conceptuales o mentales mediante el uso de IA, lo cual que les permite a los usuarios visualizar sus ideas y pensamientos de manera sistematizada, en cualquier tema que se elija (tiene una versión gratuita limitada y otra pagada).

4. Google Assistant: permite realizar búsquedas en internet por voz en Google, para facilitar a los usuarios realizar tareas diarias como recordatorios, llamadas a realizar, enviar mensajes, obtener diversos tipos de noticias, utilizando pantallas, altavoces y teléfonos inteligentes. Una ventaja adicional es que está conectado con otros servicios como Google Maps, Google Calendar y Google Photos.

5. Faceapp: está diseñada para editar fotos y con efectos como suavizado, envejecimiento, reemplazo de género, cambio expresiones faciales, entre otras, y compartirla con amigos y seguidores en redes sociales (tiene una versión gratuita limitada y otra pagada).

6. Quillbot: permite a sus usuarios parafrasear y mejorar un escrito para tener mayor calidad y claridad al sugerir sinónimos, revisión gramatical y de ortografía (tiene dos versiones gratuitas y cinco premium pagadas).

7. Elsa: por su nombre en inglés *English Language Speech Assistan*t, es una tecnología de reconocimiento de voz que se diseñó en 2015, la cual, mediante el uso de IA permite mejorar las habilidades de expresión en inglés con diversos acentos, así como reconocer a los no nativos. Su método de enseñanza se adapta según el nivel de cada usuario.

8. Databot: es una aplicación de IA que permite comunicarse con los clientes mediante el reconocimiento de voz, al convertir un texto a voz y viceversa, así como enviar mensajes, establecer alarmas y enviar información.

9. Canva: es una de las aplicaciones de IA de mayor uso en estos momentos, que sirve para crear diversos tipos de publicaciones visuales. También, ofrece opciones para redactar frases y presentar esquemas mediante su función Magic Write, todo lo cual se puede presentar en más de 100 idiomas.

10. Otter.AI: le permite al usuario grabar y transcribir reuniones y todo tipo de conversaciones, las cuales también las puede transcribir para luego enviarse como archivos de audio y video utilizando el software.

Una de las últimas novedades es el «AI Pin» (broche IA) de la empresa Humane, desarrollado junto con Microsoft y OpenAI, es un asistente virtual portátil que se prende en la ropa. Si bien no tiene pantalla, cuenta con un micrófono, altavoz, un panel táctil, una cámara para guardar información visual y herramientas para tener datos sobre calorías de un alimento, traducciones en tiempo real y toras funciones como lo hace ChatGPT. Con el AI Pin se busca dar mayor valor a las experiencias «humanas» sobre las digitales, mediante el menor uso de dispositivos con pantalla (Peralta, 2024).

Sin embargo, a mediados de mayo de 2024, OpenAI se presentó una nueva y sorprendente innovación el GPT-4º, que representa un avance significativo en la evolución del modelo original GPT-4. El GPT-4o ofrece un procesamiento multimodal que le permite al usuario relacionarse con el sistema no solo escribiendo un texto, sino que, ahora, mediante el envío de una o más imágenes, audios y vídeos, brinda a los usuarios una experiencia más enriquecedora y versátil. Las innovaciones del GPT-4o trascienden los límites convencionales al ofrecer una funcionalidad avanzada que incluye la capacidad de responder con distintos tonos de voz (de Rosa, 2024, párr. 1). «Este revolucionario modelo, además de comunicarse verbalmente, también es capaz de reír, cantar e incluso mostrar diferentes estados de ánimo. Estas nuevas características harán que la interacción con el GPT-4o sea aún más envolvente y personalizada, estableciendo un nuevo estándar en la comunicación con sistemas de inteligencia artificial» (párr. 2).

Además, el GPT-4o también se destaca por su mayor capacidad de memoria que le habilita para aprender de conversaciones anteriores con los usuarios. «Este avance le permite no solo recordar interacciones pasadas, sino también ofrecer una experiencia más personalizada y coherente. También, el modelo es capaz de realizar traducciones en tiempo real de otros idiomas, ampliando

así su utilidad y versatilidad para satisfacer las necesidades de una base de usuarios global y diversa» (párr. 5). «El mundo sigue evolucionando ante los innovadores descubrimientos, se vive un cambio de época, que transformará de manera determinante la vida de la mayor parte de la población mundial» (párr. 5).

Ante todos los avances y el uso masivo de IA ahora ella se utiliza prácticamente todas las áreas de investigación y de trabajo. Por ejemplo, Javier Sampedro (El País, 2024) escribió sobre *Doctor Google*, al que presentó como un *software* entrenado para entrevistar a pacientes que «ha demostrado que supera a los médicos de atención primaria diagnosticando enfermedades respiratorias y cardiovasculares» (párr. 2). Luego agrega que el nombre de esta aplicación es AMIE (explorador articulado de inteligencia médica, por sus siglas en inglés), el que está aún en experimento.

Si bien Google asegura que con esto no se busca sustituir al médico de familia, sino complementarle y «democratizar la medicina» (párr. 3). Obviamente, este tipo de avance en el campo de salud y en sus innumerables subáreas, así como en el trabajo, en general, educación, arte, ciencias, relaciones personales y de empresas, y en asuntos de defensa requerirán ser normados y supervisados estableciendo legislaciones con alta precisión que debe estar en procesos continuos de revisiones y ajustes ante los vertiginosos cambios e innovaciones disruptivas de la IA.

Por su parte, ante el avance de la IA el Fondo Monetario Internacional (FMI) envió un importante mensaje, al señalar que es necesario crear entornos seguros y responsable mediante la formulación de sólidos marcos de regulación que contribuyan a mantener la confianza pública. En este sentido, la Unión Europea promulgó en 2023 la primera ley sobre regulación de la IA en el mundo (Georgieva, 2024).

Consecuentemente, las economías de países emergentes y en desarrollo, también, deben considerar de manera especial la necesidad de tener sólidos marcos legales, tanto para proteger a personas naturales y empresas como para estimular las inversiones en infraestructura digital y en formación de competencias digitales en sus trabajadores/as, para que haya prosperidad para todos. Además, el FMI también advierte sobre la pérdida de empleos que causará la IA en su publicación *Artificial Intelligence and the Future of Work* (La inteligencia y el Futuro del trabajo, Cazzaniga et al., 2024). En esta publicación señala que alrededor del 40 % de los trabajadores en todo el mundo tienen ocupaciones de alta exposición por la IA: en las economías avanzadas alrededor del 60 %, en las economías emergentes 40 % y la de bajos ingresos 26 %, lo cual tendrá implicaciones macroeconómicas potencialmente importantes.

Además, la SEC, *Securities and Exchange Commission* (Comisión de Bolsa y Valores) de los Estados Unidos de América que tiene la responsabilidad de regular los mercados y protege los inversores en este país, después de oponerse alrededor de una década, aprobó el 10 de enero de 2024 los cambios normativos que permiten que el ETF de bitcoin al contado se cotice y negocie en los intercambios respectivos con esta criptomoneda en los mercados financieros (Hajric y Greifeld, 2024).

Anexo II. Predicciones futuristas sobre la evolución tecnológica de la IA

Ante el sostenido y cada vez más vertiginoso avance de la IA es importante revisar las predicciones futuristas sobre la evolución de la tecnología hacen los grandes futurólogos en el mundo, como son Raymond Kurzweil, Bill Gates, Elon Musk y Amy Webb.

Raymond Kurzweil, experto en tecnología de sistemas y de IA, es actualmente director de ingeniería de Google, se le considera un visionario de la IA y ha realizado múltiples predicciones futuristas, de las cuales ha acertado alrededor del 86 % de ellas. Con su libro *La era de las máquinas inteligentes* (1990) anticipó la rápida expansión del internet, aunque tuvo múltiples críticas porque su visión no fue totalmente comprendida. Kurzweil es el creador de la Universidad de la Singularidad (más comúnmente llamada Singularity U o SU, por sus siglas en inglés), en Silicon Valley (California).

Mas adelante escribió el libro *La era de las máquinas espirituales* (*The Age of Spiritual Machines*, 1998), en el que presenta su visión sobre el posible futuro de la IA y su capacidad para controlar el universo en el siglo XXI, en tanto que no habrá diferencias entre el ser humano y máquina, que resulta de una fusión de la sensibilidad humana con la IA que superará la velocidad que responde el cerebro humano y lograrán tener atributos propios del ser humano. Ese mundo se caracterizará por las relaciones de los seres humanos con personalidades automatizadas en el aula de clase, el trabajo y la vida personal, todo generado por la IA.

También, destaca el libro *La singularidad está cerca*, en el que Kurzweil visualiza que los cambios tecnológicos se darán cada vez con más frecuencia y vertiginosidad, en donde la inteligencia del ser humano será trillones de veces mayor y más potente por su dependencia de las computadoras. El mundo entrará a una nueva era de la civilización. En el campo de la salud, Kurzweil predice que la evolución tecnológica les permitirá a los seres humanos superar el envejecimiento y las enfermedades; y en el ámbito social visualiza que se terminará con el hambre en todo el mundo y la pobreza.

Entre las predicciones de Kurzweil destacan, según Resiliente Digital (2023), las siguientes:

- En 1990, un ordenador podría derrotar a los campeones mundiales de ajedrez hacia el año 2000, lo cual se dio.

- Para principios de la década de 2000, habrá extremidades exoesqueléticas que le permitirían caminar a los discapacitados, lo que efectivamente se ha logrado e incluso superado.

- En 2005 predijo que, en la década de 2010, habría aplicaciones informáticas con capacidad para hacer traducciones de idiomas en tiempo real, las que son actualmente de amplio uso.

- Los nanobots (pequeños robots de 50 a 100 nanómetros de ancho) serán los protagonistas de lograr revertir la edad del ser humano, en la medida que podrán reparar el cuerpo humano a nivel celular, logrando que sean inmunes a enfermedades y al envejecimiento e incluso podrían llegar a cargar su conciencia en forma digital, logrando la inmortalidad en torno a 2023 (Romero, 2023).

- En la década de los 20 los seres humanos se relacionarán con las máquinas de una forma cada vez más similar a como se relacionan con otro ser humano; y los asistentes virtuales, serán ampliamente utilizados.

- Para 2029, los ordenadores tendrán una inteligencia similar la del ser humano y en el año 2030 la realidad virtual será muy similar a la real.

- Utilizando la Ley de Moore, las máquinas alcanzarían un nivel de inteligencia similar la del ser humano en 2029 y llegará a superar la inteligencia humana en un billón de veces en 2045 (National Geographic, 2020).

- Antes de 2030 habrá un uso masivo de robots domésticos e incluso algunas personas tendrán una relación muy personal con estos asistentes virtuales.

- Hacia fines de la década de los 30 el ser humano podrá cargar la mente/consciencia.

- En 2040 la inteligencia no biológica será mil millones de veces más capaz de que la biológica.

- En torno a la década de los 40 se podrá obtener comida de la nada y cualquier objeto se podrá hacer aparecer en el mundo físico.

- Hacia 2045 la inteligencia del ser humano se habrá multiplicado por mil millones, lo que le permitirá vincularse de forma inalámbrica con la nube a través del neocórtex.

Por su parte, para Bill Gates, 2024 muestra aspectos positivos y negativos. Por ejemplo, señala que «Hay un riesgo relacionado a nivel global, una carrera armamentística donde la IA puede usarse para diseñar y lanzar ciberataques contra otros países» (Marca, 2023, párr. 3; y Foto 1).

Esta situación puede generar algo similar a una Guerra Fría mundial, porque «cada gobierno quiere tener la tecnología más poderosa para así poder detener ataques de sus adversarios. Este inventivo de desarrollo de no permitir a nadie encabezarlo puede llevar a una carrera para crear nuevas y peligrosas ciberarmas» (párr. 4). Todo podría ser peor, porque «podrían acabar con miles o millones de personas» (párr. 5), y podrían destruir algunos de los sistemas que tienen las naciones.

Foto 1: Soldado no carga fusil sino una tablet para guerra cibernética
Fuente: Freepik.

Por el lado positivo del aporte de la IA Gates destaca en la publicación en su blog GatesNotes, bajo el título *The road ahead reaches a turning point in* 2024 (El camino por recorrer llega a un punto de inflexión, 2023) que, en 2024, los avances en esta área tecnológica tendrán un impacto directo en el desarrollo humano, por sus aportes en la educación, en tanto se podrá ofrecer tutores personalizados a cada estudiante, mediante el uso de herramientas educativas de IA que están en estos momentos en prueba, como son Khanmigo y MATHia, que estarán disponibles en unos años, sea donde sea que estén viviendo los estudiantes. Y en salud, destaca los avances logrados para tratar, por ejemplo, el Alzheimer, la obesidad y la anemia falciforme, lo que permitirá mejorar la vida de millones de personas en el mundo. Asimismo, para 2024 Gates visualiza que la IA permitirá tener mejor respuesta a futuras pandemias, utilizar de mejor manera para contrarrestar la resistencia a los antibióticos ante su uso prolongado y atender de mejor manera los embarazos de alto riesgo mejorando los procesos de ultrasonidos impulsados por la IA.

La visión de Gates señala que la IA acelerará los avances y descubrimientos tecnológicos serán cada vez más rápidos vertiginosos, todo lo cual transformará la vida de los seres humanos. Por esto, desde ya advierte que «Si aún no has descubierto cómo sacar el máximo partido de la IA, no eres el único» (Gates, 2023, párr. 6), destacando que es difícil de romper en el trabajo los viejos hábitos, pero que es algo que se dará inexorablemente. En este contexto, la IA puede mejorar las condiciones en el ámbito laboral, pero también puede perjudicar a muchos trabajadores/as, donde el gran desafío será cómo protegerlos/as.

También, Gates señala que el mundo ha mejorado y es más productivo por los considerables avances de las tecnologías de la información, donde las economías que han tenido los mayores avances son las que han atenido industrias innovadoras que tuvieron la capacidad para responder a las cambiantes necesidades de la sociedad. No obstante, considera que el mundo efectivamente verá un boom tecnológico masivo hacia fines de esta década, de modo que en los próximos años se marcará una nueva era de la IA.

Sin embargo, ante los avances tecnológicos, Gates muestra preocupación porque hay una brecha en la capacidad de la población para lograr un uso significativo de la IA, porque considera que esta tecnología que tiene un alto potencial para reducir las inequidades, su uso en sí mismo conlleva inequidades. Mientras en países de altos ingresos, como EUA, su población estaría tomando entre 18 y 24 meses para alcanzar niveles significativos de uso de IA, en países de ingresos bajos, como es el caso de algunos países africanos, esto podría tomar alrededor de tres años.

Por su parte Elon Musk, en respuesta a una publicación del Wall Street Silver comenzó con una pregunta: «¿Podemos tener un año normal en 2024? (...) ¿No nos merecemos eso después de cuatro años de locura?» (Musk, 2023, párr. 2). Luego predijo que el «2024 será aún más loco». Guardando cierta coincidencia con lo expresado por Gates, los avances en IA serán monumentales en 2024.

La reconocida futurista Amy Webb, CEO del *Future Today Institute* (FTI), presentó en la Carta Anual 2024 del FTI (Webb, 2024), diez temas clave que deberían estar en el radar para el año 2024:

1. Se espera que el concepto de llevar una idea desde lo abstracto a lo concreto genere una ola de nuevas herramientas de IA. Estas herramientas permitirán a individuos o equipos idear y perfeccionar continuamente el trabajo hasta obtener un marco concreto, especificaciones técnicas o resultados similares. Con esta herramienta los usuarios podrán desarrollar una idea básica utilizando la IA para crear «una historia rica y una experiencia visual atractiva».

2. Se dará el inicio de un *criptoinvierno*, en un mercado de criptomonedas, caracterizado por fluctuaciones volátiles. Sus transacciones son difíciles de rastrear, porque este mercado «no está regulado de manera uniforme y ha causado más de una manía financiera». Para que estos activos financieros permanezcan en el largo plazo, requerirán tanto un apoyo institucional para construir una adecuada infraestructura como una masa crítica de adeptos; de lo contrario, «la manía dará paso a la desilusión y, en última instancia, al desinterés».

3. «Hacer sostenible la sostenibilidad», dada las intenciones de las empresas más grande del mundo de tener como objetivo cero emisiones netas para 2030, algo que no ha demostrado grandes avances, como es el caso de la contención del calentamiento global desde 2018. La IA puede hacer grandes aportes para avanzar con mayor determinación al cumplimiento de este objetivo.

4. «Los algoritmos son nuestra fuerza laboral y es posible que necesiten licencias profesionales», considerando que los sistemas automatizados continuarán dando los servicios que dan «los trabajadores de cuello blanco» y «los sistemas de IA vayan asumiendo trabajos de oficina más exigentes, es posible que los organismos reguladores les exijan una licencia profesional en tecnología para poder realizar su trabajo, así como un examen de ética», para garantizar que el sistema de IA va a saber «cómo tomar una decisión honesta y basada en principios».

5. «Los *wearables* (usables) están de vuelta», con lo que se dará inicio a «una nueva era de respuestas visuales y de voz», donde los teléfonos inteligentes dejarán de existir para dar paso a los «*wearables* omnipresentes... impulsados por sistemas de IA multimodal», esto es, por un ecosistema multidispositivo que pueda combinar imágenes y otras formas de datos con texto para crear respuestas en múltiples modos que permitan, incluso, «tener experiencias altamente personalizadas con IA, que llevaríamos en el cuerpo y que responderían en tiempo real».

6. «La inteligencia organoide (IO) dará forma tanto a la informática como a la geopolítica». Ya se creó este nuevo campo, que se estima será la próxima frontera de la bioinformática. La IO «utiliza materiales biológicos –en la mayoría de los casos, células cerebrales humanas– para el procesamiento de la información, aprovechando sus capacidades inherentes... (lo cual) representa un paso importante en el aprovechamiento de la eficiencia natural del cerebro para aplicaciones de IA». Estados Unidos y China están compitiendo para ganar la supremacía cuántica, junto con los semiconductores, los componentes 5G y los estándares 6G. ¿Qué pasaría si hubiera una carrera por ganar la computación biológica?

7. «Las grandes tecnológicas vuelven a enfrentarse a la justicia, y esta vez podrían tener éxito», y lograr arreglos «para mantenerse inmunes a la responsabilidad legal cuando se trata de contenidos de los usuarios» (la Sección 230 de la *Communications Decency Act*). Sin embargo, en 2023 "el Tribunal Supremo (de EUA) acordó revisar si las leyes estatales que buscan regular Meta, Google, TikTok y otras plataformas de medios sociales violan la Constitución de Estados Unidos. Los estados más adelantados son Texas y Florida, y como la IA generativa juega un papel importante en la generación de contenidos, se considera que les será difícil a las empresas tecnológicas sostener que son «solo una plataforma para el discurso de otras personas».

8. «La biotecnología crea accidentalmente un nuevo sistema de castas genéticas.». En 2023 hubo grandes avances biotecnológicos que permitirán brindar nuevas terapias de manera masiva. En efecto, la Administración de Alimentos y Medicamentos de los EUA (FDA) aprobó «la primera terapia de edición genética destinada a tratar enfermedades humanas, dando luz verde a dos terapias génicas para personas mayores de 12 años que luchan contra el tipo más grave de anemia falciforme». Otro caso es el de las empresas farmacéuticas que han creado medicamentos que ayudan a perder peso, por lo que estarán disponibles «fármacos aún más potentes que suprimen el apetito y también ayudan a descomponer el azúcar y la grasa». No obstante, es preocupante que estas innovaciones biotecnológicas de vanguardia crearán mayores desigualdades en la atención sanitaria, lo que genera preguntas sobre la ética y la equidad.

9. «Un mundo de nuevos materiales», visión que comenzó a materializarse a partir de 2003, cuando DeepMind introdujo silenciosamente la herramienta conocida como *Graphical Networks for Material Exploration* (GNoME), la que podría acelerar los descubrimientos, considerando «que ya ha predicho las estructuras de 2.2 millones de nuevos materiales. Por tanto, en 2024 se espera que haya muchos anuncios de nuevos materiales»

10. «Elecciones y desinformación involuntaria». En 2024 habrá un periodo electoral global desafiante, puesto que «habrá más de 70 elecciones, en las que votarán alrededor de 4,200 millones de personas», más de la mitad de la población mundial. Dado el avance tecnológico hará disponible más herramientas para «manipular intencionadamente a los votantes» mediante desinformación creada con contenido sintético de alta calidad (*deepfakes*) y difundirla por toda la web. A esto se agrega la desinformación involuntaria, que resulta del envío de contenidos creados con buena intención pero que, considerando que los sistemas contienen gran cantidad de datos deficientes, se termina compartiendo información errónea.

Si bien todos estos futurólogos coinciden en los grandes avances que tendrá la IA en 2024 y los aportes beneficiosos que harán para mejorar la productividad, la salud, educación, investigación, entre otras áreas, también, están las amenazas que pueden afectar negativamente todas las áreas de trabajo que existen.

Anexo III. Legislación en la Unión Europea

Los primeros pasos para legislar sobre la IA los dio la UE y tras diferentes estudios y consultas abiertas se lograron aprobar o actualizar diversas leyes. Entre 2022 y 2023 el Parlamento Europeo trabajó para regular la transformación digital, aprobando la Estrategia y actualizando o aprobando las siguientes leyes:

a. Reglamento General de Protección de Datos (27 de abril de 2016)
b. Ley de ciberseguridad de la Unión Europea (17 de abril de 2019)
c. Estrategia europea sobre datos (19 de febrero de 2020)
d. Ley de Gobernanza de Datos, DGA (6 de abril de 2022)
e. Código de buenas prácticas en materia de desinformación reforzado de 2022 (presentado el 16 de junio de 2022)
f. Ley de Mercados Digitales, DMA (19 de octubre de 2022)
g. Ley de Servicios digitales, DSA (19 de octubre de 2022)
h. Ley de Resiliencia Operacional Digital, DORA (14 de diciembre de 2022)
i. Ley de ciberresiliencia de la Unión Europea, CRA, (15 de septiembre de 2022)
j. Ley del mercado de criptoactivos, MICA (20 de abril de 2023)
k. Ley de Datos (9 de noviembre de 2023)
l. Ley de Inteligencia Artificial de la Unión Europea, (8 de diciembre de 2023 y respaldado por la Eurocámara el 13 de marzo de 2024)

Para facilitar la visualización y seguimiento de todas las aprobaciones de legislación y otras normas de la UE, se preparó un gráfico de tiempo (Gráfico 1). De estas legislaciones, propuestas de normativas, comentarios y sus puntos principales se presentan a continuación.

Gráfico 1. Tiempos de aprobación de legislación en la Unión Europea

Fuente: Elaboración propia.

a. Reglamento general de protección de datos (RGPD)

El Reglamento General de Protección de Datos (RGPD) de la Unión Europea, aprobado el 27 de abril de 2016, y en vigor desde el 25 de mayo de 2018, establece principios y normas para proteger los datos personales de las personas físicas, garantizando sus libertades y derechos fundamentales en relación con el tratamiento de dichos datos, sin importar su nacionalidad o residencia (Unión Europea, 2016).

En el RGPD se establecieron los siguientes objetivos relativos al tratamiento de datos personales y su libre circulación:

- Proteger a las personas cuando sus datos están siendo tratados por el sector privado como por la mayor parte del sector público. Sin embargo, cuando los datos sean utilizados por las autoridades competentes con fines policiales, estarán sujetos a la Directiva sobre protección de datos en el ámbito penal.

- Permitir que las personas controlen mejor sus datos personales. Esto implica modernizar y unificar las normas para que las empresas puedan reducir la burocracia y ganar mayor confianza por parte de los consumidores.

- Crear un sistema de autoridades de control completamente independiente, que supervise y vele por el cumplimiento del RGPD. Estas autoridades deben tener la capacidad de tomar medidas coercitivas en caso de incumplimiento de las normativas de protección de datos.

En el Artículo 4 del RGPD se definió como «datos personales: toda información sobre una persona física identificada o identificable ("el interesado")», y estableció que «se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente... mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona».

Luego, en el Artículo 5, principios relativos al tratamiento, establece en el numeral 1 que los datos personales serán:

> a) Tratados de manera lícita, leal y transparente en relación con el interesado (licitud, lealtad y transparencia).
> b) Recogidos con fines determinados, explícitos y legítimos, y no se tratarán ulteriormente de manera incompatible con dichos fines; (donde) el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales (limitación de la finalidad).
> c) Adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados (minimización de datos).
> d) Exactos y, si fuera necesario, actualizados... mediante medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan (exactitud).
> e) Mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales... los que podrán conservarse durante períodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos (limitación del plazo de conservación).
> f) Tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas (integridad y confidencialidad).

De esta manera, el RGPD reforzó los derechos existentes, estableció nuevos derechos para que las personas tengan un mayor control sobre sus datos personales, especialmente el derecho a saber si existe una violación de la seguridad de los datos personales, al tiempo que las empresas y organizaciones que trabaja con este tipo de información deben informar a la autoridad responsable de la protección de datos y, cuando sea un caso grave de violación de la seguridad de los datos, deben informar a las personas afectadas.

El Artículo 12 del RGPD establece importantes disposiciones sobre la transparencia y la facilidad de ejercicio de los derechos del interesado en relación con el tratamiento de sus datos personales. Respecto a la transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado estableció en el numeral 1 que «El responsable del tratamiento tomará las medidas oportunas para facilitar al interesado toda información... así como cualquier comunicación... relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño». Y en el numeral 2 estableció que «El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos... (y) no se negará a actuar a petición del interesado con el fin de ejercer sus derechos...salvo que pueda demostrar que no está en condiciones de identificar al interesado» (Unión Europea, 2016).

b. Ley de Ciberseguridad

La Comisión Europea propuso una Ley de Ciberseguridad en septiembre de 2017, para enfrentar los ciberataques y garantizar una ciberseguridad sólida en la UE. Después de múltiples diálogos tripartitos entre representantes del Parlamento Europeo, el Consejo de la Unión Europea y la Comisión Europea, entidad que formula propuestas de nuevas legislaciones, lograron acuerdos y aprobaron el 17 de abril de 2019 la Ley de Ciberseguridad de la Unión Europea (Unión Europea, 2019).

Seguidamente, la Agencia de la Unión Europea para la Ciberseguridad (ENISA, por sus siglas en inglés) definió la ciberseguridad como:

> ...la piedra angular de la transformación digital y una necesidad que es transversal a todos los sectores, por lo que resulta necesario tenerla en consideración en una amplia serie de iniciativas y ámbitos políticos. La ciberseguridad no debe limitarse a una comunidad especializada de expertos técnicos en cibernética. Deberá estar integrada en todos los ámbitos de las políticas de la UE. Resulta esencial evitar la fragmentación y contar con un enfoque coherente teniendo en cuenta al mismo tiempo las especificidades de cada sector (ENISA, 2020, p. 9).

Por su parte, Amazon (2024) define la ciberseguridad o seguridad informática como el área que trabaja para proteger la infraestructura computacional y la información que en ella exista de posibles ataques, daños y/o robos digitales. La estrategia de ciberseguridad debe formularse con una visión que involucre y coordine el trabajo de las personas, los procesos y la tecnología que tiene una organización. Por tanto, toda organización tiene la responsabilidad de proteger todos sus datos, mediante el cumplimiento de estándares, métodos, herramientas, normas y legislaciones para mantener la confianza de los usuarios, en general, y de sus clientes, en particular. A esto agrega que la ciberseguridad es el área de trabajo tecnológico que busca contener o mitigar los ataques, entre los cuales los más comunes son:

(i) Malware: software malicioso, diseñados para acceder a información confidencial o afectar negativamente la infraestructura de una organización (ej. Troyanos, spyware y virus).
(ii) Ramsomware: tecnología utilizada por delincuentes cibernéticos para extorsionar por dinero a la empresa o institución.
(iii) Ataque de intermediario: acción realizada para obtener información confidencial de manera no autorizada durante el intercambio de datos, especialmente de transacciones financieras.
(iv) Phishing: técnica utilizada para engañar a usuarios mediante la solicitud de información personal en correos electrónicos que los dirigen a sitios web falsificados que inducen a introducir datos sensibles, como números de tarjetas de crédito o cuentas bancarias.
(v) DoS tecnología utilizada para sobrecargar un servidor mediante el envío de un alto volumen de solicitudes falsas, lo que impide que los usuarios legítimos accedan al servidor objetivo.
(vi) Amenaza interna: riesgo de seguridad causado por el personal de la organización que tiene acceso a los sistemas informáticos y busca desestabilizar o dañar la infraestructura tecnológica.

En la Ley de Ciberseguridad, también denominado Reglamento sobre la Ciberseguridad (Diario Oficial de la Unión Europea, DOUE, 2019), en el considerando (5) señala que «Los ciberataques van en aumento, y una economía y una sociedad conectadas, más vulnerables a las ciberamenazas y los ciberataques, requieren unas defensas más sólidas». Luego, como señal de preocupación destaca que los ciberataques también son transfronterizos, mientras que las competencias de las autoridades de ciberseguridad y las policiales tienden a ser predominantemente nacionales. Ante esta situación, expresa que es necesaria «una respuesta efectiva y coordinada» así como «una gestión de crisis a escala de la Unión», por lo que se requieren políticas específicas e instrumentos más amplios que propicien la solidaridad y la asistencia mutua en Europa, para responder globalmente a las ciberamenazas, incluidos los incidentes transfronterizos. Finalmente, expresa que es necesario

realizar evaluaciones sistemáticas de la ciberseguridad y la resiliencia en la Unión, en respuesta a los avances, retos y amenazas que se den en el futuro.

En el considerando (8) expresa que para la ciberseguridad es no es solo de orden tecnológico porque también juega un papel determinante el comportamiento humano, por lo que se debe promover con fuerza lo que denomina como «ciberhigiene», la cual incluye «medidas sencillas de rutina que, aplicadas con regularidad por los ciudadanos, las organizaciones y las empresas, (que) minimizan su exposición a los riesgos derivados de las ciberamenazas».

La Ley de Ciberseguridad en el Artículo 1 señala como objetivo «garantizar el correcto funcionamiento del mercado interior, aspirando al mismo tiempo a alcanzar un nivel elevado de ciberseguridad, ciberresiliencia y confianza dentro de la Unión (Europea). Luego, en el Artículo 8, que se refiere al "Mercado, certificación de la ciberseguridad y normalización» en su numeral 1 mandata a ENISA a apoyar y promover «el desarrollo y la aplicación de la política de la Unión en materia de certificación de la ciberseguridad de, productos, servicios y procesos de TIC», para lo cual debe «a) controlar permanentemente los avances en los ámbitos de normalización relacionados y recomendar unas especificaciones técnicas apropiadas que se puedan utilizar en el desarrollo de los esquemas europeos de certificación de la ciberseguridad... b) preparar propuestas de esquemas europeos de certificación de la ciberseguridad... para productos, servicios y procesos de TIC».

En el Título III, Marco de Certificación de la Ciberseguridad, en el Artículo 46, correspondiente al «Marco europeo de certificación de la ciberseguridad», la de Ley Ciberseguridad de la UE señala en el punto 1., que «se crea el marco europeo de certificación de la ciberseguridad con el fin de mejorar las condiciones de funcionamiento del mercado interior incrementando el nivel de ciberseguridad» para tener un planteamiento armonizado «de esquemas europeos de certificación de la ciberseguridad, con el objetivo de crear un mercado único digital para los productos, servicios y procesos de TIC» (DOUE, 2019).

Luego, en el numeral 2 establece que el «marco europeo de certificación de la ciberseguridad» se define un mecanismo para:

> «instaurar esquemas... de certificación de la ciberseguridad y a confirmar que los productos, servicios y procesos de TIC que hayan sido evaluados con arreglo a dichos esquemas cumplen los requisitos de seguridad especificados con el objetivo de proteger la disponibilidad, autenticidad, integridad o confidencialidad de los datos almacenados, transmitidos o procesados o las funciones o servicios que ofrecen, o a los que permiten acceder, dichos productos, servicios y procesos durante todo su ciclo de vida».

Más adelante, el Artículo 51 de la Ley de Ciberseguridad establece los objetivos de seguridad de los esquemas de certificación de la ciberseguridad, para los cuales demanda cumplir por lo menos con objetivos de seguridad como proteger los datos almacenados, transmitidos o tratados de otro modo «frente al almacenamiento, tratamiento, acceso o revelación accidentales o no autorizados durante todo el ciclo de vida del producto, servicio o proceso de TIC... (y) la destrucción accidental o no autorizada, la pérdida o la alteración o la falta de disponibilidad durante todo el ciclo de vida del producto, servicio o proceso de TIC». También se busca que «las personas, programas o máquinas autorizados puedan acceder exclusivamente a los datos, servicios o funciones a que se refiere su derecho de acceso... (así como) detectar y documentar las dependencias y vulnerabilidades conocidas... (y) que los productos, servicios y procesos de TIC se entreguen siempre con un programa informático y un equipo informático actualizados que no contengan vulnerabilidades conocidas públicamente, y dispongan de mecanismos para efectuar actualizaciones de seguridad», entre otros esquemas.

Además, el Artículo 52 de la Ley de Ciberseguridad establece que el esquema europeo de certificación de la ciberseguridad podrá especificar diversos niveles de garantía para los productos, servicios y procesos de TIC de acuerdo con el nivel de riesgo que tenga el uso de un producto para «reducir el riesgo de incidentes de ciberseguridad o evitarlos». Por tanto, define tres niveles de garantía para asegurar "que los productos, servicios y procesos de TIC... cumplen los correspondientes requisitos de seguridad, incluidas las funcionalidades de seguridad:

(i) «básico»: que busca «minimizar los riesgos básicos conocidos de ciberincidentes y ciberataques».
(ii) «sustancial»: cuya finalidad es «minimizar los riesgos... de incidentes y los ciberataques cometidos por agentes con capacidades y recursos limitados».
(iii) «elevado»: que tiene como objetivo «minimizar el riesgo de ciberataques sofisticados cometidos por agentes con capacidades y recursos considerables».

Y concluye con una sentencia que establece que el esquema europeo de certificación de la ciberseguridad «estará definido por una combinación apropiada de componentes de garantía» (DOUE, 2019).

c. Estrategia europea de datos

Desde la Introducción la Estrategia Europea de Datos, difundida en Bruselas el 19 de febrero de 2020, reconoce el impacto que las tecnologías digitales ya estaban teniendo en toda la sociedad. Ante esta situación señaló que:

> En los últimos años, las tecnologías digitales han transformado la economía y la sociedad, afectando a todos los sectores de actividad y a la vida cotidiana de todos los europeos (que) Los datos están en el centro de esta transformación y hay más por venir. La innovación basada en datos aportará enormes beneficios a los ciudadanos, por ejemplo, mediante una mejor medicina personalizada, una nueva movilidad y su contribución al Pacto Verde Europeo. En una sociedad en la que los individuos generarán cantidades cada vez mayores de datos, la forma en que se recopilan y utilizan los datos debe anteponer los intereses del individuo, de acuerdo con los valores, derechos y normas fundamentales europeos. (Así) Los ciudadanos confiarán y adoptarán las innovaciones basadas en datos sólo si confían en que cualquier intercambio de datos personales en la UE estará sujeto al pleno cumplimiento de las estrictas normas de protección de datos de la UE. Al mismo tiempo, (ante) el creciente volumen de datos industriales no personales y de datos públicos en Europa, combinado con el cambio tecnológico en la forma en que se almacenan y procesan los datos, constituirá una fuente potencial de crecimiento e innovación que debería aprovecharse. (Comisión Europea, 2020, p. 1)

Sin embargo, antes de la publicación de la Estrategia, la Unión Europea (UE) ya había dado algunos pasos en esta dirección. Entre ellos, la adopción del Reglamento General de Protección de Datos (2016) que actualizó y reforzó los derechos de los ciudadanos europeos sobre sus datos personales, el Reglamento para la Libre Circulación de Datos no Personales (2018), el Reglamento de Ciberseguridad (2019) y la Directiva de Datos Abiertos (2019). La Estrategia Europea de Datos pone al centro del desarrollo de tecnologías a las personas, así como en la defensa y promoción de los valores y derechos de los europeos en el mundo digital. En adición, busca «delimitar el rumbo del modelo de economía digital de la Unión Europea», la cual «tiene como pilares fundamentales la libre circulación de los datos no personales por el territorio europeo, la protección de los derechos y libertades de las personas y el acceso generalizado a los datos por parte de las autoridades» (Centro de Competencia, 2022, párr. 5).

El objetivo de la Estrategia es «crear un mercado único de datos que garantice la competitividad mundial y la soberanía de los datos de Europa. Los espacios

comunes europeos de datos garantizarán que se disponga de más datos para su uso en la economía y la sociedad, manteniendo al mismo tiempo bajo control a las empresas y a las personas que generan los datos» (Comisión Europea, 2022, párr. 2). De esta manera, se busca que las aplicaciones basadas en datos beneficien a las personas y las empresas, como, por ejemplo, mejorar la atención en salud y hacerla más personalizada, tener sistemas de transporte más seguros y limpios, crear y producir nuevos bienes y servicios, mejorar la formulación de políticas públicas, modernizar los servicios públicos y reducir sus costos, así como hacer más eficiente y sostenible la generación de energía.

Consecuentemente, la Estrategia busca que la UE se convierta en un modelo de sociedad con capacidades para utilizar los datos, investigar y tomar decisiones, facilitar la innovación y estimular el crecimiento. Con este fin, la Estrategia busca crear un mercado único de datos que permita la circulación de dato en toda la UE, formulando una legislación que garantide la privacidad y la protección de datos, normas para el acceso y utilización de los datos de manera justa, práctica y clara (Comisión Europea, 2022).

d. Ley de Gobernanza de Datos (DGA)

El Parlamento Europeo aprobó la Ley de Gobernanza de Datos (DGA por sus siglas en inglés), el 6 de abril de 2022, mediante la cual se busca aumentar la confianza en el intercambio de datos, que estén disponibles, promover la innovación, la creación de nuevos productos y servicios, así como facilitar la transición ecológica y la transformación digital en Europa. También, se espera que esta Ley facilite a las empresas el acceso y uso de una gran cantidad de información y datos industriales de alta calidad, en especial los que se captan en el Internet de las Cosas. Esta aspiración se basa en que alrededor del el 80 % de los datos industriales no son utilizados, cuando para sacar ventajas de la IA es necesario tener una gran cantidad de datos para crear algoritmos (Parlamento Europeo, 2022).

La DGA también busca crear espacios comunes con datos europeos en áreas estratégicas como salud, medio ambiente, energía, agricultura, movilidad, finanzas, industria manufacturera, administración pública y la formación de capacidades, así como para la investigación científica y la lucha contra el cambio climático. Además, con esta Ley se espera que las empresas, personas e instituciones del sector público también accedan a estos datos con fines altruistas. Consecuentemente, las instituciones públicas «deberán evitar la creación de derechos exclusivos para la reutilización de determinados datos, y los acuerdos exclusivos deberían limitarse a un período de 12 meses para los nuevos contratos y de dos años y medio para los existentes, para que haya más datos disponibles. a PYMES y startups» (Parlamento Europeo, 2022, párr. 4).

Una característica de la DGA es que regula los vacíos que pudieran utilizar los operadores que no son de países de la UE para abusar del sistema, mediante disposiciones precisas que generen confianza, requisitos que tendrán que cumplir los servicios que estarán bajo control y facilitar un acceso justo.

e. Código de buenas prácticas en materia de desinformación reforzado (2022)

El Código de buenas prácticas en materia de desinformación reforzado de 2022 –que se basa en el Código de 2018, pionero a nivel mundial– se aprobó el 16 de junio de 2022 luego de un proceso de revisión iniciado en junio de 2021 y la presentación de una propuesta el 16 de junio de 2022, en concordancia con la Ley sobre transparencia y orientación de la publicidad política y la Ley de servicios digitales.

El Código tiene como objetivo convertirse en una medida de mitigación y un Código de Conducta reconocido en el marco co-regulador de la DSA, en el cual se establecen compromisos y medidas más estrictas para contrarrestar la desinformación en línea, para crear un entorno en línea que sea más transparente, seguro y confiable. Con esta finalidad, el Código reforzado demanda la firma de compromisos precisos, que «incluyen desmonetizar la difusión de desinformación; garantizar la transparencia de la publicidad política; mejorar la cooperación con los verificadores de datos; y facilitar el acceso de los investigadores a los datos» (European Commission, 2022, pár. 2).

En otra publicación de la *European Commission* (2022) muestra su satisfacción por la publicación del Código de buenas prácticas en materia de desinformación reforzado, que incluye las principales plataformas en línea, plataformas emergentes y especializadas, en el punto b del Preámbulo del Código señala que en respuesta a «la exposición de los ciudadanos a desinformación a gran escala, incluida información engañosa o completamente falsa información, es un gran desafío para Europa» y que «nuestras sociedades democráticas abiertas dependen de debates públicos que permitan a ciudadanos bien informados expresar su voluntad a través de procesos políticos libres y justos».

El Código fortalecido tiene como objetivo abordar las deficiencias del Código anterior, con compromisos y medidas más firmes y granulares, que se basan en las lecciones operativas aprendidas en los últimos años.

En concreto, el nuevo Código contiene compromisos para:

- Ampliar la participación: el Código no es solo para grandes plataformas, sino que también involucra a una variedad de actores diversos que

desempeñan un papel en la mitigación de la difusión de desinformación, y se invita a que se unan más signatarios;

- Recortar los incentivos financieros para la difusión de desinformación garantizando que los proveedores de desinformación no se beneficien de los ingresos por publicidad;

- Cubrir nuevos comportamientos manipuladores como cuentas falsas, bots o *deep fakes* maliciosos que difunden desinformación;

- Dotar a los usuarios de mejores herramientas para reconocer, comprender y denunciar la desinformación;

- Ampliar la verificación de datos en todos los países de la UE y en todas sus lenguas, garantizando al mismo tiempo que los verificadores reciban una remuneración justa por su trabajo;

- Garantizar una publicidad política transparente al permitir a los usuarios reconocer fácilmente los anuncios políticos gracias a un mejor etiquetado e información sobre los patrocinadores, el gasto y el período de visualización;

De esta manera, también se busca que los investigadores tengan mayor apoyo por tener un mejor acceso a los datos que están disponibles en las plataformas

f. Ley de Mercados Digitales (DMA)

El Parlamento Europeo y el Consejo de la Unión Europea adoptaron el Reglamento de la Ley de Mercados Digitales (DMA por sus siglas en inglés) el 14 de septiembre de 2022. Esta legislación pionera que tiene como objetivo «contribuir al correcto funcionamiento del mercado interior estableciendo normas armonizadas que garanticen a todas las empresas, en toda la Unión, la equidad y la disputabilidad de los mercados en el sector digital donde haya guardianes de acceso, en beneficio de los usuarios profesionales y los usuarios finales» (DMA, Artículo 1). Esta norma permite o prohíbe el uso de la IA tomando en cuenta el riesgo que le puede generar a las personas, ante lo cual establece multas de hasta 35 millones de euros (EUR-Lex/Unión Europea 2022).

Al referirse a los 'guardianes de acceso", se identifican como las grandes plataformas digitales que brindan servicios de plataforma central, como son los motores de búsqueda en línea (SEO: *Search Engine Optimization*, optimización en motores de búsqueda), establecimientos de aplicaciones y servicios de mensajería.

La DMA también provee las definiciones de cada actor o servicio en el Artículo 2 de la siguiente manera:

1. «Guardián de acceso»: una empresa que presta servicios de plataforma básica, designada de conformidad con el Artículo 3 (define los gatekeepers);

2. «Servicio de plataforma principal» significa cualquiera de los siguientes: (a) servicios de intermediación en línea; (b) motores de búsqueda en línea; (c) servicios de redes sociales en línea; (d) servicios de plataforma para compartir vídeos; (e) servicios de comunicaciones interpersonales independientes del número; (f) sistemas operativos; (g) navegadores web; (h) asistentes virtuales; (i) servicios de computación en la nube; (j) servicios de publicidad en línea, incluidas redes publicitarias, intercambios publicitarios y cualquier otro servicio de intermediación publicitaria, prestados por una empresa que proporcione cualquiera de los servicios de plataforma principal».

A estas definiciones agrega otras 31 que sirven para determinar otros conceptos y funciones.

Luego en el Artículo 3 define a quienes se designarán como gatekeepers (guardianes de acceso):

1. «Una empresa se designará guardián de acceso si: (a) tiene un impacto significativo en el mercado interior; (b) proporciona un servicio de plataforma central que es una puerta de entrada importante para que los usuarios empresariales lleguen a los usuarios finales; y (c) goza de una posición arraigada y duradera en sus operaciones, o es previsible que disfrute de esa posición en un futuro próximo.

2. Se presumirá que una empresa cumple los requisitos respectivos del apartado 1: (a) ... cuando alcance un volumen de negocios anual en la Unión (Europea) igual o superior a 7 500 millones EUR en cada uno de los tres últimos ejercicios financieros, o cuando su capitalización bursátil media o su valor justo de mercado equivalente ascienda al menos a 75,000 millones de euros en el último ejercicio financiero y proporciona el mismo servicio de plataforma central en al menos tres Estados miembros; (b) ... cuando proporcione un servicio de plataforma central que en el último ejercicio financiero tenga al menos 45 millones de usuarios finales activos mensuales establecidos o ubicados en la Unión y al menos 10,000 usuarios profesionales activos anuales establecidos en la Unión (Europea), identificados y calculados

de acuerdo con la metodología y los indicadores establecidos en el anexo; (c) ... cuando los umbrales previstos en la letra b) del presente apartado se hayan alcanzado en cada uno de los tres últimos ejercicios financieros».

La DMA también establece lo que deben hacer los guardianes de acceso (obligaciones) y lo que no deben hacer (prohibiciones) en sus operaciones diarias. Respecto a las obligaciones de los guardianes de acceso señala que deberán:

- «Permitir que terceros interoperen con los propios servicios del guardián de acceso en determinadas situaciones específicas.
- Permitir que sus usuarios comerciales accedan a los datos que generan en su uso de la plataforma del guardián.
- Proporcionar a las empresas que anuncian en su plataforma las herramientas y la información necesarias para que los anunciantes y editores lleven a cabo su propia verificación independiente de sus anuncios alojados en el gatekeeper.
- Permitir a sus usuarios comerciales promocionar su oferta y celebrar contratos con sus clientes fuera de la plataforma del guardián» (European Comission, 2023, párr. 13 al 14).
-

Luego, establece lo que no deben hacer los guardianes de acceso (prohibiciones), como son las siguientes:

- «Tratar los servicios y productos ofrecidos por el propio guardián de manera más favorable en su clasificación que los servicios o productos similares ofrecidos por terceros en la plataforma del guardián de acceso.
- Impedir que los consumidores se conecten con empresas fuera de sus plataformas.
- Impedir que los usuarios desinstalen cualquier software o aplicación preinstalado si así lo desean.
- Rastrear a los usuarios finales fuera del servicio de plataforma principal de los guardianes de acceso con fines de publicidad dirigida, sin que se haya otorgado el consentimiento efectivo» (European Comission, 2023, párr. 16 al 19).

Además, la DMA decreta multas por incumplimientos, las que se elevan hasta el 10 % de la facturación anual total de la empresa a nivel mundial, la que se eleva hasta el 20 % si es reincidente. Además, incluye multas coercitivas periódicas que llegan hasta el 5 % del volumen de negocios medio diario de la empresa.

g. Ley de Servicios digitales (DSA)

La Ley de Servicios Digitales (DSA, siglas de *Digital Services Act*) se aprobó el 19 de octubre de 2022, se establecen nuevos derechos para los usuarios de los servicios digitales, se den mejores servicios a los consumidores, haya mayor transparencia en la publicidad, las plataformas de gran tamaño y motores de búsqueda asuman mayores responsabilidades y se proteja de mejor manera a los menores. Dentro de las obligaciones que se le imponen a estas plataformas y motores de búsqueda está el evitar todo tipo de abuso de sus sistemas mediante el establecimiento de mecanismos de supervisión de su gestión de riesgos mediante auditores externos independientes (Comisión Europea, 2023).

Desde los considerandos la DSA señala que la sociedad de la información demanda tanto servicios digitales directos como servicios intermediarios, porque se han convertido en un factor determinante para la economía y las personas. Luego, señala que pasado más de 20 años desde la adopción del marco jurídico para estos servicios en 2000 (2000/31/CE) y considerando que se han creado innovadoras herramientas de negocios y de servicios –redes y servicios en línea– los usuarios normalmente suscriben contratos a distancia para tener acceso a información y realizar transacciones (European Parliament, 2022).

También se consideró que, para regular los servicios digitales, enfrentar contenidos ilegales, la desinformación y otros riesgos para la sociedad, diversos países de la UE introdujeron regulaciones nacionales discordantes que causaron un efecto negativo en el mercado interno, que se considera que debe verse como un espacio sin fronteras interiores para facilitar la libre circulación de bienes y servicios que se dan vía internet que es una herramienta transfronteriza. Para armonizar esta situación, se consideró necesaria tener una legislación para la UE para constituir un solo mercado de servicios intermediarios para facilitar a las empresas el acceso a nuevos mercados y oportunidades y brindar mayores opciones a los consumidores (European Parliament, 2022).

La DSA «regula a los intermediarios y plataformas en línea, incluyendo mercados, redes sociales, plataformas de intercambio de contenidos, tiendas de aplicaciones y plataformas de viajes y alojamiento en línea» (Comisión Europea,

2023, párr. 1). Sus objetivos principales son «proteger a los consumidores y sus derechos fundamentales en línea... favorecer la innovación, el crecimiento y la competitividad, y facilitar la expansión de las plataformas más pequeñas, las PYMES y las empresas emergentes» (párr. 2), así como «prevenir las actividades ilegales y nocivas en línea y la difusión de desinformación (párr. 1), para garantizar la seguridad de los usuarios, proteger sus derechos fundamentales», dar mayor protección a los niños en línea, reducir la exposición a contenidos ilícitos y crear un ambiente de plataformas en línea justo y abierto. También, busca proveer mayor control democrático y reducción de riesgos como la manipulación o la desinformación (Comisión Europea, 2023).

A los proveedores de servicios digitales la DSA les da seguridad jurídica al establecer una normativa única para toda la UE, así como generar condiciones que faciliten el establecimiento, la expansión de sus servicios en Europa y tener igualdad de condiciones para enfrentar a proveedores de contenidos ilícitos. La DSA comenzó a aplicarse a todas las plataformas a partir del 17 de febrero de 2024.

En otra publicación de la Comisión Europea (2023) destaca que la DSA contiene medidas para combatir y reducir los contenidos ilícitos en línea, incluyendo la oferta de bienes y servicios ilícitos, al dar espacio a los usuarios para informar sobre este tipo de contenidos y cooperar con los *alertadores fiables* especializados para detectar y eliminarlos. Entre estas medidas están las que se enfocan en rastrear a vendedores en línea, para evitar estafas e iniciar juicios contra ellos, así como la obligación para este tipo de vendedores de comprobar aleatoriamente en sus sitios web si los bienes o servicios que ofrecen cumplen con lo ofertado.

Además, para asegurar mayor transparencia en las plataformas en línea se han incluido medidas para asegurar la calidad de la información, así como en los algoritmos que se utilicen para recomendar contenidos y productos. A esto se agrega la prohibición de utilizar los llamados «patrones oscuros» en las plataformas en línea, esto es, artificios para manipular a los usuarios «para que tomen decisiones que no tenían intención de tomar» (Comisión Europea, 2023, punto 1, párr. 14).

En adición, la DSA obliga a los proveedores de plataformas en línea que son accesibles por menores de edad a incluir medidas para garantizar que sus sistemas contiene medidas que certifiquen un alto nivel de seguridad, privacidad y protección a estos usuarios. Estas medidas incluyen la prohibición de publicidad dirigida a menores que utilicen datos personales de los usuarios cuando haya certeza razonable que se trata de un menor de edad. Además, la DSA señala que cualquier tipo de publicidad, «desde la comercialización digital hasta la publicidad basada en temas y los anuncios políticos... establece,

por ejemplo, normas sobre el consentimiento de los usuarios o su derecho a oponerse a la comercialización digital para destinatarios concretos», al tiempo que introduce dos nuevas restricciones: (i) prohibición de la publicidad dirigida a menores, antes expuesta; y (ii) prohibición de publicidad personalizada utilizando perfiles con datos personales, como orientación sexual o creencias religiosas (Comisión Europea, 2023).

También, la DSA busca mitigar los riesgos causados por «la desinformación o la manipulación electoral, la ciberviolencia contra las mujeres o las agresiones a menores en línea» (Comisión Europea, 2023, punto 1, párr. 10). Sin embargo, aclara que estos mecanismos deben aplicarse cuidadosamente para no causar restricciones de la libertad de expresión que están «sujetas a auditorías independientes» (Ibidem).

Un tema adicional en línea con la DSA es la intención del Parlamento Europeo de aumentar la protección de los jugadores de videojuegos y promover el crecimiento potencial del sector. Se estima que en 2023 el mercado mundial del juego generó alrededor de US$184,000 millones, con un 0.6 % de aumento respecto al año anterior, resultantes de compras de unos 3,380 millones de jugadores en el mundo, con un 6.3 % de incremento. Para tener una clara visión de la situación en la UE, la Comisión Europea presentó el informe *Comprendiendo el valor de una sociedad europea de videojuegos*, en octubre de 2023, en el que señala que esta industria generó 23,480 millones de euros en 2022; y que en 2020 sus ventas fueron 4.3 % mayores que las de música y 1.8 % más que las de proveedores de contenido en línea. El sector de videojuegos generó más de 74,000 empleos en la UE en 2020, aunque 40 % de estas empresas de este sector tuvieron dificultades para encontrar y contratar personal con las habilidades que se requieren (Vicente, 2023).

En línea con la capacidad de este sector para innovar, expandirse, contribuir al crecimiento de la economía y la generación de empleos, se planteó la necesidad de darle un decidido apoyo, Así es como el Parlamento Europeo aprobó el 18 de enero de 2023 un informe que solicitó armonizar las normas europeas para tener una mejor protección de los jugadores de videojuegos, especialmente niños (Parlamento Europeo, 2023).

En este informe se señala la necesidad «que los padres sepan y controlen los juegos a los que juegan sus hijos, así como la cantidad de tiempo y dinero que emplean en ello» (Parlamento Europeo, 2023, pár. 1), y «proteger a los menores especialmente de los señuelos para hacer compras mientras juegan y de la práctica de vender artículos obtenidos en un videojuego a cambio de dinero real (gold-farming)... (muchas veces) vinculada con delitos financieros y abusos de derechos humanos» (párr. 2), por lo que los desarrolladores de

videojuegos «deben abstenerse de fomentar la adicción y deben tener en cuenta la edad, los derechos y las vulnerabilidades de los niños» (Ibidem).

En el informe los parlamentarios europeos también solicitan un refuerzo de la protección de los consumidores, por lo que instan a los desarrolladores de videojuegos que tengan mecanismos «para la protección de datos, el equilibrio de género y la seguridad de los jugadores, y que no discriminen a las personas con discapacidad» (Parlamento Europeo, 2023, pár. 3), así como crear condiciones para que la cancelación de una suscripción a un juego sea tan fácil de hacer como al solicitar la suscripción; y que tengan claras políticas de compra, devolución y reembolso (Parlamento Europeo, 2023).

h. Ley de Resiliencia Operacional Digital (DORA)

El Parlamento Europeo y del Consejo Europeo aprobaron el 14 de diciembre de 2022 el Reglamento sobre Resiliencia Operacional Digital, que se conoce como Ley DORA (por sus siglas en inglés de *Digital Operational Resilience Act*) que modificó los Reglamentos de 2009, 2012, 2014 y 2016. La Ley DORA es un Reglamento vinculante en todos sus elementos, por tanto, lo deberán aplicar todos los Estados miembros de la UE cuando entre en vigor a partir del 17 de enero de 2025.

14 de diciembre de 2022 sobre la resiliencia operativa digital del sector financiero. Comienza por exponer sus aspectos generales, para seguir con la estructura (elementos subjetivos y objetivos) y el funcionamiento del sistema de gestión del riesgo operativo digital que las entidades financieras deberán aplicar a partir del 17 de enero de 2025.

La Ley DORA, que es parte de un conjunto de leyes y normas de las finanzas digitales, amplia la facultad de supervisión de las entidades financieras, así como a los proveedores de servicios entregados mediante Tecnologías de la Información y la Comunicación, TIC. Así es como en el Artículo 1 establece el objeto de la Ley: «lograr un elevado nivel común de resiliencia operativa digital... (al establecer) requisitos uniformes relativos a la seguridad de las redes y los sistemas de información que sustentan los procesos empresariales de las entidades financieras». Luego, en el literal a) de este Artículo, lista los requisitos que deberán cumplir las instituciones financieras relacionados con:

i). La gestión de riesgo en el ámbito de las tecnologías de la información y la comunicación (TIC)
ii) La notificación (voluntaria) a las autoridades competentes de incidentes graves relacionados con las TIC y... de ciberamenazas importantes.

iii) La notificación a las autoridades competentes de incidentes operativos o de seguridad graves relacionados con los pagos por parte de las entidades financieras (definidas en Artículo 2).
iv) Las pruebas de resiliencia operativa digital.
v) El intercambio de información e inteligencia en relación con las ciberamenazas y las vulnerabilidades cibernéticas
vi) Las medidas para la buena gestión del riesgo relacionado con las TIC derivado de terceros.

Luego, el Artículo 2 amplia el ámbito de supervisión de instituciones financieras y de proveedores de servicios TIC, al incluir: entidades de crédito y de pago, proveedores de servicios de información sobre cuentas, proveedores de dinero electrónico, empresas de servicios de inversión, proveedores de servicios de criptoactivos, depositarios centrales de valores, entidades de contrapartida central, centros de negociación, registros de operaciones, gestores de fondos de inversión alternativos, sociedades de gestión, proveedores de servicios de suministro de datos, empresas de seguros, reaseguradoras e intermediarios de reaseguros, fondos de pensiones, agencias de calificación crediticia, administradores de índices claves de referencia, registros de titularizaciones, y proveedores terceros de servicios de TIC.

En el Artículo 3 define «resiliencia operativa digital» como «la capacidad de una entidad financiera para construir, asegurar y revisar su integridad y fiabilidad operativas asegurando, directa o indirectamente mediante el uso de servicios prestados por proveedores terceros de servicios de TIC, toda la gama de capacidades relacionadas con las TIC necesarias para preservar la seguridad de las redes y los sistemas de información que utiliza una entidad financiera y que sustentan la prestación continuada de servicios financieros y su calidad, incluso en caso de perturbaciones».

Adicionalmente, en el Capítulo II, Gestión del riesgo relacionado con las TIC, Sección I, Artículo 5, Gobernanza y organización establece que para «lograr un nivel elevado de resiliencia operativa digital, las entidades financieras dispondrán de un marco interno de gobernanza y control que garantice una gestión efectiva y prudente del riesgo relacionado con las TIC».

Complementariamente, en la Sección II, Artículo 6, Marco de gestión del riesgo relacionado con las TIC establece que «Las entidades financieras contarán con un marco de gestión del riesgo relacionado con las TIC sólido, completo y bien documentado como parte de su sistema global de gestión de riesgos», para «hacer frente al riesgo relacionado con las TIC de forma rápida, eficiente y exhaustiva y asegurar un alto nivel de resiliencia operativa digital».

Un aspecto interesante de la Ley DORA es el que presenta en el Artículo 14, Comunicación, donde establece que, como parte del marco de gestión del riesgo relacionado con las TIC, «...las entidades financieras dispondrán de planes de comunicación de crisis que permitan la divulgación responsable de, al menos, los incidentes graves relacionados con las TIC o las vulnerabilidades importantes a clientes y contrapartes, así como al público, según proceda». Este Artículo es clave para mantener informado a los consumidores y otras instancias lo que determinante para que haya transparencia ante situaciones de crisis financieras en el ámbito de las TIC.

Finalmente, es de resaltar el espíritu de cooperación que incluye la Ley DORA en el Capítulo VI, Acuerdos de intercambio de información, Artículo 45, Acuerdos de intercambio de información en relación con información e inteligencia sobre ciberamenazas, donde establece que:

> «Las entidades financieras podrán intercambiar entre sí información e inteligencia sobre ciberamenazas, incluidos indicadores de compromiso, tácticas, técnicas y procedimientos, alertas de ciberseguridad y herramientas de configuración, en la medida en que dicho intercambio de información e inteligencia... tenga por objeto mejorar la resiliencia operativa digital de las entidades financieras, en particular mediante la concienciación en relación con las ciberamenazas, la limitación o la desactivación de la capacidad de propagación de las ciberamenazas, el apoyo a las capacidades defensivas, las técnicas de detección de amenazas, las estrategias de mitigación o las fases de respuesta y recuperación».

i. Ley de Ciber Resiliencia (CRA)

El Parlamento Europeo publicó el 10 de noviembre de 2022 el artículo *Fighting cybercrime: new EU cybersecurity laws explained* (Lucha contra la ciberdelincuencia: explicación de las nuevas leyes de ciberseguridad de la UE) donde resalta que los productos que se utilizan a diario tienen cada vez más un componente digital, entre los que resalta los «vigilabebés, timbres conectados o enrutadores wifi (párr. 11), así como diversas "actividades que son críticas para la economía y la sociedad, incluidas la energía, el transporte, la banca, la salud, la infraestructura digital, la administración pública y el espacio» (párr. 8), los son susceptibles a ciberataques. Ante esta situación y para garantizar la seguridad ante las ciberamenazas, la UE está trabajando en una propuesta de Ley de Resiliencia Cibernética, para tener un conjunto uniforme de requisitos de ciberseguridad obligatorios en toda la UE para productos conectados a otro dispositivo o red.

Dada la preocupación por el alto número de casos y los altos costos de la ciberdelincuencia en un ambiente donde el uso a diario de los medios digitales se expande con celeridad, en septiembre de 2023 se reiteró la necesidad de proteger a los usuarios de las ciberamenazas, para asegurar que la sociedad funcione educadamente. Según la Comisión Europea (2023), el costo impuesto a la economía mundial por los ciberdelincuentes habría llegado hasta 5.5 billones de euros anuales a fines de 2020, el doble de 2015. Además, el 28 % de las pequeñas y medianas empresas europeas sufrieron delitos cibernéticos en 2021.

Ante esta situación, las instancias que tiene la responsabilidad de hacer proyectos de leyes comenzaron a estudiar y preparar un conjunto de normas de ciberresiliencia, con el objetivo de aumentar la seguridad de los productos digitales (hardware y software) comercializados en el mercado de la UE y durante todos sus ciclos de vida (European Parliament, 2022).

El 15 de septiembre de 2022, la Comisión Europea presentó una propuesta legislativa denominada Ley de Ciber Resiliencia (CRA, por sus siglas en inglés *Cyber Resilience Act*), para establecer requisitos obligatorios de ciberseguridad para todos los productos con elementos digitales. Por tanto, la ciber resiliencia ayuda a aumentar la capacidad de un sistema y habilidades de una organización para resistir y/o recuperarse de ataques cibernéticos malignos daños causados por un acto de piratería informática, al permitir a los usuarios de tecnología recuperar rápidamente los datos, evitar la propagación de la amenaza y volver a la normalidad lo antes posible.

Posteriormente, Consejo de la Unión Europea, el Comité de Representantes Permanentes de los Gobiernos de los Estados miembros (COREPER, 2023) y la Comisión de Industria, Investigación y Energía del Parlamento Europeo (ITRE, 2024) aprobaron el acuerdo provisional sobre la Ley de Resiliencia Cibernética, la cual se espera que sea sometida a votación del Parlamento Europeo en abril de 2024 (*European Parliament, Commission* 2019-24).

La propuesta Ley de Resiliencia Cibernética tiene como objetivo brindar mejor protección a los consumidores al imponer mayores responsabilidades a los fabricantes y obligarlos «a proporcionar soporte de seguridad y actualizaciones de software para abordar las vulnerabilidades identificadas, y proporcionándoles información sobre la ciberseguridad de los productos que compran y utilizan» (*European Parliament, Commission* 2019-24, párr. 2). De esta forma, se busca reducir el número de incidentes de ciberseguridad y dar mayor transparencia y confianza a «los consumidores en los productos con elementos digitales y garantizaría una mejor protección de sus datos y privacidad» (Ibidem).

En la propuesta de Ley de Resiliencia Cibernética se definen las reglas para la comercialización de productos con elementos digitales; la metodología para la clasificación de productos digitales; los requisitos para el diseño, desarrollo y producción de estos productos; la obligación de presentar de informes como fabricantes a fin de garantizar la ciberseguridad durante todo el ciclo de vida de los productos; y cumplir las reglas sobre vigilancia. Además, se propone ampliar en número de dispositivos cubiertos, para incluir productos como «software de sistemas de gestión de identidad, administradores de contraseñas, lectores biométricos, asistentes domésticos inteligentes y cámaras de seguridad privadas» (*European Parliament, Commission* 2019-24, párr. 12).

Si bien se han logrado importantes avances y hay propuestas adicionales para tener mayor ciberseguridad en Europa, la Comisión Europea también propuso una Ley de Ciber Solidaridad el 18 de abril de 2023. Con esta ley se busca tener mejor preparación y mayores capacidades para detectar «y responder a amenazas y ataques de ciberseguridad significativos y a gran escala» (Comisión Europea, 2023, párr. 2). Esta propuesta también considera la creación de un Escudo Cibernético Europeo conformado por Centros de Operaciones de Seguridad (SOC) interconectados en toda la UE, así como por un Mecanismo de Emergencia de Ciberseguridad global con el objetivo de mejorar la posición cibernética de esta región. Los SOC utilizarán IA y harán análisis de datos para encontrar y compartir información sobre amenazas, incluyendo las trasfronterizas.

j. Ley del mercado de criptoactivos (MICA)

En una publicación del Parlamento Europeo del 1º de abril de 2022 ya señalaba los «peligros de las criptomonedas» y los beneficios que proporcionaría una nueva legislación para regular estas actividades. Por un lado, en su análisis destaca que el mercado de los criptoactivos es atractivo porque no requiere de una entidad centralizada que registre todas las operaciones que en él se realizan, lo que permite que se realicen transacciones de manera simple, segura y anónima entre dos partes sin necesidad de intermediarios.

Por otro lado, el Parlamento Europeo (2022) advirtió sobre los grandes riesgos en el uso de criptomonedas e hizo ver que era necesario tener una legislación europea para enfrentarlos, porque ellos pueden afectar a los usuarios que, generalmente, no tienen ni la debida información ni la protección requerida, poniéndolos en riesgos de pérdidas de dinero. Luego, previno que, ante el creciente número y monto de las inversiones sin la debida regulación, son posibles diversos tipos de manipulaciones y fraudes financieros, lo que puede causar inestabilidad en el mercado financiero. Además, por ser anónimas las

transacciones en criptomonedas expresó que hay sólidos indicios que estos recursos se ha utilizado para actividades ilícitas. Finalmente, se refirió al impacto ambiental negativo que causa el mercado de criptomonedas porque sus tecnologías consumen grandes cantidades de electricidad. Según el Parlamento Europeo (2022) en el caso de Europa el consumo de energía del Bitcoin es tan grande como el total del consumo en algunos países pequeños.

Es de recordar que el Parlamento Europeo también adoptó la legislación sobre el uso de tecnologías de contabilidad distribuida –cadenas de bloques–, para el comercio de criptoactivos en marzo de 2022, las que permiten tener un registro de las acciones que se realizan, así como cada transferencia de criptoactivos. Seguidamente, la UE comenzó a trabajar en una propuesta de ley para responder al creciente uso de los criptoactivos, así como para contener los riesgos que ya se manifestaban en el mercado de criptoactivos. En este contexto, el Parlamento Europeo y el Consejo de la Unión Europea lograron un primer acuerdo el 30 de junio de 2022 y el 20 de abril de 2023, fue formalmente aprobada la Ley MICA (sigla de Markets in Crypto-Assets).

La Ley MICA es un hito porque mantiene el liderazgo de la UE en la regulación financiera a nivel mundial, en este caso, en lo relacionado a la emisión y prestación de servicios con criptoactivos y *stablecoins*. Además, la Ley MICA busca eliminar barreras para facilitar la inclusión financiera, de modo que las finanzas digitales sean accesibles a todos los consumidores y empresas en esta región. Se espera que la Ley MICA sea aplicada entre mediados de 2024 y principios de 2025 (BBVA, 2023).

Según el Artículo 1 de la Ley MICA, el objetivo es establecer normas eficientes para que haya transparencia y la debida información en la emisión y negociación de criptoactivos; en la «autorización y supervisión de los proveedores de servicios de criptoactivos, los emisores de fichas referenciadas a activos y los emisores de fichas de dinero electrónico»; establecer el «funcionamiento, organización y gobernanza de los emisores de fichas referenciadas a activos, los emisores de fichas de dinero electrónico y los proveedores de servicios de criptoactivos»; disponer de «normas de protección de los consumidores en relación con la emisión, la negociación, el canje y la custodia de criptoactivos» así como para tener efectivas medidas para «prevenir el abuso de mercado... (y) garantizar la integridad de los mercados de criptoactivos».

La Ley MICA se aplicará «a toda persona que emita criptoactivos o preste servicios relacionados con los criptoactivos en la Unión» (Art. 2, numeral 1). Seguidamente, señala las entidades y personas que no se no se aplicará esta Ley, como es el caso de: «el Banco Central Europeo, los bancos centrales nacionales de los Estados miembros cuando actúen en su condición de autoridad monetaria, ni otras autoridades públicas»... «las empresas de seguros

ni las empresas que ejerzan las actividades de reaseguro y de retrocesión», a quienes actúen como un «liquidador o administrador» que interviene en «un procedimiento de insolvencia»... «las personas que presten servicios de criptoactivos exclusivamente a sus empresas matrices, a sus filiales o a otras filiales de sus empresas matrices»... «el Banco Europeo de Inversiones»... «la Facilidad Europea de Estabilidad Financiera y el Mecanismo Europeo de Estabilidad»... y «las organizaciones internacionales públicas» (Art. 2, numeral 3).

Luego, en el Artículo 3 formula las definiciones en términos de la Ley MICA, entre los que están:

> a) «Tecnología de registro descentralizado» o «TRD» utilizada para el registro descentralizado de datos cifrados.
> b) «Criptoactivo»: representación digital de valor o derechos que puede transferirse y almacenarse electrónicamente, mediante TDR o con una tecnología similar.
> c) «Ficha referenciada a activos»: tipo de criptoactivo que, a fin de mantener un valor estable, se referencia al valor de varias monedas *fiat* (o fiduciaria emitida por un banco central) de curso legal, una o varias materias primas, uno o varios criptoactivos, o una combinación de dichos activos.
> d) «Ficha de dinero electrónico»: tipo de criptoactivo cuya principal finalidad es la de usarse como medio de intercambio y que, a fin de mantener un valor estable, se referencia al valor de una moneda fiat de curso legal.
> e) «Ficha de servicio»: un tipo de criptoactivo usado para dar acceso digital a un bien o un servicio, disponible mediante TRD, que es aceptado únicamente por el emisor de la ficha en cuestión.
> f) «Emisor de criptoactivos»: persona jurídica que oferta al público cualquier tipo de criptoactivo o que solicita la admisión de cualquier tipo de criptoactivo en una plataforma de negociación de criptoactivos.
> g) Proveedor de servicios de «criptoactivos»: la persona cuya actividad o negocio consiste en la prestación profesional de uno o varios servicios de criptoactivos a terceros.
> h) «Servicio de criptoactivos»: todo servicio y actividad, relacionada con cualquier criptoactivo (enumera ocho servicios).
> i) Y en el numeral 27 define «Información privilegiada» como «cualquier información de carácter concreto que no se haya hecho pública, referida directa o indirectamente a uno o varios emisores de criptoactivos o a uno o varios criptoactivos, y que, de hacerse pública, podría influir de manera apreciable en los precios de dichos criptoactivos».
> j) Cierra con el numeral 28 la definición de «Consumidor», que identifica como «toda persona física que actúe con fines ajenos a su actividad comercial, empresarial, oficio o profesión» (BBVA, 2023).

El estudio del Instituto de la Universidad de las Naciones Unidas para el Agua, el Medio Ambiente y la Salud 24 de octubre de 2023, reveló lo que denominó *el impacto medioambiental oculto del bitcoin* que resulta de la gran dependencia que tiene de los combustibles fósiles la red mundial de minería de las criptomonedas. En efecto, entre 2020-2021 la red mundial de minería de Bitcoin utilizó 173.42 Teravatios hora de electricidad; y la huella de carbono que dejó es equivalente «a quemar 84,000 millones de libras de carbón o hacer funcionar 190 centrales eléctricas de gas natural» (El Mundo, 2023, párr. 7), lo que solo podría compensarse con la plantación de 3,900 millones de árboles en un terrero «casi igual que la de los Países Bajos, Suiza o Dinamarca o el 7 % de la selva amazónica» (Ibidem). Sin embargo, el estudio aclara que no se debería desalentar el uso de las criptomonedas, sino que los gobiernos deberían contar con legislaciones para controlar y mitigar el impacto medioambiental de la minería de las criptomonedas; y las empresas que trabajan con criptomonedas diseñara *criptomonedas ecológicas*.

En efecto, según diversas fuentes ha habido importantes avances en la creación de criptomonedas ecológicas, mediante la generación de protocolos que buscan minimizar el adverso impacto en el medio ambiente y reducir su huella ecológica. Con esta finalidad, ellas utilizan algoritmos de consenso que requieren menos energía para su funcionamiento y utilizan tecnologías de fuentes renovables, como energía solar, eólica, hidroeléctrica, geotérmica, de la biomasa y/o energía marina en vez de combustibles fósiles.

Algunas de las criptomonedas ecológicas que son destacadas con mayor frecuencia por sus buenos protocolos son: Cardano, que tiene un enfoque en la gobernanza descentralizada y su sostenibilidad, Ethereum, Nano, Solana, Shiba inu y Maná.

El Parlamento Europeo también fortaleció las medidas destinadas a la prevención del uso de criptomonedas para actividades delictivas en abril de 2023. La nueva ley se aprobó en mayo de 2023, la que fortaleció las normas para rastrear e identificar las transferencias de criptoactivos, para «evitar su uso en el blanqueo de capitales, la financiación del terrorismo y otros delitos... bloquear las transacciones sospechosas... (y cubrir) las transacciones de criptoactivos superiores a 1,000 euros» (Parlamento Europeo, 2023, párr. 9). Esto se suma al esfuerzo de combatir la evasión y elusión fiscal, como fuera solicitado por el Parlamento Europeo a los estados de la UE en octubre de 2022, para que establecieran una mejor coordinación para gravar los criptoactivos, aplicando un sistema impositivo justo, transparente y eficaz, con un tratamiento tributario simplificado para comerciantes ocasionales o pequeños y de transacciones de bajos montos (Parlamento Europeo, 2023).

Además, se amplió la lista de entidades obligadas, como son instituciones financieras, bancos, agencias inmobiliarias, servicios de gestión de activos, casinos y comerciantes por tener información privilegiada para detectar actividades ilícitas sospechosas. También, cubrirá gran parte del sector criptográfico, para que los proveedores de servicios de criptoactivos realicen lo que se denomina debida diligencia con sus clientes, para comprobar la información que proveen sus clientes e informar sobre actividades sospechosas. En adición, los comerciantes de metales y piedras preciosas, joyerías, relojerías y orfebres de lujo, bienes culturales de alto valor, vendedores de automóviles, aviones y yates de lujo también deberán una debida diligencia (Parlamento Europeo, 2023).

k. Ley de Datos

Después de la aprobación de la Ley de Gobernanza de Datos 6 de abril de 2022, se aprobó la Ley Europea de Datos, el 9 de noviembre de 2023, la cual entrará en vigor el 11 enero de 2024 y deberá aplicarse a partir de septiembre de 2025. Con esta Ley se busca estimular la innovación al eliminar los obstáculos al acceso a los datos y abrirlos a todos los sectores económicos de la UE, mediante la introducción de nuevas regulaciones. Por tanto, de esta manera se logrará un acceso y utilización, así como, una distribución equitativa del valor de los datos en la economía europea, que ahora requiere una mayor y precisa atención ante el creciente uso del Internet de las Cosas. Consecuentemente, al aplicarse esta Ley, todos los productos conectados deberán ser diseñados y fabricados cumpliendo condiciones para que todos los usuarios puedan tener acceso, utilizar y compartir sin dificultades y de manera segura los datos generados. En estas condiciones y considerando que tanto consumidores como empresas generan gran cantidad de datos al utilizar bienes y servicios, Comisión Europea considera que «ambos sectores se beneficiarán de lo siguiente:

- Precios más baratos de los servicios posventa y de reparación de sus objetos conectados.
- Nuevas oportunidades para utilizar servicios basados en el acceso a estos datos.
- Mejor acceso a los datos recogidos o producidos por un dispositivo.
- Nuevas salvaguardias contra las transferencias ilícitas de datos.
- Reducción de los costes por trasladar datos a otro proveedor de servicios en la nube» (Comisión Europea, 2019-2024, párr. 4).

En una publicación del Parlamento Europeo (2023) se estableció el objetivo de la Ley de Datos: «eliminar los obstáculos para reutilizar datos industriales», al tiempo que «para las empresas y consumidores que generan datos, aclara quién puede utilizarlos y en qué condiciones» (párr. 14). En este sentido, la Ley de Datos instaura normas para compartir los datos que se generan cuando se hace uso de productos conectados o servicios asociados y que los usuarios puedan acceder a los datos que ellos han generado. Con esto, también se busca estimular el desarrollo de nuevos servicios, especialmente relacionados con la IA, que requiere una gran cantidad de datos para entrenar los algoritmos.

Otro aspecto interesante de la Ley de Datos es que ella genera condiciones que protegen a las microempresas y las PYMES cuando empresas de mayor calado les tratan de imponerles cláusulas abusivas en los contratos de intercambio de datos. Además, esta Ley contiene normativas para proteger los secretos comerciales.

l. Ley de Inteligencia Artificial de la Unión Europea

La primera propuesta de regulación se presentó el 21 de abril de 2021 y después de múltiples consultas y debates, el Consejo Europeo adoptó la *Ley de Inteligencia Artificial de la Unión Europea* el 21de mayo de 2024. Esta normativa tiene como objetivo establecer un marco normativo y jurídico común para la IA en la UE, para garantizar que los sistemas de IA fueran «seguros, transparentes, trazables, no discriminatorios y respetuosos con el medio ambiente» (Parlamento Europeo, 2023, párr. 2). Luego, el Parlamento Europeo y el Consejo Europeo lograron consensuar entre el 8 y 9 de diciembre de 2023 la versión final de la primera regulación sobre IA en el mundo, la cual establece la base jurídica para la Ley de Inteligencia Artificial de la Unión Europea (AI Act).

Durante el proceso legislativo, la Comisión Europea preparó el estudio denominado Evaluación de Impacto de un Marco Regulatorio para la Inteligencia Artificial (*Impact assessment on a Regulatory Framework for Artificial Intelligence*), que se presentó el 21 de abril de 2021. En el apartado denominado ¿Cuál es el problema y por qué es un problema a nivel de la UE?, señala que la IA es una tecnología emergente «muy poderosa... (con) un fuerte potencial para traer beneficios sociales, crecimiento económico y mejorar la innovación de la UE y la competitividad global». Sin embargo, adicionalmente señaló que, en algunos casos puede generar «nuevos riesgos» en seguridad y protección de los derechos fundamentales de las personas, así como crear inseguridad jurídica para empresas y hacer más lenta la adopción de las tecnologías de IA (European Commission, 2021).

Coincidentemente, Gita Gopinath (2023), Subdirectora Gerente del FMI podría generar grandes beneficios y citó a Goldman Sachs, que estimó que la IA podría aumentar un 7 % la producción mundial en un decenio, esto es, alrededor de US$7 billones. Sin embargo, Gopinath también señaló que, más allá del aumento de la productividad, el mayor uso de IA también podría golpear negativamente al mercado laboral como nunca, por «la pérdida de empleos de "nivel medio" debido a la automatización, lo que ha dado lugar a la formación de grandes grupos de empleos bien pagados y mal pagados en ambos polos de los mercados laborales» (párr. 11). Además, la IA podría presionar «a la baja los salarios de los empleos mejor pagados... (y) reducir las estructuras jerárquicas de las empresas, aumentando el número de trabajadores en puestos subalternos y disminuyendo el número en puestos de dirección intermedia y superior» (Ibidem).

Por tanto, Gopinath señala con precisión que el impacto de la IA el mercado laboral no va a beneficiar a las personas ni el número de ganadores será suficiente «para compensar a los perdedores», porque probablemente IA se limitará «a sustituir empleos humanos sin crear nuevos puestos de trabajo más productivos a los que puedan dedicarse los humanos». Esto lleva a concluir que la pérdida de empleos causaría agitación social, porque la economía funcionará y tendrá beneficios solo «para unos pocos elegidos» (párr. 13).

Más allá de las consideraciones económicas y productivas, el Parlamento Europeo señaló en la resolución del 19 de mayo de 2021 la necesidad que las tecnologías de IA cumplieran condiciones para prevenir prejuicios de género, sociales o culturales, así como la promoción de la diversidad. Concluyeron que todas las tecnologías de IA debían ser reguladas y capacitadas para proteger a las personas de la discriminación y asegurar la igualdad de género, el pluralismo, la diversidad cultural y la lingüística. Además, demandaron que, en el uso de IA en la educación, los maestros siempre deberían corregir la información suministrada por esta tecnología, especialmente en lo relacionado con la selección y evaluación de los estudiantes. Por tanto, recalcaron la necesidad de mejorar las habilidades digitales en Europa y formar a los profesores con capacidades para utilizar la IA en la educación, sin que estas tecnologías los reemplacen, especialmente en la educación infantil (Parlamento Europeo, 2021).

Dicho todo lo anterior, el Parlamento Europeo (2023) definió las obligaciones que deben cumplir los proveedores y usuarios de acuerdo con el nivel de riesgo negativo de los sistemas de IA. En este sentido, definió dos niveles:

- Riesgo inaceptable: Se refiere a los sistemas considerados una amenaza para las personas y que deben prohibirse. Esto incluye la manipulación cognitiva del comportamiento de personas o grupos vulnerables, la

clasificación de personas según su comportamiento o características personales, y los sistemas de identificación biométrica en tiempo real y a distancia, como el reconocimiento facial. Sin embargo, se excluyen de esta prohibición los sistemas de identificación biométrica a distancia a *posteriori* que permitan procesar delitos graves con aprobación judicial previa (Parlamento Europeo, 2023).

- Alto riesgo: son los sistemas de IA que comprometan la seguridad o a los derechos fundamentales y se dividen en dos categorías: (1) los que se utilicen en productos sujetos a la legislación de la UE sobre seguridad de los productos, lo que incluye juguetes, aviación, automóviles, dispositivos médicos y ascensores; y (2) los siguientes sistemas de IA que se han clasificado en 8 áreas específicas, los cuales deberán registrarse en una base de datos de la UE:

    - Categorización biométrica utilizando características sensibles
    - Gestión de infraestructuras críticas
    - Educación y formación profesional
    - Empleo, gestión de trabajadores y acceso al autoempleo
    - Acceso y disfrute de servicios privados esenciales y servicios y prestaciones públicas
    - Aplicación de la ley
    - Gestión de la migración, el asilo y el control de fronteras
    - Asistencia en la interpretación jurídica y aplicación de la ley

El Parlamento Europeo también establece que todos los sistemas de IA catalogados como de alto riesgo deben evaluarse antes de su comercialización y a lo largo de su ciclo de vida (Parlamento Europeo, 2023).

Además, se imponen requisitos de transparencia a las tecnologías que utilizan IA generativa, como ChatGPT y otras aplicaciones similares. Estas tecnologías deben: 1) revelar claramente si el contenido ha sido generado por IA y especificar si un texto, una canción o una fotografía se han creado mediante inteligencia artificial, así como garantizar que los datos utilizados para entrenar a los sistemas respeten los derechos de autor; 2) diseñar el modelo de manera que no pueda utilizarse para generar contenidos ilegales; y 3) publicar resúmenes de los datos protegidos por derechos de autor utilizados para el entrenamiento (Parlamento Europeo, 2023).

Dado que el ChatGPT y las otras aplicaciones similares prácticamente no se conocía cuando se propuso la Ley de Inteligencia Artificial de la UE en 2021, fue necesario incorporar nuevas medidas y salvaguardias. Esto ha llevado a una mayor conciencia de que toda legislación debe ser revisada y adaptada sistemáticamente ante las innovaciones tecnológicas (Ayuso, 2023).

Con relación al tema de vigilancia biométrica, el acuerdo preliminar sobre la Ley de Inteligencia Artificial de la UE se determinó que solo las fuerzas del orden podrán utilizar los sistemas de vigilancia biométrica en tiempo real en espacios públicos, aunque de manera muy limitada y sujetas a estrictas salvaguardias, como autorización judicial y un listado de los delitos a ser investigados. En el caso de la vigilancia en tiempo real, se podrá utilizar solo en «tiempo y locación» y cuando se requiera en procesos de «búsqueda de víctimas de secuestro, tráfico humano o explotación sexual, para la prevención de una amenaza terrorista "genuina y previsible" o "genuina y presente"... o para la localización o identificación de un sospechoso de crímenes específicos: terrorismo, tráfico, asesinato, secuestro, violación, robo armado o un crimen medioambiental, entre otros» (Ayuso, 2023, párr. 11).

Después de extensos debates, el Parlamento Europeo aprobó la Ley de IA el 13 de marzo de 2024, con 523 votos a favor, 46 en contra y 49 abstenciones. Solo queda pendiente la ratificación por parte los Estados miembros de la UA, lo cual podría completarse alrededor de mayo de 2024. Como la aplicación de esta Ley será gradual, se estima que entrará en vigor pleno a fines de 2026. Esta normativa es la primera ley integral sobre IA que existe en el mundo, diseñada para proteger derechos fundamentales ciudadanos sin obstaculizar la innovación en este campo tecnológico.

Según Thierry Breton, Comisario Europeo de Mercado Interior, con la aprobación de la Ley de IA Europa se convierte en un «regulador global de una IA fiable» (Ayuso, 2024, párr. 2). Sin embargo, entrará en vigor antes del terminar 2024 «la prohibición de los sistemas prohibidos de inteligencia artificial, que según el reglamento debe implementarse a los seis meses de aprobada la ley» (párr. 5). No obstante, se estima que uno de los grandes desafíos será la implementación de esta Ley de IA, porque debe regular a las mayores empresas tecnológicas del mundo.

Anexo IV. Regulación de la Inteligencia Artificial en el Reino Unido

La Oficina de Inteligencia Artificial (*Office for Artificial Intelligence – OAI*) presentó al Parlamento en septiembre de 2021 la Estrategia Nacional de IA (*National AI Strategy*) donde se planteó el Plan decenal para hacer de Reino Unido una superpotencia mundial en IA (*Our ten-year plan to make Britain a global AI superpower*). En este documento plantearon el profundo impacto que tendría la IA durante la década por venir en las empresas del Reino Unido y del resto del mundo, al tiempo que destacaba que las universidades y nuevas empresas del Reino Unido ya habían logrado un liderazgo el mundo en el desarrollo y creación de herramientas para la nueva economía. Además, consideraba que el *próspero ecosistema de IA*, la Estrategia Nacional de IA permitiría utilizar todo el potencial de la IA para lograr mayor crecimiento, prosperidad y beneficios sociales para el Reino Unido.

La estrategia planteada para el decenio próximo se basó en tres supuestos:

- «Los principales impulsores del progreso, el descubrimiento y la ventaja estratégica de la IA son el acceso a las personas, los datos, la informática y las finanzas, todos los cuales enfrentan una enorme competencia global;
- La IA se utilizará de manera generalizada en gran parte de la economía y será necesario tomar medidas para garantizar que todos los sectores y regiones del Reino Unido se beneficien de esta transición;
- Nuestros regímenes regulatorios y de gobernanza deberán seguir el ritmo de las demandas rápidamente cambiantes de la IA, maximizando el crecimiento y la competencia, impulsando la excelencia del Reino Unido en innovación y protegiendo la seguridad, las opciones y los derechos de nuestros ciudadanos» (United Kingdom Government, 2022, párr. 23, 24 y 25).

Los objetivos de la Estrategia Nacional de IA del Reino Unido planteados fueron los siguientes:

- «Invertir y planificar las necesidades a largo plazo del ecosistema de IA para continuar nuestro liderazgo como superpotencia científica y de IA;
- Apoyar la transición hacia una economía basada en la IA, aprovechando los beneficios de la innovación en el Reino Unido y garantizando que la IA beneficie a todos los sectores y regiones;

- Garantizar que el Reino Unido implemente correctamente la gobernanza nacional e internacional de las tecnologías de IA para fomentar la innovación, la inversión y proteger al público y nuestros valores fundamentales» (United Kingdom Government, 2022, párr. 27, 28 y 29).

Y concluyeron que para lograr estos objetivos sería necesario tener la confianza y el apoyo público, lo cual se podría lograr abriendo espacios para la participación de todos los talentos y puntos de vista de la sociedad. Luego, para dar a conocer los avances en la Estrategia Nacional de IA, la OAI publicó el 18 de julio de 2022, en línea con el objeto de convertir al Reino Unido en una superpotencia mundial en IA centro mundial para la creación, desarrollo e innovación de la IA (United Kingdom Government, 2022).

El Proyecto de Ley de Protección de Datos e Información Digital (DPDIB, *Data Protection and Digital Information Bill*), cuya impresión fue ordenada por la Cámara de los Comunes el 18 de julio de 2022, incluyó un conjunto de nuevas propuestas de regulación de la inteligencia artificial (IA). Este Proyecto ignoró las normas establecidas en el Reglamento General de Protección de Datos (RGPD) de la UE, lo que demostró su independencia de la organización europea después del Brexit, ocurrido el 31 de enero de 2020. Además, buscó potenciar el desarrollo de la industria de la IA en el Reino Unido.

En la DPDIB se estableció como objetivo[1] :

- «Hacer provisiones para la regulación del procesamiento de información relativa a personas vivas identificadas o identificables;
- Hacer provisiones para la regulación del tratamiento de la información relativa a individuos vivos identificados o identificables;
- Hacer provisiones sobre servicios consistente en el uso de información para conocer y verificar hechos sobre individuos;
- Establecer disposiciones sobre el acceso a los datos de los clientes y a las empresas datos; Unesco
- Establecer disposiciones sobre privacidad y comunicaciones electrónicas;
- Establecer disposiciones sobre servicios para la provisión de firmas electrónicas, sellos electrónicos y otros servicios fiduciarios;
- Hacer provisiones sobre la divulgación de información para mejorar la prestación de servicios públicos;
- Establecer disposiciones para la implementación de acuerdos sobre el intercambio de información para fines de aplicación de la ley;
- Establecer disposiciones sobre cómo llevar y mantener los registros de nacimientos y defunciones;
- Hacer provisiones sobre estándares de información para la atención sanitaria y social;

[1] Traducción personal de la Ley, sólo de manera indicativa. Para conocer el texto oficial se debe tomar su versión en inglés.

- Para establecer la Comisión de Información;
- Formular disposiciones sobre la supervisión de los datos biométricos y para propósitos conectados» (p. 1).

Guillermo Caro (2022) señala que este Reglamento propugna seis principios fundamentales: «1) Garantizar el uso seguro de la IA; 2) Incorporar la seguridad por diseño en los sistemas de IA; (3) Hacer que estos sistemas sean transparentes; 4) Considerar la equidad; 5) Garantizar que las organizaciones designen a una persona legalmente responsable de la IA; y 6) Dejar claras las vías de reparación para los clientes» (párr. 9, 10 y 11).

Tras meses de trabajo, el Departamento de Ciencia, Innovación y Tecnología del Gobierno del Reino Unido presentó el 29 de marzo de 2023 el informe *Un enfoque pro-innovación para la regulación de la IA* (A *pro-innovation approach to AI regulation*), con características de un libro blanco, mediante el cual se dio a conocer la propuesta del Gobierno para regular la IA. En el numeral 4 del Resumen Ejecutivo del documento *Inteligencia artificial: la oportunidad y el desafío* señala que «Si bien debemos capitalizar los beneficios de estas tecnologías, tampoco debemos pasar por alto los nuevos riesgos que pueden surgir de su uso, ni la inquietud que la complejidad de las tecnologías de IA puede producir en el público en general... (porque) algunos usos de la IA podrían dañar nuestra salud física y mental, infringir la privacidad de las personas y socavar los derechos humanos» (United Kingdom Government, 2023), así como su seguridad personal.

En respuesta estos riesgos, en el numeral 10 del apartado *Nuestro marco pro-innovación*, fija los cinco principios «para guiar e informar el desarrollo y uso responsable de la IA en todos los sectores de la economía»:

1. «Seguridad, protección y solidez», para tener la seguridad que los riesgos son gestionados de manera eficiente.
2. «Transparencia y explicaciones adecuadas» en términos de cómo se desarrolla e implementa la IA, cómo se utiliza y los riesgos que presenta su utilización.
3. «Justicia» para que haya equidad, para que no haya discriminación ni se saquen ventajas comerciales indebidas.
4. «Responsabilidad y gobernanza» para asegurar que existe una debida supervisión sobre el uso de la IA y sobre los resultados obtenidos.
5. «Impugnabilidad y reparación» para que los usuarios tengan la oportunidad para impugnar resultados y señalar decisiones perjudiciales por la mala información provista por la IA (United Kingdom Government, 2023).

Con este tipo de regulación, el Reino Unido deja abiertas las opciones para adaptarla para responder a los avances de la tecnología de IA, para proteger a los usuarios sin que estas medidas puedan frenar o limitar su uso en las empresas para fortalecer el crecimiento de la economía.

Así es como la Autoridad de Competencia y Mercados (*Competition and Markets Authority*, CMA) de Reino Unido propuso siete principios básicos sobre la IA para garantizar, la protección de los usuarios y mantener una libre y sana competencia para estimular su desarrollo y uso responsable, especialmente del ChatGPT y Office 365 Copilot, sin dejar de lado los riesgos por los oligopolios y su uso para desinformar, dado que «Las personas podrían estar expuestas a niveles significativos de información falsa y engañosa y a fraude impulsado por la IA... (mientras que) En el largo plazo, un puñado de empresas podrían utilizar los modelos para ganar o afianzar posiciones de poder de mercado y no ofrecer los mejores productos y servicios y/o cobrar precios altos» (ReasonWhy, 2023, párr. 3).Los siete principios rectores propuestos por la CMA son los siguientes: 1) Responsabilidad: que define a los desarrolladores e implementadores tecnologías de IA como responsables de los resultados proporcionados a los usuarios; 2) Acceso: que consiste en facilitar el acceso continuo y sin restricciones de la información clave que es utilizada en los procesos de entrenamiento; 3) Diversidad: para ofrecer modelos de negocio diversos abiertos o cerrados; 4) Elección: para que los usuarios tenga múltiples opciones para decidir cómo utilizar las aplicaciones de IA; 5) Flexibilidad: para que los usuarios puedan cambiar y/o utilizar múltiples modelos según sus necesidades; 6) Trato justo: para evitar y castigar conductas anticompetitivas, como autopreferencia, vinculación o agrupación de productos y servicios; y 7) Transparencia: para que los usuarios tengan toda la información sobre riesgos y limitaciones del contenido que provee la aplicación de IA para la toma de decisiones.

En el desarrollo de la normativa para controlar el desarrollo de la IA es de destacar la decisión de la Corte Suprema del Reino Unido que rechazó que a IA pueda ser considerada legalmente como inventora como medio para garantizar derechos de una patente. Así concluyó el caso presentado por el desarrollador estadounidense Stephen Thaler que había solicitado que su IA Dabus se considerara como la inventora de un contenedor de alimentos y una baliza luminosa, dejando claro que solo una persona física –no una máquina– puede designarse inventora. Sin embargo, expertos en litigios de propiedad intelectual consideran que esta sentencia no significa que no se pueda utilizar IA para crear una invención y luego pedir que se le patente como inventor (M. J., 2023).

Thaler tampoco obtuvo una decisión favorable en EUA, pero contrariamente, logró en Sudáfrica que Dabus fuera reconocido como inventor en una patente;

y en Australia, el Tribunal Federal dictaminó que la IA también puede ser considerada como un inventor. El futuro jurídico de la IA será parte de numerosos debates y de decisiones trascendentales, especialmente en los derechos de autor de las obras creadas mediante el uso de IA.

En un artículo de Imelda Reddington (2021) presentó la forma cómo se comenzaría a aplicar la Ley de Propiedad Intelectual a partir del 1º de enero de 2021, una vez terminado el período de transición. Siguiendo el nuevo ordenamiento jurídico, la Oficina de Propiedad Intelectual creó una marca registrada en el Reino Unido para toda aquella que se había registrado en la UE (EUTM sigla en inglés de *European Union Trade Mark*) y para cada diseño comunitario registrado (RCD sigla en inglés de *Registered Community Design*). Para tener los beneficios de esta Ley se estableció que todo propietario debía tener una inscripción en el registro de marcas/diseños del Reino Unido; cumplir los requisitos legales como si hubieran hecho la solicitud y la hubiera registrado de acuerdo con la ley del Reino Unido; conservar la fecha de presentación original de la EUTM/RCD; mantener la fecha original de prioridad o de antigüedad en el Reino Unido; ser una marca registrada/diseño en el Reino Unido totalmente independiente, que pueda ser rebatida, asignada o renovada como licencia.

Una vez terminada la revisión sobre la Regulación Pro-innovación para las Tecnologías Digitales, se recomendó que el Gobierno del Reino Unido aclarara la relación entre la propiedad intelectual y la IA generativa que fue aceptada el 15 de marzo de 2023. Así fue como se comenzó a preparar un código de prácticas sobre los derechos de autor e IA. Como objetivo de este código se estableció facilitar que las licencias para la minería de datos estén totalmente disponibles, por considerarse que se deben superar las barreras que enfrentaban las empresas y usuarios de IA, así como garantizar las debidas protecciones para los titulares de derechos de propiedad, como medio para promover y recompensar la inversión en creatividad y facilitar que el Reino Unido sea un líder mundial en investigación e innovación en IA (United Kingdom Government, 2023).

Para sustentar su trabajo de preparación del Código de prácticas del gobierno sobre derechos de autor e inteligencia artificial (*The government's code of practice on copyright and AI*), la Oficina de Propiedad Intelectual del Reino Unido invitó a representantes de las empresas de tecnologías, creativos e investigadores como fuentes de consultas a partir del 5 de junio de 2023, para que la propuesta de código sea equilibrado y pragmático. Entre los términos de referencia para el desarrollo del trabajo se deben definir tanto los derechos de propiedad intelectual como derechos de autor, los derechos de bases de datos, los derechos sobre prácticas y los derechos morales (United Kingdom Government, 2023).

En el informe de la Comisión de Cultura, Medios y Deporte, denominado *Connected tech: AI and creative technology* (Tecnología conectada: IA y Tecnología creativa) que presentó el Comité de Cultura, Medios y Deportes como respuesta del gobierno al Parlamento del Reino Unido expusieron sus recomendaciones sobre la regulación de la IA, manteniendo un enfoque pro-innovación para posicionar al país como líder mundial en IA, en un ambiente de confianza en el uso de esta tecnología con el objetivo d impulsar el crecimiento económico y la prosperidad.

1. El Gobierno debe establecer un plan para proporcionar capacitación y recursos a los reguladores del sector no digital para garantizar que puedan satisfacer las necesidades del nuevo régimen regulatorio intersectorial para la IA (párrafo. 20). De acuerdo con lo que se estableció en el libro blanco, el Gobierno ya está trabajando formar y orientar a los reguladores en los métodos para aplicar los principios regulatorios y para comprender los riesgos y desafíos emergentes que plantean los desarrollos en IA.

2. El Gobierno debe establecer una unidad de coordinación de la regulación de la IA para garantizar un trabajo coherente y permitir una sólida participación de las partes interesadas. Esta unidad debe publicar informes periódicos para que el Parlamento evalúe a profundidad el progreso en la implementación del régimen normativo (párrafo 21). Con este fin, se definieron las funciones de una central de riesgo, así como para la coordinación de trabajo entre todos los departamentos gubernamentales para la aplicación conjunta del régimen regulatorio.

3. El Comité recomendó al Gobierno que no preparara planes para una exención amplia de los derechos de autor para la minería de datos y textos, sino que dar un apoyo proactivo a los pequeños desarrolladores de IA, para que puedan para conseguir sus licencias de manera más fácil. Con esta finalidad, propuso lograr acuerdos con organizaciones de gestión de derechos y organismos comerciales de industrias creativas. Además, recomendó que el Gobierno mantuviera un régimen de derechos de autor fuerte ante solicitudes de licencias para utilizar contenido protegido por derechos de autor en IA; y que los creadores sean bien recompensados en el régimen de derechos de autor (párrafo 31).

4. El Gobierno debe trabajar para recuperar la confianza de las industrias creativas tras su Intento fallido de introducir una exención amplia de minería de datos y textos. El Gobierno debería considerar cómo los creativos pueden garantizar la transparencia y, si es necesario, el recurso y reparación si sospechan que los desarrolladores de IA están utilizando indebidamente sus trabajos en el desarrollo de IA (párrafo 32).

5. El Comité también señaló que Gobierno debería mantener procesos de actualización significativos sobre su desempeño en la gestión del impacto de la IA en las industrias creativas y cualquier discusión sobre estos temas al final de 2023 (párrafo 33).

6. Finalmente, el Comité le sugirió al Gobierno trabajar para mejorar la protección de los creativos para evitar el uso indebido de sus semejanzas y desempeño de tecnologías emergentes como la IA generativa. En adición, señaló que, como mínimo, se debería adelantar la ratificación del Tratado de Beijing sobre el sector audiovisual (párrafo 61).

En adición, con relación a la minería de textos y datos el Comité de Cultura, Medios y Deportes hizo ver que la reproducción mediante IA de obras protegidas por derechos de autor podría violar los derechos de autor, salvo que lo permita una licencia o una excepción. En este sentido, el código de prácticas sobre derechos de autor e IA busca permitir que la IA y los sectores creativos crezcan en asociación y se mantenga el apoyo y estímulo a la inversión en creatividad (párrafo 31).

En relación con el Tratado de Beijing sobre Interpretaciones y Ejecuciones Audiovisuales (*Beijing Treaty on Audiovisual Performances*) que fue firmado por la Unión Europea el 10 de junio de 2013. Este es un Tratado internacional que tiene como objetivo conferir derechos de propiedad intelectual a las interpretaciones y ejecuciones audiovisuales. El Reino Unido también firmó este Tratado en 2013, pero no lo pudo ratificar cuando era miembro de la UE, que luego del Brexit se comprometió a ratificar e implementar (EUR-Lex, 2023).

Según el Comité de Cultura, Medios y Deportes, la legislación del Reino Unido ya cumple en gran parte con el Tratado; sin embargo, hay ciertas áreas de la ley donde será necesario hacer cambios para proteger a los artistas audiovisuales y evitar todo trato ofensivo de sus interpretaciones. Ante esta situación, el Gobierno del Reino Unido continúa trabajando para establecer los derechos de propiedad intelectual para las interpretaciones audiovisuales, incluyendo las actuaciones de actores, músicos, bailarines y otros artistas que sean incorporados en películas, programas de televisión y otras grabaciones audiovisuales (párrafo 61). No obstante, preocupa en el Reino Unido que el Tratado no tiene disposiciones específicas para que los artistas audiovisuales protejan sus derechos contra, por ejemplo, los *deepfakes* que se pueden generar utilizando IA.

Para formular la propuesta de Ley el Comité de Cultura, Medios y Deportes realizó consultas que se cerraron el 9 de noviembre de 2023, para tener la mayor información posible para formular un conjunto de reformas de derechos de autor para los artistas intérpretes o ejecutantes en películas, programas de

televisión y vídeos musicales. Así, el Reino Unido espera cumplir a cabalidad con el Tratado de Beijing, que es actualmente administrado por la Organización Mundial de la Propiedad Intelectual.

Anexo V. Legislación en Estados Unidos de América

El presidente de Estados Unidos, Joseph R. Biden firmó el 30 de octubre de 2023 el *Decreto Ejecutivo sobre el desarrollo y uso seguro y confiable de la inteligencia artificial (Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*), que tiene como objetivo reducir los riesgos de un desarrollo sin control de esta tecnología (The White House, 2023). En su presentación, el presidente Biden reconoció que la IA transformará la forma cómo vive la gente y que ella conlleva grandes desafíos, ante lo cual fue enfático al expresar que «La tecnología debe ser gobernada, no puede haber discusión» (Seisdedos, 2023, párr. 1)

En su discurso también señaló: «Vamos a asistir a cambios tecnológicos más profundos en los próximos cinco años que en los últimos 50. En gran parte (la IA), está mejorando nuestras vidas, nos ayudará a explorar el universo, a predecir el tiempo, a acabar con el cáncer... pero también las está empeorando. Por ejemplo, permite emplear los datos personales de los adolescentes para descubrir qué los mantendrá pegados a sus teléfonos, o cómo hacer que las redes sociales sean más adictivas... (con) el potencial de provocar un profundo daño a su salud mental y a su bienestar» (The White House, 2023, párr. 2). Todo esto, sin olvidar los peligros asociados con los *deep fakes*, que son utilizados para difamar, difundir noticias falsas y cometer fraudes.

Este Decreto Ejecutivo se consideró como un mensaje de liderazgo y acción estratégica previa a la participación de EUA en la Primera Cumbre Mundial sobre los Riesgos de la IA que se realizó en Bletchley Park, Reino Unido el 1º de noviembre de 2023, en busca de acuerdos a nivel mundial (France24.com, 2023).

El Decreto Ejecutivo (The White House, 2023) contiene 13 secciones que especifican todo el trabajo a realizar: 1) el *Objeto*, 2) la *Política y Principios*, 3) las *Definiciones*, 4) cómo *Garantizar la seguridad de la tecnología de IA*; 5) la *Promoción de la innovación y la competencia*, 6) sobre los *Trabajadores de apoyo*, 7) la *Promoción de la equidad y los derechos civiles*, 8) la *Protección de Consumidores, Pacientes, Pasajeros y Estudiantes*, 9) la *Protección de la privacidad* 10) cómo *Impulsar el uso de la IA por parte del gobierno federal*, 11) el *Fortalecimiento del liderazgo estadounidense en el exterior*, 12) metodología de la *Implementación*, y 13) las *Disposiciones Generales*, las cuales se presentan

a continuación tomando como base lo que expone textualmente el Decreto.

Sección 1. Objeto. Reconoce que la IA tiene un potencial prometedor extraordinario, pero también peligroso. Por un lado, el uso responsable de la IA puede ayudar a resolver desafíos urgentes y contribuir a que el mundo sea más próspero, productivo, innovador y seguro. Pero su uso irresponsable podría exacerbar daños sociales como el fraude, la discriminación, los prejuicios y la desinformación; desplazar y quitar poder a los trabajadores; reprimir la competencia; y plantean riesgos para la seguridad nacional. Por tanto, para aprovechar los innumerables beneficios de la IA es necesario mitigar sus riesgos, lo que requiere la participación de toda la sociedad: gobierno, sector privado, academia y sociedad civil.

Además, como las capacidades de la IA progresan con rapidez, esto impulsa a EE. UU. a tomar el liderazgo en este momento, para asegurar la seguridad, economía y sociedad estadounidense, al mismo tiempo que garantizar seguridad y oportunidades para todos.

Sección 2. Política y Principios. Se establecen ocho principios rectores y prioridades para el desarrollo y uso de la IA:

> «(a) La Inteligencia Artificial debe ser segura y protegida».
>
> «(b) Promover la innovación, la competencia y la colaboración responsables permitirá a Estados Unidos liderar la IA y desbloquear el potencial de la tecnología para resolver algunos de los desafíos más difíciles de la sociedad».
>
> «(c) El desarrollo y uso responsable de la IA requiere un compromiso de apoyar a los trabajadores estadounidenses (para lo cual se) buscará adaptar la capacitación y la educación laboral para respaldar una fuerza laboral diversa y ayudar a brindar acceso a las oportunidades que crea la IA».
>
> «(d) Las políticas de Inteligencia Artificial deben ser consistentes... para promover la equidad y los derechos civiles».
>
> «(e) Se deben proteger los intereses de los estadounidenses que utilizan, interactúan o compran cada vez más IA y productos habilitados para IA en su vida diaria. El uso de nuevas tecnologías, como la IA, no exime a las organizaciones de sus obligaciones legales, y las protecciones al consumidor... El Gobierno Federal hará cumplir las leyes y principios existentes de protección del consumidor y promulgará salvaguardias adecuadas contra el fraude, los prejuicios involuntarios,

la discriminación, las infracciones de la privacidad y otros daños causados por la IA. ... (especialmente) en campos críticos como la atención médica, los servicios financieros, la educación, la vivienda, el derecho y el transporte, donde los errores o el uso indebido de la IA podrían dañar a los pacientes, costar a los consumidores o a las pequeñas empresas, o poner en peligro la seguridad o los derechos».

«(f) Se debe proteger la privacidad y las libertades civiles de los estadounidenses... (porque) la IA hace que sea más fácil extraer, reidentificar, vincular, inferir y actuar sobre información confidencial relativas a identidades, ubicaciones, hábitos y deseos de las personas. Las capacidades de la IA en estas áreas pueden aumentar el riesgo de que los datos personales sean explotados y expuestos. ... (por lo cual) el Gobierno Federal garantizará que la recopilación, el uso y la retención de datos sean legales, seguros y mitiguen los riesgos de privacidad y confidencialidad».

«(g) Es importante gestionar los riesgos del uso de la IA por parte del propio Gobierno Federal y aumentar su capacidad interna para regular, gobernar y apoyar el uso responsable de la IA para ofrecer mejores resultados para los estadounidenses».

«(h) El Gobierno Federal debe liderar el camino hacia el progreso social, económico y tecnológico global, como lo ha hecho Estados Unidos en épocas anteriores de innovación y cambios disruptivos. ... Un liderazgo eficaz también significa ser pionero en aquellos sistemas y salvaguardas necesarios para implementar la tecnología de manera responsable, y construir y promover esas salvaguardas con el resto del mundo. (La) Administración colaborará con aliados y socios internacionales en el desarrollo de un marco para gestionar los riesgos de la IA, liberar su potencial para el bien y promover enfoques comunes para los desafíos compartidos. El Gobierno Federal buscará promover principios y acciones responsables de seguridad de la IA con otras naciones, incluidos nuestros competidores, al tiempo que lidera conversaciones y colaboraciones globales clave para garantizar que la IA beneficie a todo el mundo, en lugar de exacerbar las desigualdades, amenazar los derechos humanos y causar otros daños».

Sección 3. Definiciones, incluye 37 casos específicos.

Sección 4. Garantizar la seguridad de la tecnología de IA. Contiene ocho mandatos:

«4.1 Desarrollo de directrices, estándares y mejores prácticas para la seguridad y protección de la IA... Dentro de los 270 días siguientes a la fecha de esta Decreto».

«4.2 Garantizar una IA segura y confiable. Dentro de los 90 días siguientes a la fecha de este Decreto, garantizar y verificar la disponibilidad continua de IA segura, confiable y eficaz de conformidad con la Ley de Producción para la Defensa» (del 8 de septiembre de 1950, emitida en respuesta al inicio de la Guerra de Corea, con el objetivo de promover las defensas civiles y estimular la movilización).

«4.3 Gestión de la IA en infraestructuras críticas y ciberseguridad».

«4.4 Reducir los riesgos en la intersección de las amenazas de IA y las amenazas CBRN (siglas en inglés de Chemical, Biological, Radiological and Nuclear, en español, Química, Biológica, Radiológica y Nuclear)».

«4.5. Reducir los riesgos que plantea el contenido sintético».

«4.6. Solicitar información sobre modelos de cimentación de doble uso con pesos de modelo ampliamente disponibles».

«4.7. Promoción de la divulgación segura y prevención del uso malicioso de datos federales para la capacitación en inteligencia artificial».

«4.8. Dirigir la formulación de un memorando de seguridad nacional».

Sección 5. Promoción de la innovación y la competencia. Consta de tres condicionantes: «5.1. Atraer talento en IA a Estados Unidos; 5.2. Promoción de la innovación. Desarrollar y fortalecer asociaciones público-privadas para promover la innovación, la comercialización y los métodos de mitigación de riesgos para la IA, y ayudar a promover sistemas de IA seguros, responsables, justos, que protejan la privacidad y sean confiables; y 5.3. Promoción de la competencia».

Sección 6. Trabajadores de apoyo. Esta en sección, se busca proteger a los trabajadores por lo cual se ordena:

«(a) Mejorar la comprensión por parte del Gobierno de las implicaciones de la IA para los trabajadores».

«(b) Ayudar a garantizar que la IA implementada en el lugar de trabajo promueva el bienestar de los empleados».

> «(c) Para fomentar una fuerza laboral diversa preparada para la IA, ... (se) priorizarán los recursos disponibles para apoyar la educación relativa a la IA y el desarrollo de la fuerza laboral relacionada con la IA a través de programas existentes».

Sección 7. Promoción de la equidad y los derechos civiles. Incluye tres mandatos: «7.1. Fortalecimiento de la IA y los derechos civiles en el sistema de justicia penal; 7.2. Protección de los derechos civiles relacionados con los beneficios y programas gubernamentales; y 7.3. Fortalecimiento de la IA y los derechos civiles en la economía en general».

Sección 8. Protección de Consumidores, Pacientes, Pasajeros y Estudiantes. Contiene cinco sugerencias de acciones a realizar:

> «(a) Se alienta a las agencias reguladoras independientes... a considerar el uso de toda su gama de autoridades para proteger a los consumidores estadounidenses del fraude, la discriminación y las amenazas a la privacidad y para abordar otros riesgos que puedan surgir del uso de la IA, incluidos riesgos para la estabilidad financiera y considerar la elaboración de normas, además de enfatizar o aclarar dónde se aplican las regulaciones y directrices existentes a la IA, ... realizar la debida diligencia y monitorear cualquier servicio de IA de terceros que utilicen, ... aclarar los requisitos y expectativas relacionados con la transparencia de los modelos de IA y la capacidad de las entidades reguladas para explicar su uso de modelos de IA».

> «(b) Ayudar a garantizar el despliegue y uso seguro y responsable de la IA en los sectores de atención sanitaria, salud pública y servicios humanos».

> «(c) Promover el desarrollo y uso seguro y responsable de la IA en el sector del transporte...».

> «(d) Ayudar a garantizar el desarrollo y la implementación responsables de la IA en el sector educativo».

> «(e) Se alienta a la Comisión Federal de Comunicaciones a considerar acciones relacionadas con la forma cómo la IA afectará a las redes de comunicaciones y a los consumidores».

Sección 9. Protección de la privacidad. Esta Sección establece tres mandatos:

«(a) Mitigar los riesgos de privacidad potencialmente exacerbados por la IA, incluido el hecho de que la IA facilite la recopilación o el uso de información sobre individuos, o la realización de inferencias sobre individuos».

«(b) Permitir que las agencias utilicen tecnologías que mejoran la privacidad (PET por sus siglas en inglés de Privacy-Enhancing Technologies) para salvaguardar la privacidad de los estadounidenses de las amenazas potenciales exacerbadas por la IA».

«(c) Avanzar en la investigación, el desarrollo y la implementación relacionados con los PET».

Sección 10. Impulsar el uso de la IA por parte del gobierno federal. Con esta finalidad le demanda: «10.1. Proporcionar orientación para la gestión de la IA; y 10.2. Aumentar del talento de IA en el gobierno».

Sección 11. Fortalecimiento del liderazgo estadounidense en el exterior. En concordancia con lo que se acordaría en la Cumbre de *Bletchley Park*, se señala que se debe:

«(a) Fortalecer el liderazgo de los Estados Unidos en los esfuerzos globales para liberar el potencial de la IA y enfrentar sus desafíos».

«(b) Promover estándares técnicos globales responsables para el desarrollo y uso de la IA fuera de las áreas militares y de inteligencia».

«(c) Promover el desarrollo y el despliegue de IA en el extranjero de forma segura, responsable y que afirme los derechos».

«(d) Abordar los riesgos transfronterizos y globales de la IA para la infraestructura crítica, (para lo cual) el Secretario de Seguridad Nacional, en coordinación con el Secretario de Estado y en consulta con los jefes de otras agencias relevantes según lo considere apropiado, deberá liderar esfuerzos con aliados y socios internacionales para mejorar la cooperación para prevenir, responder y recuperarse de posibles interrupciones de la infraestructura crítica resultantes de la incorporación de IA en sistemas de infraestructura crítica o el uso malicioso de la IA».

Sección 12. Implementación. Lo importante de esta Sección es que

«(a) Se establece, dentro de la Oficina Ejecutiva del Presidente, el Consejo de Inteligencia Artificial de la Casa Blanca (con la función de)

> coordinar las actividades de las agencias de todo el Gobierno Federal para garantizar la formulación, el desarrollo, la comunicación, la participación de la industria y la implementación oportuna de políticas relacionadas con la IA».

Sección 13. Disposiciones Generales, donde se establece que este Decreto «se implementará de conformidad con la ley aplicable».

Aunque ya se había dado a conocer públicamente el Decreto Ejecutivo sobre el desarrollo y uso seguro y confiable de la inteligencia artificial, el Congreso de los EUA desde hacía meses estaba dando seguimiento a los problemas relacionados con el mal uso de diversas plataformas digitales por depredadores sexuales, así como la introducción de desafíos que han causado daños físicos y muertes, la generación de situaciones que terminan siendo adictivas y que causan trastornos en la alimentación, la manipulación utilizando modelos de belleza difíciles de alcanzar y múltiples otras situaciones de riesgo.

Como muestra de su preocupación y buscando respuestas, el Senado de los EUA interpeló el 31 de enero de 2024 a Mark Zuckerberg, consejero delegado de Meta, la compañía matriz de Facebook; Linda Yaccarino, de X; Shou Zi Chew, de TikTok; Jason Citron, de Discord, y Evan Spiegel, de Snap ante los múltiples daños causados por los depredadores que utilizan sus plataformas, así como la urgencia de crear una legislación contra los depredadores que utilizan las redes sociales. Desde un inicio los senadores mostraron una posición muy crítica. Así es como el senador republicano Lindsey Graham les señaló: «Ustedes y sus empresas, sabemos que no es esa su intención, pero tienen las manos manchadas de sangre. Hacen un producto que mata gente» (Vidal Liy, 2024, párr. 1).

En la audiencia estaban presentes padres de niños y jóvenes que habían sido víctimas de abusos y acosos en redes que los llevaron a suicidarse. A esto se agrega la difusión de estándares de belleza, retos de diversos tipos y conceptos de felicidad prácticamente imposibles de lograr, lo que termina causando «depresión, trastornos psicológicos y de alimentación» (Vidal Liy, 2024, párr. 2), así como adicción. Ante esta deplorable situación, se acusa a las empresas tecnológicas que crearon este tipo de plataformas de no hacer los suficientes esfuerzos para proteger a los menores y jóvenes, dando prioridad a tener grandes ganancias ante la falta de una debida normativa.

Ante esta situación, el senador demócrata Jon Ossoff señaló: «Son familias que han perdido a sus hijos... Son familias de todo el país cuyos hijos se han autolesionado, que han padecido baja autoestima, a los que les han vendido píldoras mortales en internet... Internet es un lugar peligroso para los niños, y sus plataformas son lugares peligrosos para los niños... (y) No existe ninguna

herramienta para que las empresas se vean obligadas a rendir cuentas» (Vidal Liy, 2024, párr. 4). Este duro señalamiento lo presentó Ossoff ante la audiencia, donde estaban presente padres que portaban fotos de sus hijos fallecidos.

En adición, la senadora demócrata Amy Klobuchar al comparar las leyes que controlan otras industrias para su bien funcionamiento preguntó: «¿por qué no tomamos con la misma determinación medidas parecidas contra el peligro que representan estas plataformas, cuando sabemos que hay niños muriendo?... Es hora de aprobar medidas» (Vidal Liy, 2024, párr. 17). Todo esto contribuyó a que comenzaran a estudiarse proyectos de ley para garantizar la protección de los menores en las redes sociales.

Anexo VI. Regulación de la IA en la República Popular China

El gobierno de la República Popular China ha sido muy activo en la formulación de un Plan de País, de una serie de layes, normas y documentos orientadores en torno al uso de tecnologías, especialmente del área de IA, entre las que destacan:

1. Reglamento sobre la Administración de los Servicios de Información de Noticias en Internet del 25 de septiembre de 2005.
2. Plan *Made in China* 2025, presentado en 2015.
3. Ley de Ciberseguridad de la República Popular China del 1º de junio de 2017.
4. Plan de desarrollo de inteligencia artificial de próxima generación, presentado el 8 de julio de 2017.
5. Marco de IA Confiable propuesto en julio de 2021.
6. Normas Éticas para la Inteligencia Artificial de Nueva Generación 25 de septiembre de 2021.
7. Orientación sobre el fortalecimiento de la gobernanza integral de los algoritmos de los servicios de información de Internet, presentado el 29 de septiembre de 2021.
8. Ley de Protección de Datos Personales o Ley de Seguridad de Datos de la República Popular China del 30 de septiembre de 2021.
9. Ley de Protección de Información Personal de la República Popular China del 20 de agosto de 2021, en vigor desde el 10 de noviembre de 2021.
10. Disposiciones de gestión de recomendaciones algorítmicas del servicio de información de Internet, en vigor el 10 de marzo de 2022 –modificó la normativa de septiembre de 2021–.

11. Medidas para la Administración de Servicios de Inteligencia Artificial Generativa, en vigencia desde el 1 de enero de 2023

1. El Reglamento sobre la Administración de los Servicios de Información de Noticias en Internet (互联网新闻信息服务管理规定) entró en vigor el 25 de septiembre de 2005 (WIPO Lex, 2005), normativa que fue preparada por la Oficina de Información del Consejo de Estado y el Ministerio de Industria de la Información de la República Popular China. Si bien su visión se dio antes del impacto de las nuevas aplicaciones y de la IA, este Reglamento tuvo una concepción eminentemente reguladora, puesto que su objeto fue «estandarizar los servicios de información de noticias de Internet y satisfacer la demanda del público de información de noticias de Internet» para mantener «la seguridad nacional y los intereses públicos, proteger los derechos e intereses legítimos de las unidades de servicios de información de noticias de Internet y promover la información de noticias de Internet» de modo que se pudiera «asegurar el sano y ordenado desarrollo de los servicios de información» (Artículo 1).

Luego señala, que todo proveedor «de servicios de información de noticias de Internet dentro del territorio de la República Popular China» deberá cumplir con las regulaciones establecidas en este Reglamento, lo cual aplica a toda «información de noticias de actualidad, incluida la política, la economía, el ejército, la diplomacia, etc.... (así como a) Informes y comentarios sobre asuntos sociales y públicos, así como informes y comentarios sobre emergencias sociales» difundida por internet (Artículo 2). Y cierra la visión reguladora al señalar que quienes se dediquen proveer servicios de información en internet «deberán cumplir con la Constitución y las leyes y reglamentos, adherirse a la dirección de servir al pueblo y al socialismo, adherirse a la dirección correcta de la opinión pública, salvaguardar el interés de la patria interés y el interés público», alentando a que estas organizaciones «a difundir información que sea beneficiosa para mejorar la calidad nacional, promover el desarrollo económico y promover información de noticias sanas y civilizadas sobre el progreso social» (Artículo 3).

2. China dejó en claro que busca convertirse en una potencia con la capacidad de liderar e influir en los estándares mundiales de innovación y en las cadenas de suministros hacia 2030. Con este objetivo, el Ministerio de Industria y Tecnologías de Información formuló en 2015 el *Plan Made in China* 2025, que presenta una visión de largo alcance e identifica nueve funciones estratégicas con una clara visión de mercado:

> «(1) alentar la innovación; (2) promover el uso de manufacturas integradas, digital y centrada en alta tecnología; (3) fortalecer la base industrial general; (4) mejorar la calidad de los productos y crear marcas globales chinas; (5) enfocar los esfuerzos en la aplicación de

métodos de fabricación ecológicos; (6) reestructurar las industrias para mejorar la eficiencia y la producción; (7) mejorar las industrias de servicios de manufactura y fabricación orientadas a los servicios; (8) globalizar las industrias manufactureras chinas; y (10) realizar innovaciones tecnológicas en 10 sectores considerados prioritarios y de alto valor agregado» (Balderrama, 2018, párr. 6).

3. Ley de Ciberseguridad de la República Popular China (中华人民共和国网络安全法) del 1º de junio de 2017, que tiene como propósito «garantizar la ciberseguridad; salvaguardar la soberanía del ciberespacio y la seguridad nacional, y los intereses sociales y públicos; proteger los derechos e intereses legítimos de ciudadanos, personas jurídicas y otras organizaciones; y promover el sano desarrollo de la informatización de la economía y la sociedad (Artículo 1), la cual es "aplicable a la construcción, operación, mantenimiento y uso de redes, así como a la supervisión y gestión de la ciberseguridad dentro del territorio continental de la República Popular China» (Artículo 2) (Markovski y Trepykhalin, 2022; y Creemers, et al., 2018).

Esta Ley también establece que el Estado debe tomar medidas «para monitorear, prevenir y manejar los riesgos y amenazas a la ciberseguridad que surjan tanto dentro como fuera del territorio (de China)», así como para proteger la infraestructura de información crítica contra ataques, intrusiones, interferencias y destrucción... sancionar las actividades cibernéticas ilícitas y delictivas... preservando la seguridad y el orden del ciberespacio (Artículo 5), al tiempo que propugna «una conducta en línea sincera, honesta, sana y civilizada... (y) adopta medidas para aumentar la conciencia y el nivel de ciberseguridad de toda la sociedad y formular un buen entorno para que toda la sociedad participe conjuntamente en el avance de la ciberseguridad» (Artículo 6).

En adición, esta Ley señala como deber del Estado establecer «un sistema de monitoreo, de alerta temprana y comunicación de información en materia de ciberseguridad», donde diferentes instancias estatales de ciberseguridad e informatización deberán trabajar coordinadamente «para fortalecer los esfuerzos de recopilación, análisis y presentación de informes de información de ciberseguridad» (Artículo 51). Además, deberán evaluar sistemáticamente los riesgos de ciberseguridad y «formular planes de respuesta de emergencia a incidentes de ciberseguridad y organizar simulacros periódicamente» (Artículo 53).

Finalmente, en el Capítulo VI: Responsabilidad Legal, en su articulado establece severas sanciones que van desde «una suspensión temporal de operaciones, una suspensión de negocios por correcciones, el cierre de sitios web, la cancelación de los permisos de operación pertinentes o la cancelación de licencias comerciales».

4. Visualizando el futuro y ante el rápido progreso y creciente uso de la IA en China el Consejo de Estado de la República Popular China presentó el 8 de julio de 2017 el *Plan de desarrollo de inteligencia artificial de próxima generación* (Documento del Consejo de Estado No 35), en el que se establecen las normas éticas para el uso de la IA en este país. Esta normativa abarca temas relacionados con «el uso y la protección de la información personal, el control humano y la responsabilidad de la IA y la evitación de monopolios relacionados con la IA» (*Center for Security and Emerging Technology*, 2023, párr.1), aunque sin explicar cómo se harán cumplir las normas ni establecer sanciones para quienes las incumplan.

En el Artículo 1 del Plan, Sección I, Provisiones Generales, se estableció su objetivo: «incorporar la ética en todo el ciclo de vida de la IA y promover la equidad, la justicia, la armonía y la seguridad evitando al mismo tiempo problemas como prejuicios, discriminación y (violación de) privacidad y fugas de información». Luego, en el Artículo 2 se señala que «Estas normas se aplican a las personas naturales, personas jurídicas y demás instituciones dedicadas a la gestión, I+D, suministro, uso y otras actividades relevantes de la IA».

En el Artículo 5 establece la necesidad de «Promover la Gobernanza Ágil; Respetar plenamente las leyes del desarrollo de la IA; Comprender el potencial y las limitaciones de la IA y optimizar continuamente la gobernanza, mecanismos y enfoques», así como«Promover lo saludable y sostenible en el desarrollo ordenado de la IA».

El Artículo 10 demanda «Fortalecer el autocontrol en Actividades relacionadas con la I+D de IA, incorporar activamente la ética de la IA en cada eslabón del proceso tecnológico de I+D, y realizar conscientemente autoexámenes, fortalecer la autogestión y no participar en I+D de IA que sea poco ético o inmoral».

El Artículo 11 señala la necesidad de «Mejorar la calidad de los datos... En la recopilación, almacenamiento, uso, procesamiento, transmisión, provisión, divulgación y otras etapas similares, para que cumplan estrictamente con las leyes, estándares y normas relacionadas con los datos... puntualidad, coherencia, cumplimiento normativo y precisión». A esto, el Plan agrega en el Artículo 12 la necesidad de mejorar la seguridad y la transparencia... «En el diseño del algoritmo, etapas de implementación y aplicación, mejorar la transparencia, la explicabilidad, comprensibilidad, confiabilidad y controlabilidad; (así como) mejorar la resistencia de los sistemas de IA, adaptabilidad y capacidad para resistir interferencias».

Con un enfoque de mercado en el Artículo 14 el Plan demanda respetar sus reglas y «Cumplir estrictamente con las diversas normas y regulaciones

que rigen la entrada al mercado, la competencia, las transacciones y otras actividades similares» como un medio «propicio para el desarrollo de la IA», a lo que agrega la importancia de «No subvertir el orden y competencia en el mercado a través de datos o monopolios de plataformas (al tiempo que requiere) Prohibir cualquier método de infracción de derechos de propiedad intelectual por parte de otras entidades»

Finalmente, el Plan demanda en el Artículo 18 establece la necesidad de «Promover el uso bien intencionado» de la IA y, evitar su mal uso (Artículo 19), al tiempo que prohíbe las violaciones de derechos y actos maliciosos en el uso de productos y servicios de IA «que no cumplan con leyes y reglamentos, ética, estándares o normas», y «el uso de productos y servicios de IA para participar en actividades ilegales» (Artículo 20).

5. En julio de 2021, la Academia China de Tecnología de la Información y las Comunicaciones (CAICT, por sus siglas en inglés) propuso un Marco de IA Confiable, en el cual describió las metodologías para lograr una gobernanza de la IA desde la perspectiva de la industria que trabaja y desarrolla esta tecnología (Markovski y Trepykhalin, 2022).

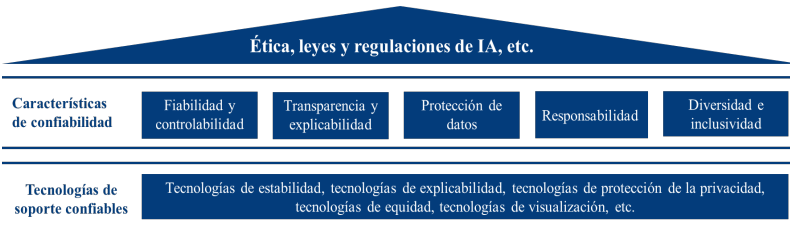
Este documento se enfocó en presentar propuestas para reducir los riesgos que la tecnología de IA, los cuales han creado una crisis de confianza por la falta de seguridad de los algoritmos que se utilizan en sus aplicaciones, donde: (i) el modelo de caja negra termina generando opacidad algorítmica, (ii) la discriminación en el uso e información sobre los datos conduce la toma de decisiones inteligentes sesgadas, (iii) por la complejidad los sistemas de toma de decisiones se dificulta la identificación de las empresas y personas responsables de acciones indebidas o de malos resultados, y (iv) el uso indebido, abuso y fuga de datos riesgos crean riesgos de violación de la privacidad de los usuarios.

Ante estos señalamientos, las autoridades chinas buscaron presentar una propuesta que permitiera hacer sistemáticamente una evaluación de impacto confiable en concordancia con lo planteado por la comunidad internacional hasta ese momento. En este sentido, se buscó poner en marcha un conjunto de normas que aseguraran una gobernanza ética con el objetivo de lograr un equilibrio entre el desarrollo innovador y una buena gobernanza del riesgo. Por tanto, las autoridades pusieron énfasis en que una IA confiable tenía que guiarse por enfoques sistemáticos con métodos de evaluación cada vez más fuertes.

En la formulación del Marco de IA Confiable el CAICT advirtió con claridad que ya no es posible definir normativas solo observando el estado de la tecnología, los productos y los servicios relacionados, sino que su concepción tenía que

ampliarse para incluir una metodología que sistemáticamente incluyera en la creación de «confiabilidad» todos los aspectos tecnológicos como son fiabilidad y controlabilidad, transparencia y explicabilidad, protección de datos, responsabilidad, diversidad e inclusividad, entre otros (Cuadro 2).

Cuadro 2. Marco general de una IA confiable



Fuente: Academia China de Tecnología de la Información y lasComunicaciones (CAICT, por sus siglas en inglés), p.8.

En la medida que las autoridades de China buscan regular todos los aspectos relacionados con las actividades tecnológicas, todo indica que ellas desean tener un fuerte control sobe estas actividades en el país, incluyendo lo relacionado con vídeo juegos, criptomonedas e IA, mediante el establecimiento de normativas éticas que apliquen a todo usuario o desarrollador de estas tecnologías. La normativa sobre ética se redactó en 2019 y tras numerosas consultas se presentó en septiembre de 2021, la que tiene como objetivo estratégico convertir a China en líder mundial en IA, de modo que hacia el 2025 sea el mayor referente de esta tecnología (Expansión.mx, 2021)

6. El 25 de septiembre de 2021, el Comité Nacional de Especialistas en Gobernanza de la Inteligencia Artificial de Nueva Generación de China publicó las Normas Éticas para la Inteligencia Artificial de Nueva Generación (Ethical Norms for New Generation Artificial Intelligence Released), la que tiene como objetivo «incorporar la "ética" en todo el ciclo de vida de la IA y promover la equidad, la justicia, la armonía y la seguridad, evitando al mismo tiempo problemas como el sesgo, la discriminación y la privacidad y las fugas de información» (Artículo 1) (*Center for Security and Emerging Technology*, 2021). Esta Ley entró en vigor el 1 de noviembre de 2021.

Lo fundamental de estas normas es que ellas aplican a toda persona natural, jurídica e instituciones en todas las actividades relevantes relacionada con la IA. Así es como, en lo referente a *actividades de gestión* se orienta a la planificación estratégica a «la formulación e implementación de políticas, regulaciones y estándares técnicos, la asignación de recursos y la supervisión y examen». Con relación a las actividades de I+D se refiere «a la investigación científica, el desarrollo tecnológico y ... de productos relacionados con la IA». En cuanto a las *actividades de suministro*, se enfoca en «la producción, operaciones y

ventas» de productos y servicios de IA. Y, sobre las actividades de uso norma «la compra, el consumo y las operaciones... con productos y servicios de IA» (Artículo 2).

Luego, en el Artículo 3 señala que todas las actividades de IA deberán cumplir fundamentalmente seis normas *éticas básicas*, que son:

> (I) «Promoción del Bienestar Humano».
>
> (II) «Promoción de la Equidad y la Justicia», para «defender la inclusión y la tolerancia, proteger... los derechos e intereses legítimos de cada entidad relevante, promover la distribución justa de los beneficios de la IA» para toda la sociedad y «promover la equidad social, la justicia y la igualdad de oportunidades».
>
> (III) «Protección de la Privacidad y la Seguridad» para garantizar «el derecho de todos a conocer el alcance de su uso y a dar consentimiento para la utilización de su información personal», donde los datos personales deben tratarse de acuerdo con «los principios de legalidad, decoro, necesidad y buena fe, para garantizar la privacidad personal y la seguridad» de ellos.
>
> (IV) «Garantía de Controlabilidad y Confiabilidad» para garantizar que se mantienen los derechos de las personas naturales para la toma de decisiones autónomas, como aceptar o rechazar los servicios mediante IA, retirarse en el momento que el usuario lo decida y finalizarlos en cualquier momento.
>
> (V) «Fortalecimiento de la Rendición de Cuentas», para asegurar el respeto de las personas, para lo cual es necesario definir las responsabilidades de los usuarios y los ofertantes, crear conciencia sobre la responsabilidad, así como practicar «la autorreflexión y la autodisciplina en cada eslabón del ciclo de vida de la IA», al tiempo que se establecen mecanismos de rendición de cuentas, para que nadie eluda sus propias responsabilidades.
>
> (VI) «Fomentar la Cultura de la Ética» para que esta forma del comportamiento humano se «aprenda y popularice activamente» en la sociedad.

El Artículo 5 se orienta a «Promover una Gobernanza Ágil» mediante respeto de las leyes del desarrollo de la IA, el conocimiento del potencial y las limitaciones de la IA y creando mecanismos y enfoques que garanticen una buena gobernanza. El Artículo 10 busca «Fortalecer la conciencia de

autodisciplina» en todas las actividades relacionadas con la I+D de IA, para lo cual señala la «necesidad de incorporar la ética en el desarrollo de tecnología I+D, así como» realizar autoexámenes, fortalecer la autogestión y no participar en trabajos de I+D de IA poco éticos o inmorales.

Un aspecto interesante lo presenta el Artículo 14, «Respetar las reglas del mercado», que señala la necesidad de «cumplir estrictamente con las distintas normas y regulaciones que rigen la entrada al mercado, la competencia, las transacciones y otras actividades similares», con lo que se abre paso a las oportunidades que brinda el mercado, especialmente para los inversionistas. Coincidentemente, tomando en cuenta la forma cómo funciona el mercado y las características de la demanda de bienes y servicio, en el Artículo 15 mandata «Fortalecer el Control de Calidad» respecto al uso de los bienes y servicios de IA, así como «evitar daños a la salud, la propiedad y la privacidad de los usuarios causados por problemas como el diseño y los defectos del producto».

Finalmente, el Artículo 18 señala la necesidad de «Promover el uso bien intencionado» de la IA, para lo cual es necesario realizar «evaluaciones previas al uso de productos y servicios de IA», conocer «los beneficios de los bienes y servicios de IA» y considerar los derechos e intereses legales de cada parte interesada... (para) promover más eficazmente la prosperidad económica, el progreso social y el desarrollo sostenible.

7. *Orientación sobre el fortalecimiento de la gobernanza integral de los algoritmos de los servicios de información de Internet* (关于加强互联网信息服务算法综合治理的指导意见), responde al continuo proceso de normar los avances tecnológicos, que fue presentada por la CAC, en conjunto con el Departamento de Publicidad del Comité Central del PCCh, los ministerios de Educación, Cultura, Ciencia, Industria y de Seguridad Pública el 29 de septiembre de 2021. Luego, el 11 de abril de 2023 se publicó el borrador Medidas de Gestión del Servicio de Inteligencia Artificial Generativa, para recibir comentarios y promover el desarrollo sano y robusto de las aplicaciones que utilizan IA generativa. Estas Medidas, que entraron en vigor el 10 de enero de 2023, tienen como «finalidad de establecer un modelo de gobernanza integral de la seguridad algorítmica en alrededor de tres años» (Yanling, 2021, párr.1).

Esta Orientación se presentó como una guía para poder «administrar, utilizar y desarrollar buenas aplicaciones algorítmicas y mejorar integralmente las capacidades integrales de gestión de la red», para fortalecer la gobernanza de la seguridad de algoritmos de servicios de información de Internet, con el fin de «construir y mejorar sistemas de supervisión de seguridad de algoritmos y promover algoritmos... (mediante) el desarrollo saludable, ordenado y próspero de algoritmos» (Introducción del Documento). También, en la parte «Principios básicos» demanda, entre otros, «Adherirse a la orientación

correcta, fortalecer la conciencia sobre la ética científica y tecnológica, la conciencia sobre la seguridad y el pensamiento de resultados, aprovechar plenamente el papel de los servicios algorítmicos en la difusión de energía positiva y crear un ciberespacio limpio y recto», así como «guiar la aplicación de algoritmos para que sea justa, transparente y explicable, y proteger plenamente los derechos e intereses legítimos de los internautas», sin dejar de lado la necesidad de «promover vigorosamente el trabajo de investigación de innovación de algoritmos... proteger los derechos de propiedad intelectual de los algoritmos, fortalecer el despliegue y la promoción de algoritmos de desarrollo propio y mejorar la competitividad central de los algoritmos de China».

En el apartado «Objetivos principales» reconoce que tomarán alrededor de tres años «establecer gradualmente una estructura de gobernanza integral para la seguridad de los algoritmos con un mecanismo de gobernanza sólido, un sistema de supervisión completo y una ecología de algoritmos estandarizada».

Luego, en el numeral 2 de esta Orientación demanda «Mejorar el mecanismo de gobernanza de la seguridad de los algoritmos» estableciendo procesos para: 1) Fortalecer los estándares de gobernanza de algoritmos; 2) Optimizar la estructura de gobierno del algoritmo; 3) Fortalecer la coordinación y la gobernanza generales; 4) Fortalecer la responsabilidad principal de las empresas; 5) Fortalecer la autodisciplina de las organizaciones industriales; y 6) Alentar a los internautas a supervisar y participar. Finalmente, demanda Establecer un sistema de supervisión de seguridad algorítmica y Promover el desarrollo de estándares ecológicos de algoritmos (Yanling, 2021).

Con esta orientación, las autoridades chinas, reconocen que los algoritmos han tenido una función determinante «en la difusión de información, la prosperidad de la economía digital y la promoción del desarrollo social» (Forbes, 2021, párr.1), pero, también advierten que la «aplicación irracional de algoritmos también afecta al orden normal de la comunicación y a los derechos e intereses legítimos de los cibernautas» (párr.3). Ante esta situación, plantean la necesidad de regular los algoritmos de las tecnológicas mediante un sistema de supervisión sólido para la aplicación «justa, abierta y transparente».

En cuanto al desarrollo ecológico de algoritmos, la normativa orientadora promueve la apertura y transparencia de los algoritmos como una forma que permita potenciar el desarrollo innovador de algoritmos, reducir el riesgo de abuso, mantener las condiciones de mercado y establecer un orden social en el ciberespacio. Todo esto acompañado por recomendaciones para fortalecer la gobernanza integral de los algoritmos de los servicios de información de Internet asegurando el uso responsable de estas herramientas tecnológicas (Yanling, 2021).

8. *La nueva Ley de Seguridad de Datos, también conocida como Ley de Protección de Datos Personales* [中华人民共和国个人信息保护法] la aprobó el Congreso de la República Popular de China el 20 de agosto de 2021 (en vigor el 1º de noviembre de 2021), la cual tiene como objetivo establecer un conjunto de normas relacionadas con la recopilación y procesamiento de información personal y promover el uso razonable para proteger los derechos de los internautas, estandarizar su tratamiento, así como salvaguardar el flujo legal y libre de la información (Gobierno de la República Popular China, 2021), todo lo cual tiene alta coincidencia con lo que dicta el Reglamento General de Protección de Datos de la UE.

Esta ley señala que «La información personal... está protegida por la ley y ninguna organización o individuo puede infringir los derechos e intereses... (en el uso de esta) información» (artículo 2). Este mandato aplica tanto a la utilización de información personal dentro como fuera del territorio de China (artículo 3).

El concepto de *información personal* lo define como toda «información relacionada con personas físicas identificadas o identificables registradas electrónicamente o por otros medios, excluida la información anónima», mientras que define el procesamiento de información como «la recopilación, almacenamiento, uso, procesamiento, transmisión, suministro, divulgación, eliminación... de información personal» (Artículo 4), todo lo cual se debe realizar «de acuerdo con los principios de legalidad, legitimidad, necesidad y buena fe», la cual tampoco «se procesará mediante engaño, fraude, coerción u otros medios» (Artículo 5). Luego señala que «El procesamiento de información personal seguirá los principios de apertura y transparencia, divulgará las reglas para el procesamiento de información personal y establecerá claramente el propósito, método y alcance del procesamiento» (Artículo 7).

Esta norma jurídica sentencia que ninguna organización o individuo «pueden comprar, vender, proporcionar o divulgar ilegalmente información personal de otras personas (ni) participar en actividades de procesamiento de información personal que pongan en peligro la seguridad nacional, seguridad o intereses públicos» (Artículo 10).

A los procesadores de información personal que utilicen este tipo de data «para tomar decisiones automatizadas» se les exige que garanticen «la transparencia de la toma de decisiones y la justicia e imparcialidad de los resultados... (sin) imponer un trato diferencial irrazonable a las personas en términos de precios de transacción y otras transacciones... (y que)... al enviar información y marketing comercial... deben proporcionar opciones que no estén dirigidas a sus características personales» (Artículo 24). Además, los

procesadores no podrán «divulgar la información personal que procesan, excepto con el consentimiento por separado del individuo» (Artículo 25).

Esta norma también define el concepto de información personal sensible como aquella «que, una vez filtrada o utilizada ilegalmente, puede fácilmente causar que se viole la dignidad de una persona... o que se ponga en peligro la seguridad personal y de la propiedad, incluidos los datos biométricos, religiosos, creencias, identidad específica, salud médica, cuentas financieras, paradero y otra información, así como la información personal de menores de catorce años». Por tanto, los procesadores de información personal sensible la pueden procesar «solo cuando existe un propósito específico... y se toman estrictas medidas de protección» (Artículo 28) y siempre cuando hayan logrado el consentimiento del dueño de la información (Artículo 29). Además, en el caso del tratamiento de datos personales de menores de 14 años, «deberán obtener el consentimiento de los padres u otros tutores del menor» (Artículo 31).

Los procesadores de información personal que por razones comerciales necesiten proporcionar información fuera del territorio de China, deberá solicitar autorización y obtener «una certificación... de acuerdo con las regulaciones del departamento nacional del ciberespacio, tener un contrato con el destinatario en el extranjero... y estipular los derechos y obligaciones de ambas partes» (Artículo 38). En el caso de información personal almacenada en el territorio de China los procesadores no pueden darla «sin la aprobación de las autoridades competentes" chinas; y cuando sea solicitada por "organismos judiciales o de aplicación de la ley extranjeros" se podrá proveer "de conformidad con el principio de igualdad y reciprocidad» (Artículo 41).

Es de desatacar que si una persona encuentra que su información personal «es inexacta o está incompleta, tiene derecho a solicitar al procesador... que (la) corrija o complemente» (Artículo 46) En caso de que se trate de una persona natural que ha fallecido, sus familiares, por derecho, pueden solicitar «copia, rectificación, supresión... (de) los datos personales relevantes... para sus propios intereses legales y legítimos, a menos que el causante haya otros arreglos antes de su muerte» (Artículo 49).

En términos de sanciones, se establece que quien maneje datos personales y viole las disposiciones de esta Ley «será ordenado a corregir, amonestado y confiscado por el departamento que desempeña responsabilidades de protección de información personal... (y) serán ordenadas a suspender o cancelar los servicios», al tiempo que también se establecen multas pecuniarias al personal directamente responsable (Artículo 66).

9. La *Ley de Protección de Información Personal* (PIPL, por sus siglas en inglés; 中华人民共和国个人信息保护法) de la República Popular China fue aprobada en

la 30ª Reunión del Comité Permanente del 13er Congreso Nacional del Pueblo el 20 de agosto de 2021 (Creemers y Webster, 2021) y en vigor desde el 1º de noviembre, la cual tiene como objeto «proteger los derechos e intereses de la información personal, estandarizar las actividades de manejo de la información personal y promover el uso racional de la información personal» (Artículo 1), por considerar que "ninguna organización o individuo puede infringir los derechos e intereses de información personal de las personas físicas (Artículo 2).

Esta Ley aplica al manejo de información personal de personas físicas en China «registrada por medios electrónicos o de otro tipo... sin incluir la información posterior al tratamiento de anonimización» (Artículo 4). Además, señala que «el tratamiento de los datos personales se observarán los principios de licitud, corrección, necesidad y sinceridad» por lo que prohíbe «manejar información personal de manera engañosa, fraudulenta, coercitiva o de otro tipo» (Artículo 5). También, considera que en el «tratamiento de datos personales se observarán los principios de apertura y transparencia, divulgándose las reglas para el tratamiento de datos personales e indicando claramente el propósito, método y alcance del tratamiento» (artículo 7).

En adición, señala que «Ninguna organización o individuo puede recopilar, usar, procesar o transmitir ilegalmente información personal de otras personas, ni vender, comprar, proporcionar o divulgar ilegalmente información personal de otras personas, ni participar en actividades de manejo de información personal que perjudiquen la seguridad nacional o el interés público» (artículo 10). Y agrega que «Los encargados de la información personal no podrán revelar la información personal que manejan; excepto cuando obtengan un consentimiento por separado» (artículo 25), sin dejar de considerar que «Las personas tienen derecho a conocer y decidir sobre sus datos personales, y tienen derecho a limitar o negar el tratamiento de sus datos personales por parte de otros, salvo que las leyes o reglamentos administrativos estipulen lo contrario» (artículo 44).

10. Las *Disposiciones de gestión de recomendaciones algorítmicas del servicio de información de Internet* (互联网信息服务算法推荐管理规定), en vigor el 10 de marzo de 2022 –modificó la normativa de septiembre de 2021– fueron presentadas por la Oficina de la Comisión Central de Asuntos del Ciberespacio (CAC, siglas de Office of the Central Cyberspace Affairs Commission), en el cual se presentaron algunos cambios al documento de septiembre de 2021. Estas Disposiciones tienen como objeto:

> «... estandarizar las actividades de recomendación algorítmica de los servicios de información de Internet, promover la visión de valores fundamentales socialistas, salvaguardar la seguridad nacional y el

interés social y público, proteger los derechos e intereses legítimos de los ciudadanos, personas jurídicas y otras organizaciones, y estimular el sano desarrollo de los servicios de información en Internet» (artículo 1).

Estas Disposiciones se concibieron sobre la base de la *Ley de Ciberseguridad de la República Popular China*, la *Ley de Seguridad de Datos de la República Popular China*, la *Ley de Protección de Información Personal de la República Popular China*, la *Ley de Gestión de Servicios de Información de Internet Normas*, y otras leyes y reglamentos administrativos similares (Webster, 2022).

En las Disposiciones se establece que «la prestación de servicios de recomendación algorítmica deberá respetar... la moral y la ética social, la ética comercial y la ética profesional y respetar los principios de equidad y justicia, apertura y transparencia... sinceridad e integridad» (artículo 4). Consecuentemente, alienta «a fortalecer la autodisciplina sectorial, establecer y completar estándares... normas sectoriales y ... supervisar y orientar a los proveedores de servicios de recomendación algorítmica» (artículo 5), así como evitar el ingreso de «información ilegal o dañina como palabras clave en los intereses de los usuarios ni convertirlas en etiquetas de usuario para utilizarlas como base para recomendar contenido informativo» (artículo 10).

En adición, se estableció que los proveedores de servicios de recomendación algorítmica que provean noticias en Internet, «deberán obtener un permiso de servicio (licencia)... y estandarizar ... (los) servicios de recopilación, edición y difusión de información». También, se les prohibió «generar ni sintetizar información noticiosa falsa» (artículo 13). Sobre la base del concepto de mercado, en las Disposiciones se les ordena a los proveedores de servicios de recomendación algorítmica no «imponer restricciones irrazonables a otros proveedores... ni obstruir o destruir el funcionamiento regular de sus servicios de información de Internet prestados lícitamente, ni realizar actos monopólicos o de competencia indebida» (artículo 15).

Como defensa y protección de los derechos de los menores de edad las Disposiciones establecen que los proveedores de servicios de recomendación algorítmica deberán «cumplir con los deberes de protección en línea de los menores de edad... y facilitar que los menores obtengan información beneficiosa para su salud física y mental, mediante el desarrollo de modelos adecuados para uso con menores, prestación de servicios adaptados a las características específicas de los menores» (artículo 18). En el caso de personas mayores, los proveedores de este tipo de servicios deberán «defender los derechos de los que disfrutan las personas mayores... considerar plenamente (sus) necesidades... a la hora de salir, someterse a tratamientos médicos, consumir, manejar asuntos, y proporcionar servicios inteligentes... adaptados a las personas mayores...

(prevenir fraudes) y facilitar que las personas mayores utilicen de forma segura los servicios de recomendación algorítmica» (artículo 19).

11. El borrador Medidas de Gestión del Servicio de Inteligencia Artificial Generativa (生成式人工智能服务管理办法(征求意见稿) fue publicado el 11 de abril de 2023 por la Administración del Ciberespacio de China (CAC, por sus siglas en inglés) para recibir comentarios y promover el desarrollo sano y robusto de las aplicaciones que utilizan IA generativa, en concordancia con la Ley de Ciberseguridad de la República Popular China y otras normas y regulaciones. Las Medidas aprobadas de Gestión del Servicio de Inteligencia Artificial Generativa entraron en vigor el 15 de agosto de 2023, tienen como objeto «promover el desarrollo saludable y la aplicación estandarizada de la inteligencia artificial generativa» las que se complementan con la Ley de Ciberseguridad, la Ley de Protección de Datos Personales, también conocida como Ley de Seguridad de Datos, la Ley de Protección de Información Personal y demás leyes y reglamentos administrativos de la República Popular China (artículo 1).

Estas Medidas deben ser cumplidas por «quienes desarrollen y utilicen productos de inteligencia artificial generativa para brindar servicios al público dentro del territorio de... China». Luego señala que «El término 'inteligencia artificial generativa' ... se refiere a la tecnología que genera texto, imágenes, sonidos, videos, códigos y otros contenidos basados en algoritmos, modelos y reglas» (artículo 2). Sin embargo, también sostiene que «El Estado apoya la innovación, promoción y aplicación independientes y la cooperación internacional de tecnologías básicas como algoritmos y marcos de inteligencia artificial, y fomenta el uso prioritario de software, herramientas, recursos informáticos y de datos seguros y confiables» (artículo 3), aunque en la prestación de estos bienes o servicios se deberá cumplir con los requisitos de las diferentes normativas y «respetar la moral social, el orden público y las buenas costumbres», así como con los siguientes requisitos (Artículo 4):

1. «El contenido generado utilizando inteligencia artificial generativa debe reflejar los valores fundamentales del socialismo y no debe contener contenido que subvierta el poder estatal, derroque el sistema socialista, incite a la secesión, socave la unidad nacional, promueva el terrorismo y el extremismo, o promueva el odio nacional y discriminación, información violenta, obscena y pornográfica, información falsa y contenido que pueda alterar el orden económico y social».
2. «En el proceso de diseño de algoritmos, selección de datos de entrenamiento, generación y optimización de modelos y prestación de servicios, se deben tomar medidas para prevenir la discriminación

por motivos de raza, etnia, credo, nacionalidad, región, género, edad, ocupación, etc.».
3. «Respetar los derechos de propiedad intelectual y la ética empresarial, y no utilizar ventajas como algoritmos, datos y plataformas para participar en competencia desleal».
4. «El contenido generado mediante inteligencia artificial generativa debe ser verdadero y exacto, y ... evitar la generación de información falsa».
5. «Respetar los intereses legítimos de los demás, evitar daños a la salud física y mental de los demás, daños a los derechos de retrato, derechos de reputación y privacidad personal, e infringir los derechos de propiedad intelectual. Se prohíbe la adquisición, divulgación y uso ilegal de información personal, privacidad y secretos comerciales».

Las organizaciones e *individuos proveedores* «asumen la responsabilidad del productor del contenido» que contenga el producto y «asumen la responsabilidad legal» si no cumple con «las obligaciones de protección de información personal» (artículo 5).

Artículo 6. Antes de utilizar productos de inteligencia artificial generativa para brindar servicios al público, se deberá presentar una evaluación de seguridad al departamento nacional de ciberseguridad e informatización de acuerdo con el «Reglamento sobre evaluación de seguridad de los servicios de información de Internet con atributos de opinión pública o capacidad de movilización social». y las «Recomendaciones de Algoritmos de Servicios de Información de Internet» y el «Reglamento de Gestión» para realizar los procedimientos de presentación de algoritmos y de cambio y cancelación.

Artículo 7. Los proveedores serán responsables de la legalidad de las fuentes de datos previos a la formación y de datos de formación optimizados para productos de inteligencia artificial generativa.

Los datos de entrenamiento previo y optimizado para productos de inteligencia artificial generativa deben cumplir los siguientes requisitos:

1. Cumplir con los requisitos de leyes y regulaciones como la Ley de Ciberseguridad de la República Popular China;
2. No contiene contenido que infrinja los derechos de propiedad intelectual;
3. Si los datos contienen información personal, se deberá obtener el consentimiento del titular de la información personal u otras circunstancias consistentes con las leyes y reglamentos administrativos
4. Capaz de garantizar la autenticidad, exactitud, objetividad y diversidad de los datos;

5. Otros requisitos reglamentarios del departamento nacional de ciberseguridad e informatización en materia de servicios de inteligencia artificial generativa.

El proveedor también «deberá formular reglas de etiquetado claras, específicas y operables que cumplan con los requisitos de estas Medidas, realizar la capacitación necesaria para el personal de etiquetado y verificar la exactitud del etiquetar el contenido a modo de muestra» (artículo 8). Tampoco podrá generar «contenidos discriminatorios por razón de raza, nacionalidad, género, etc. del usuario» (artículo 12); aunque sí deberán crear «un mecanismo para recibir y manejar las quejas de los usuarios, atender con prontitud las solicitudes individuales de corrección, eliminación y bloqueo de su información personal... y evitar que el daño continúe» (artículo 13).

En adición, cada proveedor deberá estar en condiciones de guiar a los usuarios para «que comprendan científicamente y utilicen racionalmente el contenido generado por la inteligencia artificial generativa... (cuidando de no) dañar la imagen, la reputación y otros derechos e intereses legítimos de otros». Además, señala que los proveedores «no participarán en exageraciones comerciales o marketing desleal»; y si no cumplen el usuario pude denunciarlo ante «la autoridad competente» (artículo 18). El otro lado de la moneda de este concepto normativo establece si es el *proveedor* el que «descubre que el usuario viola las leyes y regulaciones, la ética empresarial y la moral social en el proceso de uso de productos de inteligencia artificial generativa, incluida la participación en publicidad en internet, publicaciones y comentarios maliciosos, creación de spam, escritura de malware (programa maligno) y cometimiento desleal de marketing comercial, etc., los servicios se le deben suspender o cancelar» (artículo 19).

Como se ha visto, China ha estado poniendo atención y normando el uso de nuevas tecnologías y su entorno desde 2005 incluyendo su visión estratégica de largo plazo, Sundar Pichai, director ejecutivo de Google considera que por «la escala de trabajo que está llevando a cabo China en el ámbito de la IA [...] va a estar a la vanguardia de esta disciplina. Es un hecho» (López, 2023, párr. 5), y va a ser imbatible en IA.

Anexo VII. Legislación de IA en América Latina

En la Cumbre de *Bletchley Park*, Reino Unido (2023) 29 países, incluyendo la Unión Europea, acordaron establecer normas para el desarrollo seguro de la IA y que ésta se utilice para el bien de todos a nivel mundial (ver Parte III. Legislaciones en vigencia y en procesos de aprobación, literal n. Acuerdo para regular la Inteligencia Artificial en diversos países del mundo).

Este Acuerdo difundido mundialmente, alertó a todos los países sobre la necesidad de regular la IA, por lo que se estima que en el año 2024 haya una atendencia generalizada de tomar medidas normativas respecto a la IA, la cual, se estima que debe tener alta prioridad en los países que tienen un alto grado de desigualdad, para reducir los adversos resultados que pueden resultar por falta de regulación. En estas condiciones, las normativas a ser diseñadas y puestas en marcha deberían concentrarse en: 1) dar mayor seguridad y calidad a la que se utiliza en el sector público y 2) establecer condiciones en el ámbito privado para generar confianza, dar transparencia, establecer principios y códigos de ética y evitar el uso indebido de la IA para evitar daños a la sociedad, en general.

Índice de Desarrollo del Gobierno Electrónico 2022

Así es como, con una visión propia del sector público, en el Reporte de Gobierno Electrónico 2022 de las Naciones Unidas (UN E-Government Survey in 2022) se presenta el panorama del gobierno digital en los 193 países miembros, que los clasifica y genera el Índice de Desarrollo del Gobierno Electrónico (EGDI por su nombre en inglés E-Government Development Index), en lo referente al uso e incidencia de las tecnologías de la información en este sector. El Índice refleja el promedio ponderado de tres subíndices: 1) Servicios en línea, 2) Infraestructura de telecomunicaciones y 3) Capital humano. Los 10 países del mundo con la puntuación más alta son: Dinamarca (0.9717), Finlandia (0.9533), República de Corea (0.9529), Nueva Zelanda (0.9432), Islandia (0.9410), Sue cia (0.9410), Australia (0.9405), Estonia (0.9393), Países Bajos (0.9384), Estados Unidos (0.9151).

En el caso de América Latina, el Índice de Desarrollo del Gobierno Electrónico 2022 califica en un rango muy alto a seis países. A Uruguay lo mantiene en el primer puesto por octavo año consecutivo y ocupa el lugar 35 en el mundo con 0.8388 puntos. Chile está en el segundo lugar y la posición 36 en el mundo con 0.8377 puntos; tercero Argentina con 0.8198 puntos y en el puesto 41 en el mundo; cuarto Brasil con 0.7910 puntos y en el lugar 49 en el mundo; Costa Rica en el puesto 5 –primer lugar en Centroamérica ampliada– y la ubica en el número 56 en el mundo; y Perú en el sexto lugar en Latinoamérica y en el puesto 59 en el mundo (Cuadro 3). A El Salvador el Índice lo ubica en la posición número 14 entre 19 países de América Latina y en el 117º en el mundo.

Por su parte, los tres países de América Latina con las calificaciones más baja son: Nicaragua en el puesto 17 con 0.5032 puntos y en la posición 130 en el mundo, Cuba situada en el puesto 18 con 0.4945 y en lugar 136 en el mundo, para cerrar con Honduras que con 0.394 puntos se ubica en la posición 19, mientras que a nivel mundial el Índice la coloca en el puesto 155 entre 193 países evaluados en el mundo.

De manera prácticamente paralela, la OCDE, en conjunto con la CAF – Banco de Desarrollo de América Latina–, preparó el informe «Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe», el que presentó en septiembre de 2022. Este informe, señaló que algunos gobiernos de América Latina y el Caribe (ALC) ya estaban trabajando para utilizar la IA de una manera estratégica y confiable. En este sentido, destacó que siete países del ALC ya habían concluido o estaban en proceso de desarrollo de estrategias nacionales de IA: Argentina, Brasil, Chile, Colombia, México, Perú y Uruguay.

Cuadro 3. Índice de Desarrollo del Gobierno Electrónico

País	Puntos	Posición: En América Latina	Posición: En el mundo
Uruguay	0.8388	1	35
Chile	0.8377	2	36
Argentina	0.8198	3	41
Brasil	0.7910	4	49
Costa Rica	0.7659	5	56
Perú	0.7524	6	59
México	0.7473	7	62
Colombia	0.7261	8	70
Panamá	0.6956	9	82
Ecuador	0.6889	10	84
Rep. Dominicana	0.6429	11	92
Paraguay	0.6332	12	94
Bolivia	0.6165	13	98
El Salvador	0.5519	14	117
Guatemala	0.5111	15	126
Venezuela	0.5053	16	128
Nicaragua	0.5032	17	130
Cuba	0.4945	18	136
Honduras	0.394	19	155

Fuente: CEPAL, https://biblioguias.cepal.org/ld.php?-con-tenr id=68864903

Los gobiernos de estos países se fijaron como objetivo mejorar la eficiencia y la toma de decisiones, para mantener contacto y brindar servicios de mejor calidad a la sociedad, dar mayor seguridad pública, tener mayor transparencia en la rendición de cuentas del sector público y lograr una mejoría en los sistemas educativos. Sin embargo, deja en evidencia que las capacidades entre los sectores públicos de los países de ALC variaba significativamente en el uso estratégico y responsable de la IA (OECD, 2022).

Índice de Ciberseguridad Global 2020

Otra medición, con un enfoque más apropiado para diseñar y aplicar normas en el sector privado es el Índice de Ciberseguridad Global (ICG)

2020, que prepara la Unión Internacional de Telecomunicaciones (UIT) y que presentó el 29 de junio de 2021, el cual da a conocer el nivel de avance de los compromisos relativos a ciberseguridad adoptados por los 193 países miembros de la UIT y del Estado de Palestina. Este Índice se construyó sobre la base de 82 preguntas sobre los compromisos de ciberseguridad de los estados miembros, las que están divididas en cinco pilares: 1) medidas jurídicas, 2) medidas técnicas; 3) medidas institucionales; 4) medidas de capacitación; y 5) medidas de cooperación.

El objetivo de este Índice es «identificar las carencias, servir de hoja de ruta para orientar las estrategias nacionales, fundamentar los marcos jurídicos, ofrecer capacitación, destacar las prácticas idóneas, reforzar las normas internacionales y fomentar una cultura de la ciberseguridad» (UIT, 2021, párr. 14). En la publicación se destaca que cada vez es más grande el compromiso de los países para enfrentar y reducir las amenazas y riesgos en ciberseguridad, de modo que alrededor del 50 % de estados en el mundo ya habían conformado equipos de trabajo para intervenir ante casos informáticos y el 64 % tenía una estrategia nacional de ciberseguridad y 70 % habían realizado campañas de sensibilización en materias de ciberseguridad en 2020, lo que obviamente siguió mejorando de cara al 2024.

El Informe de Ciberseguridad Global 2020 destacó que aún había insuficiencias en cibercapacidad y demandó «abordar la brecha cibernética» en áreas clave como:

- Formación en ciberseguridad, la que debe adaptarse a las necesidades de los particulares y de las micro, pequeñas y medianas empresas (MIPYME).
- Finanzas, sanidad, energía, y otros sectores clave, que requieren medidas específicas para colmar las lagunas en materia de ciberseguridad.
- Protección de la infraestructura esencial, que exige una mejora para hacer frente a las nuevas y evolutivas ciberamenazas.
- Protección de datos personales, que requiere un refuerzo continuo a medida que aumentan las actividades en línea.

Seguidamente agregó que ante el creciente uso y dependencia de las herramientas digitales era necesario tomar medidas de protección más firmes, aunque cuidando que sean accesibles y de fácil uso.

Según el Índice de Ciberseguridad Global 2020, que evaluó a 181 países, Estados Unidos tiene el primer lugar en el mundo con 100 puntos (Cuadro 4). Reino Unido y Arabia Saudita (99.54 puntos ambos) se ubican en el segundo puesto; Estonia con 99.48 puntos en el tercer lugar en el mundo; y en 4° lugar República de Corea, Singapur y España (98.52 puntos cada uno). En el lugar

12, después de 16 países, está Australia con 97.47 puntos. Es de destacar que la diferencia entre estos 17 países, esto es, entre Estados Unidos en el 1er lugar y Australia es de sólo 2.53 puntos, lo que muestra el alto grado de cumplimiento de los compromisos relativos a ciberseguridad de estos países.

En el caso de América Latina la dispersión entre el país que ocupa el primer lugar (96.60 puntos) y el que ocupa el último lugar en la región (2.20 puntos) es extremadamente grande 94.40 puntos, lo que significa que este último país tiene un grado de cumplimiento de 2.28% respecto al primero.

Cuadro 4. Índice de Ciberseguridad Global 2020

País	Puntos	Posición: En el mundo
Estados Unidos	100.00	1
Reino Unido	99.54	2
Arabia Saudita	99.54	2
Estonia	99.48	3
República de Corea	98.52	4
Singapur	98.52	4
España	98.52	4
Federación de Rusia	98.06	5
Emiratos Árabes Unidos	98.06	5
Malasia	98.06	5
Lituania	97.93	6
Japón	97.82	7
Canadá**	97.67	8
Francia	97.60	9
India	97.50	10
Turquía	97.49	11
Australia	97.47	12

Fuente: ITU. https://www.itu.int/dms pub/itud/opb/str/D-STR-GCI.01-2021-PDF-S.pdf
***Sin respuesta al cuestionario.

De acuerdo con el Índice de Ciberseguridad Global 2020, en América Latina (Cuadro 5) Brasil ocupa el primer lugar y el 18° a nivel mundial con 96.60 puntos; segundo está México con 81.68 puntos en el puesto 52 en el mundo; tercero se ubica Uruguay con 75.15 puntos y en el lugar 64 en el mundo. El Salvador, con 13.30 puntos está en el puesto 16 en América Latina y es el número 148 en el mundo. Cierra el Índice Honduras, con 2.20 puntos en el 19° lugar en la región y ubicado en el puesto 178 en el mundo entre 181 países.

Si bien estos indicadores relativos a ciberseguridad son de alta importancia, y deben formularse normativas precisas y con fuerza para proteger a los usuarios, así como el diseño de estrategias nacionales para estimular la inversión en el desarrollo innovador y el uso de IA, para lo cual, hay gran cantidad de antecedentes en las normas y legislaciones en la UE, EUA, Reino Unido y China, entro muchos otros países, así como documentos orientadores de instituciones multilaterales.

Sin embargo, es de recalcar que, en la generación de todo el marco jurídico para regular la IA en un país y establecer sanciones y multas en dinero por incumplimientos, es fundamental tener como marco conceptual: (1) sus propias características socioeconómicas, (2) sus relaciones con los países limítrofes o de la región a que pertenece, para formar redes de información o para homogeneizar las normativas y leyes, y (3) el juego geopolítico internacional. Además, si el país ya tiene una institucionalidad propia para definir, plantear normas y supervisar la creación, desarrollo y uso de la IA, será trascendental mantener un estudio sistemático de lo que sucede en este sector tecnológico, la capacidad y conocimiento de sus técnicos, sus condiciones de trabajo y la asignación de presupuestos para responder a las crecientes necesidades que emergen del vertiginoso desarrollo innovador y el uso de esta tecnología, para evitar situaciones que afecten adversamente al progreso económico o que generen desconfianza e incertidumbre o que dañe a las personas, en particular, o a la sociedad, en general.

Cuadro 5. Índice de Ciberseguridad Global 2020: América Latina

País	Puntos	Posición: En América Latina	Posición: En el mundo
Brasil	96.60	1	18
México	81.68	2	52
Uruguay	75.15	3	64
Rep. Dominicana	75.05	4	66
Chile	68.83	5	74
Costa Rica	67.45	6	76
Colombia	63.72	7	81
Cuba	58.76	8	82
Paraguay	57.09	9	84
Perú	55.67	10	86
Argentina	50.12	11	91
Panama	34.11	12	103
Venezuela	27.06	13	116
Ecuador	26.30	14	119
Bolivia	16.14	15	140
El Salvador	13.30	16	148
Guatemala	13.13	17	150
Nicaragua	9.00	18	165
Honduras	2.20	19	178

Fuente: ITU, https://www.itu.int/dms pub/itu-d/opb/str/DSTR-GGI.01-2021-PDF-S.pdf

Índice Latinoamericano de Inteligencia Artificial 2023

El Centro Nacional de IA de Chile, en conjunto con el Banco Interamericano de Desarrollo (BID), la Corporación Andina de Fomento (CAF), la Organización de Estados Americanos (OEA), con la asistencia técnica de la Organización de las Naciones Unidas para la Educación, la Ciencia y la

Cultura (UNESCO), y con el apoyo del Amazon Web Service (AWS), Google, Hub APTA y el HAI de la Universidad de Stanford y publicaron 11 de agosto de 2023 el *Índice Latinoamericano de Inteligencia Artificial 2023* (ILIA 2023), el cual brinda una visión detallada del estado actual de la IA en 12 países de América Latina: Argentina, Bolivia, Brasil, Chile, Colombia, Costa Rica, Ecuador, México, Panamá, Paraguay, Perú y Uruguay. Para cada país generó una ficha con los hallazgos específicos en cada una de las tres dimensiones de estudio y sus subdimensiones.

- Dimensión Nº 1. Factores habilitantes: todos los elementos necesarios «para que se constituyan y desarrollen sistema de IA robustos en cada país», el cual está compuesto por tres subdimensiones: 1) Infraestructura, 2) Datos y 3) Desarrollo de talento.

- Dimensión Nº 2. Investigación, desarrollo y adopción: «mide los avances del ecosistema de investigación y el desarrollo e innovación (I+D+i) del país, considerando el desempeño del sector privado, la academia y el sector público». Incluye tres subdimensiones: 1) Investigación, 2) Innovación y Desarrollo y 3) Adopción.

- Dimensión Nº 3. Gobernanza, «mide el nivel de desarrollo del entorno institucional y regulatorio con respecto a los ecosistemas de IA en América Latina» a través de tres subdimensiones: 1) Visión e institucionalidad, 2) Internacional y 3) Regulación». En esta parte, se examinan las brechas que hay entre los países, así como las oportunidades que se deben aprovechar para «impulsar un desarrollo en IA con un enfoque ético, transparente y equitativo» de estos sistemas.

Según los puntajes obtenidos por cada país en el ILIA 2023, en cada una de las tres dimensiones, las posiciones en América Latina son las siguientes: Chile con 72.67 puntos se ubica en el primer lugar de la región, Brasil está en la segunda posición con 65.31 puntos y Uruguay registra el tercer puesto con 54.99 puntos (Cuadro 6). De los países de Centro América, Costa Rica ocupa el 8º lugar con 33.41 puntos y le sigue Panamá en el 9º puesto; y cierra este Índice de IA Bolivia que está ubicada en 12º lugar con 15.10 puntos.

Al revisar la Dimensión No 3, subdimensión Regulación, presentado en el Índice Latinoamericano de Inteligencia Artificial 2023, es posible identificar las leyes y normas en preparación o en vigencia que tienen como objetivo la protección de datos personales y de ciberseguridad para los sistemas de IA, así como las experiencias en su aplicación. Los resultados para los 12 países evaluados, más información de normas y leyes obtenida directamente de cada país son los siguientes.

Cuadro 6. Índice Latinoamericano de Inteligencia Artificial 2023

País	Posición	Puntaje del Indice	Dimensión 1: Factores Habilitantes	Dimensión 2: I+D+i y Adopción	Dimensión 3: Gobernanza
Chile	1	72.67	63.71	74.46	79.83
Brasil	2	65.31	60.32	47.37	88.23
Uruguay	3	54.99	53.82	75.95	35.19
Argentina	4	54.76	47.50	41.18	75.60
México	5	48.55	50.15	44.58	50.93
Colombia	6	47.62	51.28	35.04	73.21
Perú	7	45.55	38.39	21.51	65.08
Costa Rica	8	33.41	38.37	36.88	41.67
Panama	9	24.66	31.52	34.14	8.33
Ecuador	10	22.17	30.53	27.65	8.33
Paraguay	11	18.82	24.35	23.19	8.33
Bolivia	12	15.10\	21.99	23.31	0.00

Fuente: CENIA, Índice Latinoamericano de Inteligencia Artificial 2023 (ILIA2023). https://indicelatam.cl/

- **Argentina: no cuenta con una ley específica para IA**

Una de las primeras acciones sobre IA en Argentina fue *Plan Nacional de Inteligencia Artificial*, preparado entre 2018 y 2019, el cual, más que un Plan fue un informe sobre la situación de la IA en el país. El objetivo establecido originalmente fue crear mediante el uso de IA «un Estado ágil, eficiente y moderno que impulse medidas relevantes a los objetivos de crecimiento y desarrollo, garantice soluciones a las necesidades de los ciudadanos brindando más y mejores servicios y actuando como un actor clave en el impulso de la tecnología basada en IA y la transformación del país» (OECD Library). Con la implementación de este Plan se esperaba: aumentar la productividad y eficiencia de la administración pública a través de soluciones específicas; la utilización de sistemas IA trazables, con lógica fundamentada y transparente; garantizar procesos de compra e implementación de IA estandarizados, eficientes y exitosos. Sin embargo, después de su presentación no hubo avances ni se retomó el tema y quedó en el olvido, por lo que Argentina no tiene una estrategia nacional relativa a la IA.

La Ley de Protección de Datos (25326 del 4 de octubre de 2000) fue derogada y reemplazada por una nueva versión en junio de 2023 (Mensaje 87/2023), la que en su Artículo 1 señala que el objeto de esta normativa es «garantizar el ejercicio del derecho fundamental de las personas humanas a la protección de sus datos personales y su privacidad» (Gobierno de Argentina, 2023).

Con relación a los ciberdelitos, el Congreso de Argentina aprobó el 22 de noviembre de 2017 el Convenio sobre Ciberdelito del Consejo de Europa (Budapest, 23 de noviembre de 2001), al promulgar la Ley 27411 Convenio sobre Ciberdelito. Luego, el 4 de junio de 2008, mediante reforma al Código Penal (Ley 26388) se incorporó el concepto de *delito informático* de modo que en el Artículo 8 estableció que:

> Será reprimido con la pena de prisión de un (1) mes a dos (2) años el que: (1) A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales; (2) Ilegítimamente proporcionare o revelare a otro información registrada en un archivo o en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de la ley; (3) Ilegítimamente insertare o hiciere insertar datos en un archivo de datos personales. Sin embargo, no hay experiencias en el uso de las normativas para la IA. (Gobierno de Argentina, junio de 2008).

- **Bolivia: no cuenta con una ley específica para IA ni leyes para proteger los datos personales ni para combatir la ciberdelincuencia, por lo que no hay evidencias de casos de aplicación de regulaciones para el uso de IA.**

- **Brasil: En febrero de 2022 se creó una Comisión Parlamentaria para formular una Ley para regular las actividades que se realizan utilizando IA en Brasil.**

En respuesta a este mandato, se formuló el Proyecto de Ley 2338/2023 para regular la IA, para el cual se fijó como objetivo la «protección de los derechos y libertades fundamentales, la valorización del trabajo y la dignidad de la persona humana y la innovación tecnológica representada por la inteligencia artificial». El Proyectos de Ley (PL) fue presentado al Senado en diciembre de 2022, pero la Comisión dictaminó que había que realizar consultas públicas con representantes de la sociedad civil, las empresas de este sector tecnológico y con expertos en estas áreas del conocimiento, por lo que se esperaba que fuera aprobada a inicios de 2023. Sin embargo, aún no se logra aprobar porque se continúan haciendo modificaciones ante el avance innovador de las tecnologías que utilizan IA (DatacenterDynamics.com, 2024).

En Brasil, hay una correlación entre el PL para regular la IA y la Ley General de Protección de Datos (Nº13.709/18, del 14 de agosto de 2018), la que en su Artículo 1 estableció que «el tratamiento de datos personales, incluso en medios digitales, por parte de una persona física o jurídica de derecho público o privado, tiene como objeto proteger los derechos fundamentales

de la libertad y la privacidad y el libre desarrollo de la personalidad de las personas naturales» (Gobierno de Brasil, 2018). Además, mediante el Decreto Federal Nº 10.222, del 5 de febrero de 2020 se presentó la Estrategia Nacional de Ciberseguridad –E-Ciber– la que constituyó una orientación del Gobierno Federal sobre las principales acciones para aplicar en el área de ciberseguridad durante cuatrienio 2020-2023 (Gobierno de Brasil, 2020).

Además, la Autoridad Nacional de Protección de Datos publicó Análisis Preliminar sobre el PL 2338/2023 el 6 de julio de 2023, mediante el cual se busca regular los sistemas de IA en Brasil, en este caso, incluyendo normativas para la regulación de sandboxes para incentivar la innovación responsable y ética de la IA. También, este documento señala que el PL en estudio guarda relación con la Ley General de Protección de Datos, especialmente en lo correspondiente a los derechos de las personas y de los titulares de los datos, los riesgos en el uso de los datos personales y las normas de gobernanza (Gobierno de Brasil, 2023).

Finalmente, en Brasil se está preparando un proyecto para la creación de prototipos de políticas (*policy prototyping*) para orientar y abrir espacios a las empresas para utilizar las tecnologías que protegen y mejoran la privacidad (PET, siglas en inglés de *Privacy-Enhancing Technologies*) y reducir los riesgos de violación de la privacidad, lo cual también incluye los sistemas de IA. En la preparación de este PL están trabajando en conjunto autoridades de las áreas tecnológicas con el equipo *Open Loop* de Meta.

- **Chile: aunque ha habido avances y hay propuestas en proceso de aprobación, el país aún no cuenta con una ley específica para la IA**

En 2021 se presentó la Política Nacional de IA 2021, la que tiene tres ejes: 1) Factores Habilitantes, 2) Desarrollo y Adopción y 3) Gobernanza y Ética, los que proveen los lineamientos estratégicos a aplicar en materia de IA para los próximos 10 años. En adición, el marco de la Política Nacional de IA, en septiembre de 2021, autoridades de diversas instancias del gobierno de Chile con el apoyo del Banco de Desarrollo de América Latina (CAF), iniciaron estudios para crear un *sandbox* regulatorio de IA, para potenciar la innovación, atraer la inversión y estimular el aprendizaje conjunto público-privado (Gobierno de Chile, 2021).

Desde el 18 de agosto de 1999 tiene la Ley 19628, Sobre Protección de la Vida Privada, que en su Artículo 1º señala que «El tratamiento de los datos de carácter personal en registros o bancos de datos por organismos públicos o por particulares» estarán normados por esta ley, y aplicará a toda persona que trabaje con «datos personales», quien «deberá respetar el pleno ejercicio de los derechos fundamentales de los titulares de los datos» (Biblioteca del Congreso Nacional de Chile, 2020).

En Chile están las siguientes leyes y propuestas normativas sobre IA:

La Ley 21.459, aprobada el 9 de junio de 2022, estableció las normas que, sobre delitos informáticos, al tiempo que hizo otros ajustes a diversos cuerpos legales para cumplir con el Convenio de Budapest sobre ciberseguridad. En lo relativo a cualquier ataque a la integridad de un sistema informático, esta Ley impone sanciones a quien «obstaculice o impida el normal funcionamiento, total o parcial, de un sistema informático, a través de la introducción, transmisión, daño, deterioro, alteración o supresión de los datos informáticos» (artículo 1). También, estableció sanciones para quien haga un acceso ilícito, definido como un acto realizado «sin autorización o excediendo la autorización que posea y superando barreras técnicas o medidas tecnológicas de seguridad» (artículo 2), (Biblioteca del Congreso Nacional de Chile, 2022).

En adición, para promover la competencia e inclusión financiera mediante el uso de tecnologías innovadoras en la provisión de servicios financieros se aprobó la Ley FINTEC el 22 de diciembre de 2022 (Ley Nº 21.521), la cual «tiene por objeto establecer un marco general para incentivar la prestación de servicios financieros a través de medios tecnológicos que realicen los proveedores regidos por ella» (artículo 1). Esta Ley sustenta los principios de inclusión e innovación financiera, al tiempo que promueve la competencia, busca proteger al cliente financiero y los datos utilizados, así como contribuir a mantener la integridad y estabilidad financiera y prevenir el lavado de activos, el financiamiento del narcotráfico y del terrorismo (Biblioteca del Congreso Nacional de Chile, 2022).

Finalmente, se tiene la PL 15869-19, presentada el 26 de abril de 2023, que tiene como finalidad regular los sistemas de IA, la robótica y las tecnologías conexas en sus distintos ámbitos de aplicación. En el Artículo 1 de la propuesta dice: «La presente ley tiene el objetivo de establecer un marco jurídico en lo que respecta al desarrollo, comercialización, distribución y utilización de los sistemas de Inteligencia Artificial ... asegurando la protección de los derechos fundamentales garantizados por el Estado de Chile». El 11 de enero de 2024, la Comisión de Futuro de la Cámara de Diputados aprobó en términos generales este PL, el cual aún debe pasar varios trámites adicionales para su aprobación (Cámara de Diputados de Chile, 2023).

- **Colombia: no cuenta con una ley específica para IA**

Colombia presentó la Política Nacional para la Transformación Digital e Inteligencia Artificial el 8 de noviembre de 2019, en el cual presenta los fundamentos «para potenciar la generación de valor social y económico» en el país mediante el «uso estratégico de tecnologías digitales de manera amplia, involucrando al sector público y el sector privado... para impulsar

la productividad y favorecer el bienestar de los ciudadanos, quienes son los beneficiarios y consumidores de los bienes y servicios que se producen» (CONPES, 2019).

En adición, actualmente hay cuatro Proyectos de Ley (PL) en procesos de estudio en el Congreso para regular la IA, de los cuales dos crearían un marco regulatorio para el desarrollo, uso e implementación de IA, uno para normar el derecho de información y otro para complementar su uso con el derecho al trabajo. Además, el Ministerio de Ciencia, Tecnología e Innovación presentó en febrero de 2024 la Hoja de Ruta para garantizar la adopción ética y sostenible de la IA.

El 8 de marzo de 2022 se aprobó el Decreto 338, «Lineamientos Generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital», con el cual busca fortalecer la gobernanza de la seguridad digital (Gobierno de Colombia, 2022).

Es de destacar, que en Colombia se han aplicado *sandboxes* regulatorios de IA con la orientación de la OECD (para la establecer normas y regulaciones en conjunto con la participación de reguladores y organizaciones tecnológicas, para responder a los rápidos avances innovadores de la IA y la tecnología financiera (FINTECH) (ColombiaInteligente.org, 2023).

Actualmente hay cuatro PL en procesos de estudio. Ellos son:

(1) PL 59-23 (en el Senado), que tiene como objeto, según el Artículo 1: «establecer los lineamientos de política pública para el desarrollo, uso e implementación de Inteligencia Artificial». Conceptualmente, la política que se establece en este proyecto de Ley señala que debe estar centrada en el ser humano y la equidad, de modo que la inteligencia humana debe prevalecer sobre la IA (artículo 9); luego, ordena que «para el uso, desarrollo e implementación de la inteligencia artificial deberán tener como propósito la preservación del ser humano y su entorno ambiental» (artículo 10); y también se refiere a la «Igualdad en el Dato», para lo cual establece que el uso de datos por medio de IA «no pueden permitir que se generen resultados que resulten como actos discriminatorios» por lo que «se deberá garantizar la igualdad de trato e igualdad de oportunidades». También, esta PL establece sanciones en el uso de IA cuando esta cause «restricciones de la libre competencia» (Congreso de la República de Colombia, 2023).

(2) PL 91/23 (en el Senado) del 9 de agosto de 2023, para establecer «el deber de información para el uso responsable de las Inteligencias Artificiales en Colombia, dentro de los parámetros éticos y legales que garanticen la seguridad, transparencia, igualdad u equidad» (Gobierno de Colombia, 2023).

(3) PL 130/23 (en el Senado), para armonizar la AI «con el derecho al trabajo de las personas». Este PL «tiene como finalidad la protección de los derechos de los trabajadores y la correcta utilización de la inteligencia artificial buscando garantizar la estabilidad laboral y el derecho al trabajo de las personas» (numeral 2) (Asuntos Legales, 2023).

(4) PL Estatutaria 200/23 (en la Cámara de Representantes), que busca definir y regular la AI en Colombia, en concordancia con los estándares de Derechos Humanos, para lo cual «se establecen límites frente a su desarrollo, uso e implementación». En el Numeral 2 del AP de la Ley Estatutaria tiene señala que su objeto es «ajustar a estándares de respeto y garantía de los derechos humanos la inteligencia artificial, regular su desarrollo y establecer límites frente a su uso e implementación por parte de personas naturales y jurídicas... (y) pretende establecer un marco jurídico seguro para el desarrollo tecnológico sin que represente cargas administrativas innecesarias para las pymes y las empresas emergentes, pero basado en consideraciones éticas y en el respeto de los derechos humanos y fundamentales», al tiempo que busca reforzar la protección de datos personales (IABcolombia.com, 2023).

- **Costa Rica: no cuenta con una ley específica para IA**

Tienen la Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, No 8968, del 27 de junio de 2011, la cual «tiene como objetivo garantizar a cualquier persona, independientemente de su nacionalidad, residencia o domicilio, el respeto a sus derechos fundamentales, concretamente, su derecho a la autodeterminación informativa en relación con su vida o actividad privada y demás derechos de la personalidad, así como la defensa de su libertad e igualdad con respecto al tratamiento automatizado o manual de los datos correspondientes a su persona o bienes» (OEA, 2011).

Con el apoyo de la Embajada del Reino Unido, Costa Rica comenzó a trabajar en un proceso que le tomará alrededor de 9 meses (agosto de 2018 y abril 2019) para hacer una propuesta para la creación de un *sandbox* de innovación, *Revolutionary Sandbox.* Así, busca estimular el crecimiento económico del país, especialmente, facilitando un desarrollo más rápido de ecosistemas como Blockchain/Fintech y Diseño/Innovación, dando un espacio que facilite y habilite condiciones favorables para el emprendimiento y la innovación disruptiva (IdeasLabs.org, 2022).

El 27 de febrero de 2023 el Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones (MICITT) inició el proceso para la formulación de la Estrategia de Inteligencia Artificial, en un acto público que llamó «Hacia una Estrategia de Inteligencia Artificial en Costa Rica». Esta estrategia se formulará en concordancia con la «Recomendación sobre la ética en la inteligencia

artificial» de la UNESCO, con el apoyo del Banco de Desarrollo de América Latina y el Caribe (CAF), con el objetivo de establecer la hoja de ruta para construir procesos de vinculación y transformación social y productiva del país, mediante un trabajo conjunto con *fAIr Lac* y el Centro Nacional de Alta Tecnología. De esta manera, Costa Rica busca convertirse en Hub centroamericano para el desarrollo de IA (MICITT, 2023).

El *fAIr Lac* es una herramienta que tiene seis dimensiones: 1) Conceptualización y diseño, 2) Gobernanza y seguridad, 3) Involucramiento humano en los sistemas de IA, 4) Ciclo de vida de la IA (datos y algoritmos), 5) Actores relevantes, y 6) Comunicaciones, que tiene como objetivo orientar a los emprendedores a identificar los desafíos más importantes y soluciones a encontrar, para reducir sesgos, discriminación y exclusiones. Si bien esta herramienta se orienta principalmente al uso responsable de la IA en el sector público, también contiene herramientas para el sector privado, en especial, para los emprendedores (Torres, *et al.*, 2021).

En adición, la Comisión Permanente Especial de Ciencia, Tecnología y Educación emitió un Dictamen Afirmativo Unánime, del Proyecto de Ley de Ciberseguridad de Costa Rica (expediente 23.291). En su Artículo 1 establece como «objetivo crear el marco jurídico para la regulación, el resguardo y protección de la seguridad cibernética de las infraestructuras de tecnologías críticas del país, en las instituciones del Gobierno Central, Descentralizadas y Semiautónomas» (Asamblea Legislativa, 2023).

- **Ecuador: no cuenta con una ley específica para IA**

Ecuador tiene la Ley orgánica de protección de datos personales, aprobada el 10 de mayo de 2021, la cual tiene como «objeto y finalidad... garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter , así como su correspondiente protección» (artículo 1); normativa jurídica que será aplicada «al tratamiento de datos personales contenidos en cualquier tipo de soporte, automatizados o no, así como a toda modalidad de uso posterior» (Asamblea Nacional, 2021).

En Ecuador está en proceso de revisión la propuesta de Ley orgánica de seguridad digital, ciberseguridad, ciber defensa y ciberinteligencia, la que tiene como objeto «establecer un Sistema de Seguridad Digital, con los componentes o subsistemas de ciberseguridad, ciberdefensa que permita prevenir, combatir, reaccionar, neutralizar, manejar la o las crisis y recuperar información en caso de amenazas, riegos y/o ataques informáticos... y promover la seguridad digital en los distintos niveles del gobierno y de la ciudadanía en el ciberespacio. El Ecuador debe defender y proteger la soberanía, seguridad integral, las

infraestructuras críticas públicas y privadas, la integridad política, la seguridad económica y la seguridad nacional; así también, salvaguardar los sistemas de información digital de los organismos estratégicos, operacionales y tácticos ante ataques, riesgos o amenazas en el ciberespacio». La aprobación de esta propuesta de Ley requerirá «adecuar los tipos penales que establece el Convenio de Budapest (y) el Código Orgánico Integral Penal» (Asamblea Nacional, 2023).

En el Ecuador no hay antecedentes de experimentación regulatoria para el uso de IA

- **México: no cuenta con una ley específica para IA**

El 21 de marzo de 2018 la Coordinación de Estrategia Digital Nacional presentó la Estrategia de Inteligencia Artificial de México 2018, la que tiene como objetivo establecer un marco de gobernanza para fomentar el diálogo multisectorial, definir los usos y necesidades en la industria e identificar las mejores prácticas. En este contexto, se realizaron consultas públicas (Gobierno de México, 2018).

México cuenta con la Ley orgánica de protección de datos personales de julio de 2010, la que «tiene por objeto la protección de los datos personales en posesión de los particulares... regular su tratamiento legítimo, controlado e informado, a efecto de garantizar la privacidad y el derecho a la autodeterminación informativa de las personas» (artículo 1). Luego, en el Artículo 6 establece que «"Los responsables en el tratamiento de datos personales, deberán observar los principios de licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad» (Gobierno de México, 2010).

Además, está en estudio el Proyecto de Ley Federal de Ciberseguridad, que en el Artículo 2 señala que su objeto es «Regular la integración, organización y funcionamiento de la instancia encargada de las actividades de ciberseguridad a nivel nacional», «Implementar y revisar periódicamente la Estrategia Nacional de Ciberseguridad», «Salvaguardar el uso seguro y responsable de las redes, los sistemas de información y comunicaciones», «Establecer el catálogo de delitos cibernéticos de competencia federal y contribuir a la prevención especial y general de dichos delitos; y "Contribuir a la investigación y la persecución de los delitos cibernéticos» (Gobierno de México, 2024).

También en México se está trabajando en el Proyecto de creación de prototipos de políticas (*policy prototyping*) para sistemas de IA con el apoyo del Banco Interamericano de Desarrollo, C Minds, aportes de expertos regionales, la academia y la sociedad civil. Por medio de este Proyecto se diseñó la iniciativa fAIr LAC, para promover el uso responsable de la IA como herramienta para mejorar la prestación de servicios sociales y generar igualdad de oportunidades

de desarrollo para así contribuir a la reducción de las brechas y la desigualdad (C Minds, 2023).

- **Panamá: no cuenta con una ley específica para IA**

Panamá presentó su primera versión de la Estrategia Nacional de Seguridad Cibernética y Protección de Infraestructuras Críticas desde el 12 de marzo de 2013, en la que se establecieron diversas acciones para mejorar la ciberseguridad y proteger las infraestructuras tecnológicas claves del país. Sin embargo, esta Estrategia no se puso en marcha. No fue hasta el 10 se septiembre de 2021 que se aprobó la Estrategia Nacional de Ciberseguridad para el período 2021-2024, la cual tiene cuatro pilares: 1) Proteger la privacidad y los derechos fundamentales de los ciudadanos en el ciberespacio; 2) Disuadir y castigar el comportamiento Criminal en el ciberespacio; 3), Fortalecer la seguridad y la resiliencia de la infraestructura crítica; y 4), Fomentar una cultura nacional de ciberseguridad (Gobierno de Panamá, 2022).

Panamá, también, cuenta con la Ley Nº 81 sobre Protección de Datos Personales del 26 de marzo de 2019, la que tiene como objeto «establecer los principios, derechos, obligaciones y procedimientos que regulan la protección de datos personales, considerando su interrelación con la vida privada y demás derechos y libertades fundamentales de los ciudadanos, por parte de las personas naturales o jurídicas, de derecho público o privado, lucrativas o no, que traten datos personales» (artículo 1) (Gobierno de Panamá, 2019).

Panamá: El PL Nº 558 sobre ciberseguridad, que se presentó en la Asamblea Nacional, el 10 de agosto de 2017, mediante el cual modifica y adiciona artículos al Código Penal, en aspectos relacionados con el cibercrimen. Este PL plantea como objetivo hacer modificaciones al Código Penal de Panamá para cumplir con los estándares internacionales de seguridad informática, aspectos relacionados con el cibercrimen y el Convenio de Budapest, que fuera probado por Panamá en 2013 (Cámara de Comercio, 2017).

En Panamá no hay antecedentes de experimentación regulatoria para el uso de IA.

- **Paraguay: no cuenta con una ley específica para IA**

Paraguay no cuenta con un Plan o una Estrategia Nacional de IA, aunque tiene un Plan Nacional de Ciberseguridad aprobado el 24 de abril de 2017, que brinda una visión estratégica mediante el establecimiento de las bases para la coordinación de las políticas públicas de ciberseguridad, para desarrollo tecnológico en un ambiente cibernético confiable y resiliente (Gobierno de Paraguay, 2017). Además, con la Ley Nº 5994 del 27 de julio de 2017, aprobó

la *Convención sobre Ciberdelincuencia* (Budapest, 23 de noviembre de 2001), y el Protocolo Adicional al Convenio sobres Ciberdelincuencia Relativo a la Penalización de Actos de Índole Racista y Xenófoba cometidos por medio de Sistemas Informáticos (Estrasburgo) (Gobierno de Paraguay, 2017).

Paraguay tiene la Ley Nº 4439 del 8 de septiembre de 2011, mediante la cual se modificaron varios artículos del Código Penal de Paraguay, para definir y castigar ciberdelitos como la pornografía relativa a niños y adolescentes, el acceso indebido a datos y su interceptación, el uso indebido de sistemas informáticos, estafas mediante el uso de sistemas informáticos y la falsificación de medios electrónicos de pago. Con estas modificaciones, se cumplieron los estándares mínimos del Convenio de Budapest (Gobierno de Paraguay, 2011).

También, cuenta con la Ley Nº 6534 de Protección de Datos Personales Crediticios del 28 de abril de 2020, la cual tiene como objeto «garantizar la protección de datos crediticios de toda persona, cualquiera sea su nacionalidad, residencia o domicilio», así como regular la «recolección y el acceso a datos de información crediticia... constitución, organización, funcionamiento, derechos, obligaciones y extinción de las personas jurídicas que se dediquen a la obtención y provisión de información crediticia... (para) preservar los derechos fundamentales, la intimidad, la autodeterminación informativa, la libertad, la seguridad y el trato justo de las personas» (Gobierno de Paraguay, 2020).

En Paraguay no hay antecedentes de experimentación regulatoria para el uso de IA.

- **Perú: tiene una ley específica para IA, para proveer un entorno seguro, confiable y ético**

Perú presentó la Estrategia Nacional de Inteligencia Artificial (ENIA) para el período 2021-2026, para impulsar el desarrollo de la IA en el país, para convertirlo «en un referente regional en investigación, desarrollo y aplicaciones de esta tecnología» (Gobierno de Perú, 2021). La ENIA se enfoca en seis ejes estratégicos para generar nuevas oportunidades de desarrollo, con prioridad en los sectores productivos y servicios públicos: 1) Formación y atracción del talento, «para la investigación, desarrollo y usos de IA», 2) Modelo Económico, para «promover el desarrollo de la IA y su adopción» para impulsar «el desarrollo, la innovación y el bienestar del país», 3) Infraestructura tecnológica, «para facilitar la creación y el fortalecimiento» de ella, 4) Datos, para desarrollar «una infraestructura de datos para poner a disposición de datos públicos de alta calidad en un formato abierto, reutilizable y accesible», 5) Ética, para «adoptar lineamientos... para un uso sostenible, transparente y replicable de la IA con definiciones claras sobre

responsabilidades y protección de datos, y (6) Colaboración, para facilitar un ecosistema de colaboración de IA a nivel nacional e internacional».

Además, está la Ley Nº 31814, del 13 de junio de 2023, que «tiene por objeto promover el uso de la inteligencia artificial en el marco del proceso nacional de transformación digital privilegiando a la persona y el respeto de los derechos humanos con el fin de fomentar el desarrollo económico y social del país, en un entorno seguro que garantice su uso ético, sostenible, transparente, replicable y responsable» (artículo 1). Luego, define en el Artículo 2 el concepto de interés nacional como «la promoción del talento digital en el aprovechamiento de las tecnologías emergentes y nuevas tecnologías en favor del bienestar social y económico, así como el fomento del desarrollo y uso de la inteligencia artificial para la mejora de los servicios públicos, de la educación y los aprendizajes, la salud, la justicia, la seguridad ciudadana, la seguridad digital, la economía, la inclusión, los programas sociales, la seguridad y la defensa nacional, así como para toda otra actividad económica y social a nivel nacional» (Gobierno de Perú, 2023).

También, tiene la Ley Nº 30999 de ciberdefensa del 26 de agosto de 2019, la cual «tiene por objeto establecer el marco normativo en materia de ciberdefensa del Estado…regulando las operaciones militares en y mediante el ciberespacio a cargo de los órganos ejecutores del Ministerio de Defensa dentro de su ámbito de competencia, conforme a ley» (Gobierno de Perú, 2019).

Desde el 21 de junio de 2011 Perú tiene la Ley No 29733, Protección de Datos Personales, que estableció como su objeto «garantizar el derecho fundamental a la protección de los datos personales… a través de su adecuado tratamiento, en un marco de respeto de los demás derechos fundamentales…» (artículo 1). Y en el Artículo 3 fijó su ámbito de aplicación «a los datos personales contenidos o destinados a ser contenidos en bancos de datos personales de administración pública y de administración privada, cuyo tratamiento se realiza en el territorio nacional… (especialmente, la) protección los datos sensibles» (Gobierno de Perú, 2011).

En Perú no hay antecedentes de experimentación regulatoria para el uso de IA.

- Uruguay: no cuenta con una ley específica para IA

Sin embargo, Uruguay se adhirió a la declaración regulatoria a nivel global sobre IA en el transcurso de la 4ª Asamblea de la Alianza Europea de IA en noviembre de 2023, que es un compromiso de los países de Europa, Latinoamérica y el Caribe por avanzar en la cooperación conjunta de políticas y marcos regulatorios de esta tecnología (Gobierno de Uruguay, 2023).

Uruguay tiene definida la Estrategia de Inteligencia Artificial, presentada por la Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento el 23 de abril de 2021, mediante la cual fijó las bases «para la transformación digital... con el propósito de promover y fortalecer su uso responsable en la Administración Pública». Se definió como objetivo de la Estrategia «promover y fortalecer el uso responsable de IA en la Administración Pública», para lo cual se establecieron cuatro pilares: 1) Gobernanza de IA en la Administración Pública, 2) Desarrollo de capacidades para la IA, en los funcionarios públicos, 3) Uso y aplicación de la IA para fortalecer su buen uso en la Administración Pública, y 4) Ciudadanía Digital e IA, para «preparar a la ciudadanía para aprovechar las oportunidades y hacer frente a los desafíos que trae aparejados la IA... generar la confianza necesaria en las personas para desarrollar y utilizar las nuevas tecnologías» (Gobierno de Uruguay, 2021).

Para el desarrollo del trabajo se definieron nueve principios generales: 1) Finalidad, 2) Interés general, 3) Respeto de los Derechos Humanos, 4) Transparencia, para poner a disposición los algoritmos y datos utilizados para el entrenamiento de la solución y su puesta en práctica, así como las pruebas y validaciones realizadas, así como visibilizarlos a través de mecanismos de transparencia activa, para quienes IA, ya sea en la generación de servicios públicos o en el apoyo a la toma de decisiones, 5) Responsabilidad, definiendo claramente el responsable y para responder ante cualquier acto indebido, 6) Ética, 7) Valor agregado, para potenciar el desarrollo del Gobierno Digital, 8) Privacidad por diseño para proteger la privacidad de las personas, y 9) Seguridad, para proteger la información y cumplir con la normativa de ciberseguridad (Gobierno de Uruguay, 2021).

Uruguay tiene la Ley de Protección de Datos Personales Nº18331, del 11 de agosto de 2008, la cual señala que la normativa aplicará «a los datos personales registrados en cualquier soporte que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los ámbitos público o privado» (Artículo 3). También estableció la forma de actuar de toda persona del sector público o privado que trabajen con datos personales de terceros, deberán cumplir con siete principios generales: 1) Legalidad, 2) Veracidad, 3) Finalidad, 4) Previo consentimiento informado, 5) Seguridad de los datos, 6) Reserva y 7) Responsabilidad (IMPO, 2008).

Si bien la República Dominicana no se incluyó entre los 12 países que evaluó el Índice Latinoamericano de Inteligencia Artificial 2023, es de señalar que este país tiene la Ley Nº172/13, Protección Integral de los Datos Personales, del 13 de diciembre de 2013. En el Artículo 1 señala que el objeto de la Ley es «la protección integral de los datos personales asentados en archivos, registros públicos, bancos de datos u otros medios técnicos de tratamiento de datos destinados a dar informes, sean estos públicos». En adición, está

la Ley Nº107-13, del 6 de agosto de 2013, sobre los Derechos de las Personas en sus Relaciones con la Administración y de Procedimiento Administrativo, que en su artículo 3.20 sustenta el principio de protección de la intimidad, al decir: «...el personal al servicio de la Administración Pública que maneje datos personales respetará la vida privada y la integridad de las personas, prohibiéndose el tratamiento de los datos personales con fines no justificados y su transmisión a personas no autorizadas».

Como se puede observar en la información jurídica y normativa antes presentada, las leyes de los países de América Latina no consideran específicamente la regulación de la IA, salvo Chile que está en proceso para regular los sistemas de IA, la robótica y las tecnologías conexas y Brasil que tiene una propuesta de Ley de IA.

No obstante, hay un marcado interés por enfrentar los desafíos y oportunidades que presenta el desarrollo y utilización de la IA, el cual condujo a la realización del *Encuentro Latinoamericano de Inteligencia Artificial* realizado entre el 6 y el 10 de marzo de 2023, KHIPU 2023, en la que participaron expertos referentes en tecnología internacional y más de 100 especialistas y de la comunidad científica de la región, quienes firmaron la Declaración de Montevideo sobre la Inteligencia Artificial, en la que instaron a los gobiernos y empresas "a que los desarrollos de IA se pongan al servicio de las personas, reflejando las particularidades y problemáticas de América Latina", para lograr una mejora en la calidad de vida, en concordancia con los principios democráticos y de los derechos humanos. Sus participantes fueron principalmente de la academia de 18 países: Argentina, Bolivia, Brasil, Canadá, Colombia, Costa Rica, El Salvador (Universidad Centroamericana José Simeón Cañas), Ecuador, España, Estados Unidos de América, Guatemala, Francia, Israel, México, Paraguay, Reino Unido, Uruguay, Venezuela; así como representantes de ONG que trabajan en áreas relacionadas con la IA (Giandana, 2023).

Posteriormente, en octubre de 2023 se realizó la Cumbre Ministerial sobre la Ética de la Inteligencia Artificial, en la que participaron más de 20 ministros, representantes de gobiernos, la academia, organismos internacionales y del sector privado, en la que discutieron sobre la formulación de políticas públicas, regulación y los habilitadores para el uso ético de la Inteligencia Artificial en la región. Esta Cumbre fue organizada por la CAF, UNESCO y el Gobierno de Chile. Representantes de Argentina, Brasil, Chile, Colombia, Costa Rica, Cuba, Ecuador, El Salvador, Guatemala, Honduras, Jamaica, México, Perú, Paraguay, República Dominicana, Santa Lucía, San Vicente y las Granadinas, Surinam, Uruguay y Venezuela tomaron la decisión de trabajar conjuntamente en la regulación, ética, gobernanza y adopción de estándares relacionados con la IA.

En esta Cumbre, los gobiernos participantes aprobaron la Declaración de Santiago en la que reiteraron «la universalidad, la indivisibilidad, interdependencia e interrelación de todos los derechos humanos y libertades fundamentales», los que también aplican en el entorno digital (Gobierno de Chile, 2023, numeral 1). También, reconocieron que «la IA puede contribuir a la transformación de los modelos de desarrollo en los países de América Latina y el Caribe, haciéndolos más productivos, inclusivos y sostenibles, y que para aprovechar sus oportunidades y mitigar sus potenciales amenazas se requiere reflexión, visión estratégica, regulación, gobernanza y coordinación regional y multilateral» (Ibidem, numeral 2).

Además, expresaron su preocupación por que algunas aplicaciones de la IA pueden afectar adversamente los derechos humanos, lo cual puede generar "temor e incertidumbre tanto en el mundo del trabajo, como respecto de la protección de la vida privada y los datos personales, en la democracia y el quehacer de los Estados, y en el surgimiento de nuevas desigualdades y brechas (Ibidem).

También, en la Declaración resaltaron «que el derecho internacional de los derechos humanos y las normas y principios éticos previstos en la Recomendación sobre la Ética de la Inteligencia Artificial, así como las recomendaciones de políticas en la materia, ofrecen un marco universalmente aceptado, justo, plural, y equitativo, para considerar, evaluar y, en última instancia, corregir los impactos negativos de la IA sobre las personas y la sociedad, y maximizar sus beneficios, respetando y representando diferencias culturales, geográficas, económicas, ideológicas, religiosas entre otras, y no reforzar estereotipos o profundizar la desigualdad» (Ibidem, numeral 5).

Además, reconocieron que, «sin las debidas salvaguardias, la IA puede reforzar la discriminación, exclusión y sesgos de género, incluyendo las desigualdades estructurales, así como agravar las divisiones y desigualdades existentes dentro de los países y entre ellos» (numeral 7); y que ante los posibles escenarios positivos y negativos que presenta la IA, es necesario «normar el desarrollo tecnológico en un marco ético, y ... adoptar acciones concretas (para ampliar) sus beneficios y mitigar sus riesgos, con el fin de garantizar el bienestar humano y una convivencia pacífica con las tecnologías» (Gobierno de Chile, 2023, numeral 8).

Además, fueron enfáticos en la necesidad «de elaborar y adoptar medidas de política pública y normas jurídicas que tengan como marco todas las normas y principios transversales de derechos humanos, incluyendo la proporcionalidad e inocuidad, la seguridad y protección, la equidad y la no discriminación, la igualdad de género, la accesibilidad, la sostenibilidad –social, cultural, económica y ambiental–, el derecho a la intimidad y la protección de datos

personales, la supervisión y decisión humana, la seguridad de la información, la transparencia y la explicabilidad, la responsabilidad y la rendición de cuentas, la sensibilización y educación, y la gobernanza y colaboración adaptativas y de múltiples partes interesadas, entre otros». Responder adecuadamente a esta necesidad, se consideró como el punto de inicio para la generación de políticas públicas que promuevan el uso ético de la IA (Ibidem, numeral 9).

Los participantes en la cumbre Ministerial de Santiago, también reconocieron que son responsables de garantizar el respeto de los derechos humanos en el diseño, desarrollo y uso de la IA «las empresas privadas, las organizaciones de la sociedad civil, el sector público, organismos internacionales y las instituciones de investigación y educación... (así como el) diseño e implementación de medidas oportunas para prevenirlos, mitigarlos o repararlos, de acuerdo a sus propias legislaciones internas» (Ibidem, numeral 11).

Finalmente, la *Declaración de Santiago* proclamaron que ante las oportunidades y riesgos que presenta el uso de la IA, los Estados deben anticiparse y diseñar de «políticas, planes y estrategias nacionales, regionales e internacionales, para el diseño, desarrollo y uso seguro, ético y responsable de esta tecnología... con un enfoque de Derechos Humanos» (Gobierno de Chile, 2023, Proclama, numeral 1). Además, señalan que concordaron que es necesario «elaborar y adoptar nuevos marcos jurídicos y agendas regulatorias para el diseño, desarrollo y uso responsable de la IA», manteniendo como base «todos los principios transversales de derechos humanos, en especial los principios de la proporcionalidad e inocuidad, de la seguridad y protección, la equidad y la no discriminación, de la inclusión, de la diversidad de género, de la diversidad cultural, de la accesibilidad, de la sostenibilidad –social, cultural, económica y ambiental–, del derecho a la intimidad y la protección de datos personales, de la supervisión y decisión humana, de la transparencia y la explicabilidad, de la responsabilidad y la rendición de cuentas, de la sensibilización y educación, y de la gobernanza inteligente y colaboración adaptativas y de múltiples partes interesadas» (Ibidem).

Con un enfoque de desarrollo, en esta Declaración se señaló la necesidad de incentivar las inversiones para promover la innovación y aprovechar la potencialidad de la IA para solucionar diversos problemas. Concluye la Declaración expresando que tiene beneficios «fortalecer la gobernanza, representatividad y calidad de los datos utilizados para entrenar los sistemas de IA, y promover e invertir en mecanismos que permitan el intercambio seguro, equitativo, legal y ético de datos, en coherencia con la Recomendación sobre la Ética de la Inteligencia Artificial de la UNESCO» (Gobierno de Chile, 2023, cierre de la Declaración).

Bibliografía

A

Acemoğlu, Daron; y Johnson, Simon. IMF. (diciembre de 2023). *Rebalancing AI.* https://www.imf.org/en/Publications/fandd/issues/2023/12/Rebalancing-AI-Acemoglu-Johnson

Agencia de la Unión Europea para la Ciberseguridad [ENISA]. (junio de 2020). *Una Europa que ofrece ciberseguridad y confianza. Estrategia de la ENISA.* https://www.enisa.europa.eu/publications/enisa-strategy-leaflet-translations/enisa-strategy-leaflet-es.pdf

Amazon, AWS. (2024). *¿Qué es la ciberseguridad?* https://aws.amazon.com/es/what-is/cybersecurity/#:~:text=La%20ciberseguridad%20es%20la%20pr%C3%A1ctica,cliente%20y%20cumplir%20la%20normativa.

Asamblea Legislativa de El Salvador. (18 de abril de 2023). *Ley de fomento a la innovación y manufactura de tecnologías.* https://www.asamblea.gob.sv/sites/default/files/documents/decretos/C4062E8E-154F-4F82-9835-7C1D16EF4616.pdf

Asamblea Legislativa de El Salvador. (11 de enero de 2023). Ley de emisión de activos digitales. https://www.asamblea.gob.sv/sites/default/files/documents/decretos/BED5A3F8-8937-4547-A291-CE06802B0B23.pdf

Asamblea Legislativa de El Salvador. (8 de junio de 2021). *Ley Bitcoin.* https://www.asamblea.gob.sv/sites/default/files/documents/decretos/43DA8049-AA39-4DA8-B892-437B2DD27C1C.pdf

Asamblea Legislativa de El Salvador. (13 de abril de 2021). *Ley de Protección de Datos Personales, Proyecto Final.* https://www.asamblea.gob.sv/sites/default/files/documents/dictamenes/498798FA-A563-4830-A0C8-306AFBC71497.pdf

Asamblea Legislativa de El Salvador. (15 de febrero de 2013). *Ley de Desarrollo Científico y Tecnológico.* https://www.asamblea.gob.sv/sites/default/files/documents/decretos/171117_073311194_archivo_documento_legislativo.pdf

Asamblea Legislativa de El Salvador. (2 de diciembre de 2010). *Ley de acceso a la información pública.* https://www.asamblea.gob.sv/sites/default/files/documents/decretos/6FEC6152-A946-4C2E-B232-04C3EA89FCE0.pdf]

Asamblea Legislativa de la República de Costa Rica, Departamento Estudios, Referencias y Servicios Técnicos. (julio de 2023). *Informe de: Proyecto de Ley, Dictamen, Ley*

de Ciberseguridad de Costa Rica, Expediente No 23292. https://d1qqtien6gys07.cloudfront.net/wp-content/uploads/2023/11/ST_23292INFORME-TECNICO3024.pdf

Asuntos Legales, Colombia. (28 de diciembre de 2023). *Colombia avanza en la regulación de Inteligencia Artificial.* https://www.asuntoslegales.com.co/consultorio/colombia-avanza-en-la-regulacion-de-inteligencia-artificial-3773836

Ayuso, S. (13 de marzo de 2024). *La Eurocámara apoya con amplia mayoría la ley de inteligencia artificial. El País, Tecnología.* https://elpais.com/tecnologia/2024-03-13/la-eurocamara-apoya-con-amplia-mayoria-la-ley-de-inteligencia-artificial.html

Ayuso, S. (8 de diciembre de 2023). *La UE aprueba la primera ley de inteligencia artificial del mundo. El País, Tecnología.* https://elpais.com/tecnologia/2023-12-08/la-ue-aprueba-la-primera-ley-de-inteligencia-artificial-del-mundo.html

B

Balderrama, R., Trejo, A. (2018). El proyecto "Hecho en China 2025": Impulso del Estado hacia la transformación industrial con alcance global. Volume XVIII, Number 1. https://revista.drclas.harvard.edu/made-in-china-2025/

Barrera, J. (21 de febrero 2024). *Las 10 apps de inteligencia artificial más populares y fáciles de usar. ElSalvador.com.* https://www.elsalvador.com/entretenimiento/tecnologia/10-aplicaciones-inteligencia-artificial-mas-populares-faciles-de-usar/1124538/2024/

Banco Bilbao Vizcaya Argentaria [BBVA]. (20 de abril de 2023). *¿Qué es y por qué es importante? Regulación europea sobre Mercados de Criptoactivos (MiCA).* https://www.bbva.com/es/innovacion/regulacion-europea-sobre-mercados-de-criptoactivos-mica-que-es-y-por-que-es-importante/

Bejerano, P. G. (4 de enero de 2024). *¿Máquinas con ética? Cómo enseñar moral a los ordenadores al traducir deontología a números. El País, Tecnología.* https://elpais.com/tecnologia/2024-01-05/maquinas-con-etica-como-ensenar-moral-a-los-ordenadores-al-traducir-deontologia-a-numeros.html

Biblioteca del Congreso Nacional de Chile. (s.f)Ley Nº 21.521, *Promueve la Competencia e Inclusión Financiera a través de la Innovación y Tecnología en la prestación de Servicios Financieros, Ley FINTEC. Chile.* https://www.bcn.cl/leychile/navegar?idNorma=1187323

iblioteca del Congreso Nacional de Chile. (8 de abril de 2024). Ley 21.459, normas que sobre delitos informáticos. https://www.bcn.cl/leychile/navegar?idNorma=1177743&idVersion=Diferido

Biblioteca del Congreso Nacional de Chile. (10 de noviembre de 2022). Ley 19628 del 18 de agosto de 1999, Sobre Protección de la Vida Privada. https://www.bcn.cl/leychile/navegar?idNorma=141599&idVersion=2023-05-09&idParte=8642700

Blog.carsync.com. (17 de diciembre de 2021). *¿Quién inventó el GPS? La historia del rastreo* satelital. https://blog.carsync.com/blog/quien-invento-el-gps-la-historia-del-rastreo-satelital

Brascia, C. A. (26 de enero de 2024). *La red se llena de porno 'deepfake' de Taylor Swift y muestra el peligro de la IA para las mujeres. El País, Tecnología.* https://elpais.com/tecnologia/2024-01-26/la-red-se-llena-de-porno-deepfake-de-taylor-swift-y-muestra-el-peligro-de-la-ia-para-las-mujeres.html

Brynjolfsson, E; Unger, G. (diciembre de 2023). *The macroeconomics of Artificial Intelligence.* https://www.imf.org/en/Publications/fandd/issues/2023/12/Macroeconomics-of-artificial-intelligence-Brynjolfsson-Unger

C

Cámara de Comercio, Industrias y Agricultura de Panamá. Proyecto de Ley (No. 558 de 2017). *Que Modifica y Adiciona Artículos al Código Penal, Relacionados con El Cibercrimen.* https://www.panacamara.com

Cámara de Diputados de Chile. (26 de abril de 2023). *Proyecto de ley que regula los sistemas de IA, la robótica y las tecnologías conexas en sus distintos ámbitos de aplicación.* https://www.camara.cl/verDOC.aspx?prmID=72777&prmTipo=FICHA-PARLAMENTARIA&prmFICHATIPO=DIP&prmLOCAL=0

Arteaga, G., C. (8 de agosto de 2022). *La protección de datos y regulación de la IA en UK.* https://www.hosteltur.com/comunidad/005126_los-detalles-de-reforma-de-la-proteccion-de-datos-y-regulacion-de-la-ia-en-uk.html

Cazzaniga, Cazzaniga, M., Li., L., Rockall,E. J Pizzinelli, C., Panton, A.J., Jaumotte, F., Melina, G. (2024). *AI: Artificial Intelligence and the Future of Work. International Monetary Fund.* https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2024/01/14/Gen-AI-Artificial-Intelligence-and-the-Future-of-Work-542379

Center for Security and Emerging Technology, [CSET]. (October 21, 2021). Ethical Norms for New Generation Artificial Intelligence Released (新一代人工智能伦理规范发布). Georgetown University's Walsh School of Foreign Service. https://cset.georgetown.edu/publication/ethical-norms-for-new-generation-artificial-intelligence-released/

Centro de Documentación Europea de Almería. (22 de mayo de 2023). *Cumbre del G7 en Hiroshima del 19 a 21 de mayo.* https://www.cde.ual.es/cumbre-del-g7-en-hiroshima-del-19-a-21-de-mayo/

Centro de Competencia. (16 de marzo de 2022). *La Estrategia Europea de Datos y sus proyectos de ley*. https://centrocompetencia.com/la-estrategia-europea-de-datos-y-sus-proyectos-de-ley/

Centro de Información Oficial [IMPO]. (11 de agosto de 2008). *Normativa y Avisos Legales del Uruguay. Ley de Protección de Datos Personales No18331.* https://www.impo.com.uy/bases/leyes/18331-2008#:~:text=%2D%20Toda%20persona%20f%C3%ADsica%200%20jur%C3%ADdica,de%20la%20que%20es%20titular.

Chirino, A. Manual. (febrero de 2015). *Operativo de protección de datos en El Salvador. EUROsociAL, Programa para la Cohesión Social en América Latina, Documento de Trabajo No 26 Serie: Guías y Manuales Área: Institucionalidad Democrática. Madrid.* https://sia.eurosocial-ii.eu/files/docs/1432887451-DT_26_Chirino.pdf

CMinds, fAIr LAC Jalisco. (junio de 2023). *Programa de fortalecimiento de capacidades para funcionarios públicos en el aprovechamiento de la IA responsable para políticas públicas más efectivas.* https://www.cminds.co/_files/ugd/de03fd_31658b46211f411db7f27902edbb9f8f.pdf

CMinds, fAIr LAC Jalisco. (2023). https://es.cminds.co/fairlac-jalisco

ColombiaInteligente.org. (18 de julio de 2023). *Regulatory sandboxes in artificial intelligence.* https://colombiainteligente.org/tendencias/regulatory-sandboxes-in-artificial-intelligence/

Comisión Económica para América Latina y el Caribe[CEPAL]. (2022). *UN E-Government Survey, Desde el gobierno digital hacia un gobierno inteligente. Reporte de Gobierno Electrónico de las Naciones Unidas.* Adaptado de la ONU. https://biblioguias.cepal.org/gobierno-digital/unegovernment-survey

Comisión Europea, (19 de diciembre de 2023). *Preguntas y respuestas: Ley de Servicios Digitales.* Press Corner. https://ec.europa.eu/commission/presscorner/detail/es/QANDA_20_2348

Comisión Europea. (2023). *La Ley de Ciber Solidaridad de la UE.* https://digital-strategy.ec.europa.eu/es/policies/cyber-solidarity

Comisión Europea. (2023). *Reglamento de Servicios Digitales.* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_es

Comisión Europea. (2023). *Estrategia Europea de Datos.* https://digital-strategy.ec.europa.eu/es/policies/strategy-data

Comisión Europea. (2023). *Estrategia Europea de Datos.* https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-data-strategy_es

Congreso de la República de Colombia. (10 de agosto de 2023). *PL 59-23 (Senado) Lineamientos de política pública para el desarrollo, uso e implementación de Inteligencia Artificial.* http://leyes.senado.gov.co/proyectos/index.php/textos-radicados-senado/p-ley-2023-2024/2964-proyecto-de-ley-059-de-2023

Congressional Research Service. (May 3, 2007). *Data Brokers: Background and Industry Overview.* https://www.everycrsreport.com/reports/RS22137.html

Creemers, R; G., Webster. (22 de agosto de 2021). *Translation: Personal Information Protection Law of the People's Republic of China – Effective. Comité Permanente de la Asamblea Popular Nacional de la República Popular de China. Ley de Protección de Información Personal.* https://digichina.stanford.edu/work/translation-personal-information-protection-law-of-the-peoples-republic-of-china-effective-nov-1-2021/

Creemers, R.; Graham W.; Triolo, P. (29 de junio de 2018). *Ley de Ciberseguridad de la República Popular China. Digi China, Standford University.* https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/

D

DAIL Software. (16 de diciembre de 2019). *Lo más importante en Inteligencia Artificial del 2019.* https://www.dail.es/progresos-inteligencia-artificial-2019/

Darthmouth Conference. (15 de abril de 2014). *Sinopsis Histórica de la IA.* https://darthmouthconference.wordpress.com/

Data Brokers Market. (s.f.)Pronóstico 2022-2031. Panorama del mercado global de corredores de datos. https://www.transparencymarketresearch.com/data-brokers-market.html

DatacenterDynamics.com. (8 de febrero de 2024). *El proyecto de ley para regular la IA en Brasil debe ser votado hasta abril.* https://www.datacenterdynamics.com/es/noticias/el-proyecto-de-ley-para-regular-la-ia-en-brasil-deberia-ser-votado-hasta-abril/

De Rosa, C., M. (20 de mayo de 2024). *GPT-4o: escucha, habla y responde a comandos de voz y más. La Prensa Gráfica.* https://www.laprensagrafica.com/opinion/GPT-4o-escucha-habla-y-responde-a-comandos-de-voz-y-mas-20240519-0025.html

Diario Colatino. (7 de marzo de 2019). *Una niña, un niño, una computadora: un futuro promisorio para El Salvador.* https://www.diariocolatino.com/una-nina-un-nino-una-computadora-un-futuro-promisorio-para-el-salvador/

Diario El Mundo. (24 de octubre de 2023). *La ONU revela el impacto medioambiental oculto del bitcoin. El Salvador, Europa Press.* https://diario.elmundo.sv/economia/la-onu-revela-el-impacto-medioambiental-oculto-del-bitcoin

Diario Oficial de la Unión Europea. (7 de junio de 2019). *Reglamento sobre la Ciberseguridad. DOUE en el Boletín Oficial del Estado, España* https://www.boe.es/buscar/doc.php?id=DOUE-L-2019-80998

E

El País. (26 de diciembre de 2023). Guerra entre Israel y Gaza: resumen del 26/12/2023. https://elpais.com/internacional/2023-12-26/guerra-entre-israel-y-gaza-en-directo.html

EUR-Lex. Decision 2013/275/EU on the signing, on behalf of the EU, of the Beijing Treaty on Audiovisual Performances. (June 10, 2023). https://eur-lex.europa.eu/EN/legal-content/summary/beijing-treaty-on-audiovisual-performances.html#:~:text=The%20treaty%20modernises%20intellectual%20rights,DVD%20or%20other%20audiovisual%20platforms.

European Union (S.F). EUR-Lex, Access to European Union law, Document 32022R1925, Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022, Digital Markets Act (DMA). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32022R1925

Europa Press. (17 de diciembre de 2018). *La tecnología CRISPR, los drones y la IA, entre los avances científicos más importantes de 2018, según Fundación Gadea. Ciencia.* https://www.europapress.es/ciencia/noticiatecnologia-crispr-drones-ia-avances-cientificos-mas-importantes-2018-fundacion-gadea-20181217151811.html#google_vignette

European Commission. (June 16, 2022). 2022 *Strengthened Code of Practice on Disinformation. Policy and Legislation.* https://digitalstrategy.ec.europa.eu/en/library/2022-strengthened-code-practicedisinformation

European Commission. (June 16, 2022). *Disinformation: Commission welcomes the new stronger and more comprehensive Code of Practice on disinformation*. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3664

European Commission (April 21, 2021). *Impact assessment on a Regulatory Framework for Artificial Intelligence.* https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SWD:2021:0085:FIN:EN:PDF

European Commission (February 19, 2020). *A European strategy for data.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066

European Parliament. (December 9, 2023). *Artificial Intelligence Act: dealon comprehensive rules for trustworthy AI.* News. https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligenceact-deal-on-comprehensive-rules-for-trustworthy-ai

European Parliament. (10 de noviembre de 2022). *Fighting cybercrime:new EU cybersecurity laws explained.* Topic https://www.europarl.europa.eu/topics/en/article/20221103STO48002/fighting-cybercrime-new-eucybersecurity-laws-explained

European Parliament. (S.F).Legislative Train Schedule, Commission 2019-24. *Horizontal cybersecurity requirements for products with digital elements.* https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-european-cyber-resilience-act?sid=7101

European Parliament and of the Council. (19 October 2022). *Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), Regulation 2022/2065 of the Europe-an Parliament and of the Council.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014

Expansión.mx. (5 de octubre de 2021). *China presenta una guía ética para regular la Inteligencia Artificial.* Tecnología https://expansion.mx/tecnologia/2021/10/05/china-presenta-una-guia-etica-para-regular-la-inteligencia-artificial

F

Fernández, A. (9 de octubre de 2023). *Por qué es importante regular la inteligencia artificial: 5 claves para entender cómo te van a afectar las normas de Europa. 20minutos.es, Tecnología.* https://www.20minutos.es/tecnologia/inteligencia-artificial/5-claves-regulacion-inteligencia-artificial-europa-5177374/

Fernández de Lis, P. (20 de febrero 2024). B*rad Smith, presidente de Microsoft: Debemos tener una manera de ralentizar o apagar la inteligencia artificial. El País, Tecnología.* https://elpais.com/tecnologia/2024-02-20/brad-smith-presidente-de-microsoft-debemos-tener-una-manera-de-ralentizar-o-apagar-la-inteligencia-artificial.html

Forbes, Staff (EFE). (29 de septiembre de 2021). *China publica directrices para regular los algoritmos de las tecnológicas.* https://forbescentroamerica.com/2021/09/29/china-publica-directrices-para-regular-los-algoritmos-de-las-tecnologicas

France24.com. (1º de noviembre de 2023). *Comienza en Reino Unido la primera cumbre mundial sobre los riesgos de la IA.* https://www.france24.com/es/minuto-a-minuto/20231101-reino-unido-celebra-la-primera-cumbre-mundial-sobre-los-riesgos-de-la-ia

G

García, J. G. (1º de julio de 2023). *'Brokers' de datos: Facebook y Google no son los únicos que te conocen. El País* https://elpais.com/retina/2019/01/07/tendencias/1546871859_023579.html

Gates, B. (December 29, 2023). *The road ahead reaches a turning point in 2024. GatesNotes, The Blog of Bill Gates*, https://www.gatesnotes.com/The-Year-Ahead-2024

Georgieva, K. (16 de enero de 2024). *La economía mundial transformada por la inteligencia artificial ha de beneficiar a la humanidad. Fondo Monetario Internacional*. https://www.imf.org/es/Blogs/Articles/2024/01/14/ai-will-transform-the-global-economy-lets-make-sure-it-benefits-humanity

Gestión. (28 de diciembre de 2016). *Los principales productos deinteligencia artificial del 2016. Tecnología.* https://archivo.gestion.pe/tecnologia/principales-productos-inteligencia-artificial-2016-2178285

Gigena, G. F. (2024). *Radiografía Normativa: ¿Dónde, qué y cómo se está regulando la Inteligencia Artificial en América Latina? Access Now (accesnow.org)*. https://www.accessnow.org/wp-content/uploads/2024/02/LAC-Reporte-regional-de-politicas-de-regulacion-a-la-IA.pdf

Gobierno de Argentina. (junio de 2023). *Propuesta de Ley de Protección de Datos. Agencia de Acceso a la Información Pública.* https://www.argentina.gob.ar/sites/default/files/mensajeyproyecto_leypdp2023.pdf

Gobierno de Argentina. (junio de 2023). *¿Qué es la huella digital en internet? Ministerio de Justicia.* https://www.argentina.gob.ar/justicia/convosenlaweb/situaciones/que-es-la-huella-digital-en-internet#:~:text=La%20huella%20digital%20es%20el,tu%20computadora%2C%20dej%C3%A1s%20informaci%C3%B3n%20personal

Gobierno de Argentina. (junio de 2008). *Reformas al Código Penal (Ley 26388).* https://www.argentina.gob.ar/normativa/nacional/ley-26388-141790/texto

Gobierno de Brasil, Autoridad Nacional de Protección de Datos. (6 de julio de 2023). *Análisis Preliminar sobre el PL 2338/2023 (ANPD publica análise preliminar do Projeto de Lei nº 2338/2023, sobre o uso da Inteligência Artificial).* https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-publica-analise-preliminar-do-projeto-de-lei-no-2338-2023-que-dispoe-sobre-o-uso-da-inteligencia-artificial

Gobierno de Brasil. (5 de febrero de 2020). *Estrategia Nacional de Ciberseguridad –E-Ciber– (Estratégia Nacional de Segurança Cibernética).* https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm#:~:text=DECRETO%20N%C2%BA%2010.222%2C%20DE%205,que%20lhe%20confere%200%20art.

Gobierno de Brasil. (14 de agosto de 2018). *Ley General de Protección de Datos (Lei Geral de Proteção de Dados Pessoais).* https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

Gobierno de Chile, Ministerio de Ciencia, Tecnología e Innovación. (octubre 2023). *Declaración de Santiago, Para promover una inteligencia artificial ética en América Latina y el Caribe.* https://minciencia.gob.cl/uploads/filer_public/40/2a/402a35a0-1222-4dab-b090-5c81bbf34237/declaracion_de_santiago.pdf

Gobierno de Chile, Centro Nacional de IA de Chile. (11 de agosto de 2023). *Índice Latinoamericano de Inteligencia Artificial 2023* (ILIA 2023), https://indicelatam.cl/

Gobierno de Chile, Ministerio de Ciencia, Tecnología, Conocimiento e Innovación. (s.f).Política Nacional de IA 2021. https://www.minciencia.gob.cl/areas/inteligencia-artificial/politica-nacional-de-inteligencia-artificial/

Gobierno de la República Popular China. (20 de agosto de 2021). *Ley de Protección de Datos Personales o Ley de Seguridad de Datos.* https://www.audit.gov.cn/n6/n36/n10084378/c10241260/part/10241606.pdf

Gobierno de Colombia. (agosto de 2023). *PL 91/23, Uso responsable de las Inteligencias Artificiales en Colombia.* https://leyes.senado.gov.co/proyectos/images/documentos/Textos%20Radicados/proyectos%20de%20ley/2023%20-%202024/PL%20091-23%20Inteligencia%20Artificial.pdf

Gobierno de Colombia, Ministerio de Tecnologías de la Información y las Comunicaciones. (marzo de 2022). *Decreto de Seguridad Digital, 338 de 2022.* https://gobiernodigital.mintic.gov.co/692/articles-238198_recurso_1.pdf

Gobierno de Colombia, Consejo Nacional de Política Económica y Social [CONPES]. *(8 de noviembre de 2019). Política Nacional para la Transformación Digital e Inteligencia Artificial.* https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf

Gobierno de Colombia, Sistema Único de Información Normativa [SUIN]. (17 de octubre de 2012). *Disposiciones generales para la protección de datos personales*. https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Leyes/1684507

Gobierno de Ecuador, Asamblea Nacional. (23 de febrero de 2023). *Análisis del Proyecto de Ley de Seguridad Digital es una de las Prioridades de la Comisión Especializada.* https://www.asambleanacional.gob.ec/es/noticia/87874-el-analisis-del-proyecto-de-ley-de-seguridad-digital-es

Gobierno de Ecuador, Asamblea Nacional. (26 de mayo de 2021). *Ley Orgánica de Protección de Datos Personales.* https://www.telecomunicaciones.gob.ec/wp-content/uploads/2021/06/Ley-Organica-de-Datos-Personales.pdf

Gobierno de El Salvador, Presidencia de la República. (7 de mayo de 2021). *Veto del Decreto Legislativo No 875 la Ley de Protección de Datos Personales.* https://www.asamblea.gob.sv/sites/default/files/documents/correspondencia/EFBA7BEE-871B-40BE-BD0A-5BD80237CA90.pdf

Gobierno de El Salvador, Presidencia de la República. (4 de febrero de 2021). *Gobierno de El Salvador entrega computadoras a estudiantes en 2021.* https://www.presidencia.gob.sv/las-computadoras-que-entrega-el-gobierno-a-los-estudiantes-son-de-calidad-con-acceso-a-internet-y-gratuitas/

Gobierno de El Salvador, Presidencia de la República. (2010). *Dirección de innovación tecnológica e informática de la Presidencia de la República.* https://www.transparencia.gob.sv

Gobierno de El Salvador, Secretaría de Innovación de la Presidencia de la República. (enero de 2020). *Agenda Digital El Salvador 2020-2030*. https://www.innovacion.gob.sv/downloads/Agenda%20Digital.pdf

Gobierno de El Salvador, Consejo de Ministros. (Acta de Sesión No 50, del 8de noviembre de 2018). *Conocimiento y Aprobación del Decreto Ejecutivo que contiene la Derogatoria de la Comisión Nacional para la Sociedad de la Información.* https://www.transparencia.gob.sv

Gobierno de El Salvador. (mayo de 2018). *Política Nacional de Innovación, Ciencia y Tecnología.* Secretaría Técnica de la Presidencia, Ministerio de Economía y Ministerio de Educación, (UNCTAD). https://unctad.org/system/files/non-official-document/Politica%20ICT%20version%20digital.pdf

Gobierno de El Salvador. (mayo de 2017). Política Nacional de Datos Abiertos, Guía de implementación. Secretaría de Participación Ciudadana, Transparencia y Anticorrupción de la Presidencia, en Organización de Estados Americanos. http://portal.oas.org/LinkClick.aspx?fileticket=odyIptz9PgE%3D&tabid=1814

Gobierno de El Salvador. (febrero de 2016). Ley Especial Contra los Delitos Informáticos y Conexos. Jurisprudencia. https://www.jurisprudencia.gob.sv/DocumentosBoveda/D/2/2010-2019/2016/02/B6B74.PDF

Gobierno de México. (14 de febrero de 2024). Iniciativa con Proyecto de Decreto por el que se expide la Ley Federal de Ciberseguridad. Senado. https:/infosen.senado.gob.mx/sgsp/gaceta/65/3/2024-02-14-1/assets/documentos/Inic_Morena_diversos_senadores_art_211_CPF.pdf

Gobierno de México. (22 de marzo de 2018). *Estrategia de Inteligencia Artificial de México 2018.* https://www.gob.mx/epn/articulos/estrategia-de-inteligencia-artificial-mx-2018

Gobierno de México. (5 de julio de 2010). *Ley Federal de Protección de Datos Personales en Posesión de los Particulares.* https://www.diputados.gob.mx/LeyesBiblio/pdf/LFPDPPP.pdf

Gobierno de Panamá, Autoridad Nacional para la Innovación Gubernamental [AIG]. (7 de marzo de 2022). *Estrategia Nacional de Ciberseguridad para el período 2021-2024.* https://cert.pa/?p=3011

Gobierno de Panamá. (29 de marzo de 2019). *Ley No 81 sobre Protección de Datos Personales del 26 de marzo de 2019. Gaceta Oficial.* https://www.gacetaoficial.gob.pa/pdfTemp/28743_A/GacetaNo_28743a_20190329.pdf

Gobierno de Paraguay. (28 de abril de 2020). *Ley No 6534 de Protección de Datos Personales Crediticios. Biblioteca y Archivo del Congreso Nacional (BACN).* https://www.bacn.gov.py/archivos/9417/LEY%25206534.pdf

Gobierno de Paraguay. (27 de julio de 2017). *Ley No 5994 que aprueba la Convención sobre Ciberdelincuencia y el Protocolo Adicional al Convenio sobres Ciberdelincuencia Relativo a la Penalización de Actos de Índole Racista y Xenófoba cometidos por medio de Sistemas Informáticos. Biblioteca y Archivo del Congreso Nacional (BACN).* https://www.bacn.gov.py/archivos/9900/Ley+5994.pdf

Gobierno de Paraguay. (abril de 2017). Plan Nacional de Ciberseguridad. *Secretaría Nacional de Tecnologías de la Información y Telecomunicaciones.* https://gestordocumental.mitic.gov.py/share/s/zkKW1CkKScSvapqlB7UhNg

Gobierno de Paraguay. (8 de septiembre de 2011). *Ley No 4439 que Modifica y Amplía varios Artículos de la Ley No 1160/97 Código Penal. Biblioteca y Archivo del Congreso Nacional (BACN).* https://www.bacn.gov.py/archivos/3777/20150817113434.pdf

Gobierno de Perú. (s.f).*Estrategia Nacional de Inteligencia Artificial (ENIA).* https://guias.servicios.gob.pe/creacion-servicios-digitales/inteligencia-artificial/enia

Gobierno de Perú. (s.f). *Ley que promueve el uso de inteligencia artificial en favor del desarrollo económico y social del país.* https://cdn.www.gob.pe/uploads/document/file/5038703/ley-que-promueve-el-uso-de-la-inteligencia-artificial-en-fav-ley-n-31814.pdf?v=1692895308

Gobierno de Perú. (26 de agosto de 2019). *Ley de Ciber defensa.* https://cdn.www.gob.pe/uploads/document/file/1671813/Ley%20N%C2%B030999%2C%20Ley%20de%20Ciberdefensa.pdf

Gobierno de Perú. (21 de junio de 2011). *Ley de Protección de Datos Personales.* https://cdn.www.gob.pe/uploads/document/file/272360/Ley%20N%C2%BA%2029733.pdf.pdf

Gobierno de Uruguay. (21 de noviembre de 2023). *Uruguay adhiere a declaración regulatoria a nivel global sobre Inteligencia Artificial. Agencia de Gobierno Electrónico y Sociedad de la Información y el Conocimiento.* https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/noticias/uruguay-adhiere-declaracion-regulatoria-nivel-global-sobre-inteligencia

Gobierno de Uruguay. (23 de abril de 2021). *Estrategia de Inteligencia Artificial. Agencia de Gobierno Electrónico y Sociedad de la Información y del Conocimiento.* https://www.gub.uy/agencia-gobierno-electronico-sociedad-informacion-conocimiento/comunicacion/publicaciones/estrategia-inteligencia-artificial

Gopinath, G. (6 de junio de 2023). *El poder y los peligros de la mano artificial: La inteligencia artificial a la luz de las ideas de Adam Smith. Fondo Monetario Internacional, Discursos*

https://www.imf.org/es/News/Articles/2023/06/05/sp060523-fdmd-ai-adamsmith

Gopinath, G. (diciembre de 2023). *Harnessing AI for Global Good. Fondo Monetario Internacional* https://www.imf.org/en/Publications/fandd/issues/2023/12/ST-harnessing-AI-for-global-good-Gita-Gopinath

Government of China, Office of the Central Cyberspace Affairs Commission, [CAC.] (11 de abril de 2023). Aviso de la Administración del Ciberespacio de China sobre la solicitud pública de opiniones sobre las Medidas para la Administración de Servicios de Inteligencia Artificial Generativa (Borrador para Comentarios), 生成式人工智能服务管理办法(征求意见稿). https://www.cac.gov.cn/2023 04/11/c_1682854275475410.htm

Government of China, China Academy of Information and Communication *Technology [CAICT] and JD Explore Academy. (July 2021). Trustworthy AI White Paper (Libro blanco sobre IA confiable).* http://www.caict.ac.cn/english/research/whitepapers/202110/P020211014399666967457.pdf

H

Harari, Y.N. (2024). *Nexus. Una breve historia de las redes de información desde la Edad de Piedra hasta la IA.* 1ª. Edición, Penguin Ramdom House.

Hajric, V.; Greifeld, K. (10 de enero de 2024). *La SEC aprueba ETF de bitcoin en un hito para los activos digitales. Bloomberg Línea.* https://www.bloomberglinea.com/2024/01/10/sec-aprueba-los-etf-de-bitcoin-spot-en-milestone-para-activos-digitales/

Hernández, L. (19 de marzo de 2021). *Ley de datos personales: sin pausa, pero sin prisa y de cara a la sociedad. Derechos digitales.* https://www.derechosdigitales.org/15341/ley-de-datos-personales-sin-pausa-pero-sin-prisa-y-de-cara-a-la-sociedad/

Home Security Heroes. (2023). *State of Deepfakes: Realities, Threats, and Impact.* https://www.homesecurityheroes.com/state-of-deepfakes/#deepfake-porn-survey

House of Commons, Culture, Media and Sport Committee. *(11 January 2024). Connected tech: AI and creative technology: Government Response to the Committee's Eleventh Report of Ses-sion 2022–23.* https://committees.parliament.uk/publications/42766/documents/212749/default/

I

IABcolombia.com. (2023). *Novedades regulatorias en materia digital.* https://www.iabcolombia.com/novedades-regulatorias-en-materia-digital/

Índice Latinoamericano de Inteligencia Artificial. (2024). Informe Índice Latinoamericano de Inteligencia Artificial. https://indicelatam.cl/

IdeasLabs.org. (28 de febrero de 2022). *Sandbox de Innovación para apoyar el crecimiento económico de Costa Rica.* https://ideaslabs.org/blog/regulabs/sandbox-de-innovacion-para-apoyar-el-crecimiento-economico-de-costa-rica/2022/02/

Ley de Protección de Datos Personales. (18 de agosto de 2008). Ley No 18331 promulgada el 11 de agosto de 2008. *Dirección Nacional de Impresiones y Publicaciones Oficiales (IMPO).* https://www.impo.com.uy/bases/leyes/18331-2008#:~:text=-%20Toda%20persona%20f%C3%ADsica%20o%20jur%C3%ADdica,de%20la%20que%20es%20titular

J

Jabbour, G. (16 de junio de 2023). *Mareas normativas: así es como se está regulando la Inteligencia Artificial. Expansión.mx, Tecnología.* https://expansion.mx/tecnologia/2023/06/16/regulacion-inteligencia-artificial-en-el-mundo

Jiménez, M. (16 de febrero de 2024). *Open AI lanza Sora, una revolucionaria herramienta de vídeo con inteligencia artificial. El País, Tecnología, Washington.* https://elpais.com/tecnologia/2024-02-16/open-ai-lanza-sora-una-revolucionaria-herramienta-de-video-con-inteligencia-artificial.html

Joma, S., Vides, C. (19 de septiembre de 2020). *Educación necesita $240 millones para cumplir promesa de entregar computadoras a estudiantes. Elsalvador.com.* https://historico.elsalvador.com/historico/755439/educacion-millones-promesa-computadoras-pandemia.html

K

Korinek, A. (diciembre de 2023). Scenario Planning for an A(G)I future. IMF. https://www.imf.org/en/Publications/fandd/issues/2023/12/Scenario-Planning-for-an-AGI-future-Anton-korinek

L

La Prensa Gráfica. (22 de octubre de 2014). https://www.laprensagrafica.com/elsalvador/DICOM-debe--vaciar--bases-de-datos-crediticios-20141022-0074.html

Legal Corp, Abogados. (2011). Amparo 934-2007. https://legalcorp.com.sv/index.php?option=com_content&view=article&id=26:el-derecho-a-la-proteccion-de-datos-personales&catid=2:actualidad&Itemid=3

Limón, R. (8 de febrero de 2024). *Google sustituye a Bard por Gemini e incorpora la nueva aplicación de inteligencia artificial a los móviles. El País, Tecnología.* https://elpais.com/tecnologia/2024-02-08/google-sustituye-a-bard-por-gemini-e-incorpora-la-nueva-aplicacion-de-inteligencia-artificial-a-los-moviles.html

Limón, R. (10 de noviembre de 2023). *Entramos en una era que conduce a algo increíble y profundo nunca visto: la IA toma la mayor feria tecnológica. El País, Tecnología.* https://elpais.com/tecnologia/2023-11-10/entramos-en-una-era-que-conduce-a-algo-increible-y-profundo-nunca-visto-la-ia-toma-la-mayor-feria-tecnologica.html

Limón, R. (29 de junio de 2023). *Armas autónomas y nucleares, robots e inteligencia artificial: cómo regular tecnologías de consecuencias imprevisibles para la humanidad. El País, Tecnología.* https://elpais.com/tecnologia/2023-06-30/armas-autonomas-y-nucleares-robots-e-inteligencia-artificial-como-regular-tecnologias-de-consecuencias-imprevisibles-para-la-humanidad.html#?rel=mas_sumario

López, J., C. (17 de noviembre de 2023). *China va a ser imbatible en inteligencia artificial. No lo dice cualquiera, lo defiende el director general de Google.* Xataka.com. https://www.xataka.com/robotica-e-ia/china-va-a-ser-imbatible-inteligencia-artificial-no-dice-defiende-director-general-google

López, J., M. (12 de abril de 2022). *2022 ha sido el año de la inteligencia artificial: un repaso a todos sus hitos. Blogthinkbig.com, Inteligencia Artificial.* https://blogthinkbig.com/aplicaciones-inteligencia-artificial-2022

M

Marca. (4 de agosto de 2023). *Bill Gates y su nueva predicción que matará a miles o millones de personas.* https://www.marca.com/tiramillas/actualidad/2023/08/04/64ccc1aeca4741472d8b45b8.html

Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones. (febrero de 2023). MICITT inicia formulación de estrategia de Inteligencia Artificial. https://www.micitt.go.cr/el-sector-informa/micitt-inicia-formulacion-de-estrategia-de-inteligencia-artificial

M. J. (20 de diciembre de 2023). *La inteligencia artificial no puede patentar invenciones, según la Corte Suprema del Reino Unido. Cinco Días.* El País, Compañías, Madrid https://cincodias.elpais.com/companias/2023-12-20/la-inteligencia-artificial-no-puede-patentar-invenciones-segun-el-tribunal-supremo-del-reino-unido.html

Elon Musk predice que el 2024 será un año "aún más loco". (s.f). https://www.instagram.com/notibomba/p/C1pii3gLrbG/

N

National Geographic. (2 de diciembre de 2020). Breve historia visual de la inteligencia artificial. https://www.nationalgeographic.com.es/ciencia/breve-historia-visual-inteligencia-artificial_14419

O

OECD Library.(s.f). *Aspectos relevantes de las estrategias nacionales sobre IA en ALC.* https://www.oecd-ilibrary.org/sites/63e9e0bf-es/index.html?itemId=/content/component/63e9e0bf-es

OECD Library. (14 de septiembre de 2022). *Uso estratégico y responsable de la inteligencia artificial en el sector público de América Latina y el Caribe.* https://www.oecd-ilibrary.org/sites/1f334543-en/index.html?itemId=/content/publication/1f334543-en

Organización de las Naciones Unidas [ONU]. (21 de marzo de 2024). *La Asamblea General adopta una resolución histórica sobre la IA. Noticias.* https://news.un.org/es/story/2024/03/1528511

Organización Mundial de la Propiedad Intelectual. (25 de septiembre de 2005). *Reglamento sobre la Administración de los Servicios de Información de Noticias en Internet. WIPO Lex.* https://www.wipo.int/wipolex/es/text/337955

P

Organización Pardo, D. (19 de julio de 2019). *Las 11 predicciones de futuro de Ray Kurzweil. Pandorafms.com, Cultura geek, Tecnología.* https://pandorafms.com/blog/es/predicciones-ray-kurzweil/

Parlamento Europeo. (19 de junio de 2024). *Ley de IA de la UE: primera normativa sobre inteligencia artificial.* https://www.europarl.europa.eu/pdfs/news/expert/2023/6/story/20230601STO93804/20230601STO93804_es.pdf

Parlamento Europeo. (14 de junio de 2023). *Ley de IA de la UE: primera normativa sobre inteligencia artificial.* https://www.europarl.europa.eu/topics/es/article/20230601STO93804/ley-de-ia-de-la-ue-primera-normativa-sobre-inteligencia-artificial

Parlamento Europeo. (20 de abril de 2023). *Luz verde del Parlamento a la primera regulación europea sobre criptoactivos.* https://www.europarl.europa.eu/news/es/press-room/20230414IPR80133/luz-verde-del-parlamento-a-la-primera-regulacion-europea-sobre-criptoactivos

Parlamento Europeo. (18 de enero de 2023). *Videojuegos: el PE reclama protección para los jugadores e impulsar el sector.* https://www.europarl.europa.eu/news/es/press-room/20230113IPR66646/videojuegos-el-pe-reclama-proteccion-para-los-jugadores-e-impulsar-el-sector

Parlamento Europeo. (17 de enero de 2023). *Cinco formas con las que el Parlamento Europeo quiere proteger a los jugadores en línea.* https://www.europarl.europa.eu/news/es/headlines/society/20230112STO66402/como-quiere-el-parlamento-europeo-proteger-a-los-jugadores-en-linea

Parlamento Europeo. (27 de abril de 2022). I*nteligencia artificial: la hoja de ruta del Parlamento para la UE.* https://www.europarl.europa.eu/news/es/headlines/society/20220422STO27705/inteligencia-artificial-la-hoja-de-ruta-del-parlamento-para-la-ue

Parlamento Europeo. (6 de abril de 2022). *Data governance: Parliament approves new rules boosting intra-EU data sharing.* https://www.europarl.europa.eu/news/es/press-room/20220401IPR26534/data-governance-parliament-approves-new-rules-boosting-intra-eu-data-sharing

Parlamento Europeo. (6 de abril de 2022). *Promoción de la disponibilidad de datos: ¿cuáles son los beneficios?* https://www.europarl.europa.eu/news/es/headlines/society/20220331STO26411/promocion-de-la-disponibilidad-de-datos-cuales-son-los-beneficios

Parlamento Europeo. (1º de abril de 2022). Peligros de las criptomonedas y beneficios de la nueva legislación de la UE. https://www.europarl.europa.eu/news/es/headlines/economy/20220324STO26154/peligros-de-las-criptomonedas-y-beneficios-de-la-nueva-legislacion-de-la-ue

Parlamento Europeo. (19 de mayo de 2021). *MEPs call for an ethical framework to ensure artificial intelligence respects EU values.* https://www.europarl.europa.eu/news/es/press-room/20210517IPR04135/meps-call-for-an-ethical-framework-to-ensure-ai-respects-eu-values

Parlamento Europeo. (26 de marzo de 2021). *¿Qué es la inteligencia artificial y cómo se usa?* https://www.europarl.europa.eu/topics/es/article/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa

Parra, S. (31 de octubre de 2023). *El presidente de Estados Unidos ha firmado una orden ejecutiva para regular el desarrollo de la inteligencia artificial.* National Geographic, España, Ciencia. https://www.nationalgeographic.com.es/ciencia/presidente-estados-unidos-ha-firmado-orden-ejecutiva-para-controlar-desarrollo-inteligencia-artificial_20965

Pieczynski, F. (24 de diciembre de 2017). *2017: el despertar de la inteligencia artificial. Expansión, Economía Digital.* https://www.expansion.com/economia-digital/protagonistas/2017/12/24/5a381a94268e3eda478b45e7.html

Ponjoan, N. (7 de noviembre de 2023). José Luis Hernández, informático: *Es muy fácil engañar a la inteligencia artificial para que genere un ataque. El País, Tecnología.* https://elpais.com/tecnologia/2023-11-08/jose-luis-hernandez-informatico-es-muy-facil-enganar-a-la-inteligencia-artificial-para-que-genere-un-ataque.html

Prego, C. (9 de diciembre de 2023). *La UE pacta la primera ley sobre inteligencia artificial del mundo: usos prohibidos, multas y otras claves de la norma.* Xataka.com. https://www.xataka.com/legislacion-y-derechos/abre-camino-a-innovacion-ia-fiable-ue-pacta-primera-ley-mundo-inteligencia-artificial

Markovski, V. ; Trepykhalin A. (31 enero 2022). *Informe de enfoque por países: leyes e iniciativas de políticas relacionadas con Internet en China. ICANN.* https://itp.cdn.icann.org/es/files/government-engagement-ge/ge-010-31jan22-en.pdf

Meaker, M.; Johnson, K. (May 8, 2023). *The Global Battle to Regulate AI Is Just Beginning. Wired.com, UK.* https://www.wired.co.uk/article/the-global-battle-to-regulate-ai-is-just-beginning

Michele, R.; Adam J. (December 13, 2023). Why Digital Trade Should Remain Open. https://www.imf.org/en/Blogs/Articles/2023/12/13/why-digital-trade-should-remain-open?utm_medium=email&utm_source=govdelivery

Organización de Estados Americanos [OEA]. (junio de 2011). *Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales, No 8968.* https://www.oas.org/es/sla/ddi/docs/CR4%20Ley%20de%20Protecci%C3%B3n%20de%20la%20Persona%20frente%20al%20Tratamiento%20de%20sus%20Datos%20Personales.pdf

Parlamento Europeo. (9 de noviembre de 2023). *El Parlamento respalda el plan para facilitar el acceso a los datos y su uso.* https://www.europarl.europa.eu/news/es/press-room/20231106IPR09025/el-parlamento-respalda-el-plan-para-facilitar-el-acceso-a-los-datos-y-su-uso

Parlamento Europeo. (26 de marzo de 2021). *¿Qué es la inteligencia artificial y cómo se usa?* https://www.europarl.europa.eu/news/es/headlines/society/20200827STO85804/que-es-la-inteligencia-artificial-y-como-se-usa

Peralta, L., A. (28 de febrero de 2024). *Pantallas en la palma de la mano y 'tamagotchis': la carrera por imaginar los dispositivos más allá del móvil.* El País, Tendencias, Madrid. https://elpais.com/proyecto-tendencias/2024-02-28/pantallas-en-la-palma-de-la-mano-y-tamagotchis-la-carrera-por-imaginar-los-dispositivos-mas-alla-del-movil.html

R

ReasonWhy. (21 de septiembre de 2023). *Reino Unido establece siete principios rectores de la IA para garantizar la competencia sana y la protección de los usuarios.* https://www.reasonwhy.es/actualidad/reino-unido-principios-rectores-inteligencia-artificial-competencia-consumidor

Reddington, I. (14 January 2021). *Intellectual property after 1 January 2021. Field Seymour Parkes Law.* https://www.fsp-law.com/intellectual-property-after-1-january-2021/

Resiliente Digital. (2023). *Quién es Ray Kurzweil y qué predicciones tecnológicas hace para el futuro* https://resilientedigital.com/quien-es-ray-kurzweil-y-que-predicciones-tecnologicas-hace-para-el-futuro/

Romero, S. (21 de julio de 2023). *¿Cuándo nació la inteligencia artificial?* Muy interesante. es, Tecnología. https://www.muyinteresante.es/tecnologia/60947.html

Romero, S. (4 de abril de 2023). *Los humanos podrían alcanzar la 'inmortalidad' en menos de 10 años.* Muy Interesante. https://www.muyinteresante.es/actualidad/60056.html#:~:text=Kurzweil%20afirma%20que%20cuando%20la,algo%20que%20alcanzar%C3%ADamos%20en%202030.

Roose, K. (10 de diciembre de 2023). *This A.I. Subculture's Motto: Go, Go, Go. The New York Times.* https://www.nytimes.com/2023/12/10/technology/ai-acceleration.html

Rubio, I. (20 de enero 2024). *El 'hermano' maligno de ChatGPT y otras amenazas de la inteligencia artificial generativa.* El País, Tecnología. https://elpais.com/tecnologia/2024-01-20/el-hermano-maligno-de-chatgpt-y-otras-amenazas-de-la-inteligencia-artificial-generativa.html

S

Sahuquillo, M., R.; Ayuso, S. (4 de diciembre de 2023). *La UE se inclina por la autorregulación en la nueva ley de inteligencia artificial.* https://elpais.com/tecnologia/2023-12-05/bruselas-se-inclina-por-la-autorregulacion-en-la-nueva-ley-de-inteligencia-artificial.html?event_log=oklogin

Sandoval V., R. (19 de marzo de 2024). *Innovación y Regulación: El Futuro de la IA en México a través del Sandbox Regulatorio.* https://es.linkedin.com/pulse/innovaci%C3%B3n-y-regulaci%C3%B3n-el-futuro-de-la-ia-en-m%C3%A9xico-rodrigo-2tckc

Santander Universidades. (23 de noviembre de 2021). *Test de Turing: ¿pueden las computadoras sustituir a los humanos?* https://www.santanderopenacademy.com/es/blog/test-de-turing.html

Seisdedos, I. (30 de octubre de 2023). *Biden recurre a una ley de tiempos de guerra para regular la inteligencia artificial: La tecnología debe ser gobernada.* El País, Tecnología, Washington. https://elpais.com/tecnologia/2023-10-30/biden-recurre-a-una-ley-de-tiempos-de-guerra-para-regular-la-inteligencia-artificial-la-tecnologia-debe-ser-gobernada.html?event_log=oklogin

Seminario, F. (29 de marzo de 2021). *Sandbox regulatorio en LatAm: Los entornos de pruebas fintech toman forma.* Asociación de empresas Fintech de Chile, FinteChile. https://www.fintechile.org/noticias/sandbox-regulatorio-en-latam-los-entornos-de-pruebas-fintech-toman-forma

Sobrino, A; y Barro, S. (1993). *Estudios de lógica borrosa y sus aplicaciones.* Universidad de Santiago de Compostela. https://minerva.usc.es/xmlui/bitstream/handle/10347/8748/78%20Estudios%20de%20l%c3%b3gica%20borrosa%20y%20sus%20aplicaciones.pdf?sequence=1&isAllowed=y

T

The White House, Beefing Room. (October 30, 2023). *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence.* https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

Torres, R.; Said, C; Buenadicha S., C; y Tetsuro, N. (mayo de 2021). *Autoevaluación ética de IA para actores del ecosistema emprendedor: Guía de aplicación.* Banco Interamericano de Desarrollo, Publicaciones. https://publications.iadb.org/es/autoevaluacion-etica-de-ia-para-actores-del-ecosistema-emprendedor-guia-de-aplicacion

Treviño, R. (23 de diciembre de 2019). *Las tecnologías que predominaron este 2019. Conecta, Tecnológico de Monterrey.* https://conecta.tec.mx/es/noticias/nacional/educacion/las-tecnologias-que-predominaron-este-2019#:~:text=Inteligencia%20Artificial%2C%20asistentes%20virtuales%2C%20innovaciones,m%C3%A1s%20relevantes%20de%20este%20%C3%A1mbito

U

Unión Europea. (9 de noviembre de 2023). Ley de Datos. Parlamento Europeo https://www.europarl.europa.eu/doceo/document/TA-9-2023-0385_ES.html

Unión Europea. (20 de abril de 2023). Ley del mercado de criptoactivos, MICA. eur-lex.europa.eu. https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:52020PC0593

Unión Europea. (15 de septiembre de 2022). Ley de ciberresiliencia de la Unión Europea, CRA. https://digital-strategy.ec.europa.eu/es/policies/cyber-resilience-act

Unión Europea. (14 de diciembre de 2022). *Ley de Resiliencia Operacional Digital, DORA.* Seaslpeth.com. https://www.sealpath.com/es/blog/regulacion-dora-guia-cumplimiento/

Unión Europea. (19 de octubre de 2022). Ley de Servicios digitales. https://digital-strategy.ec.europa.eu/es/policies/digital-services-act-package

Unión Europea. (16 de junio de 2022). *Código de buenas prácticas en materia de desinformación de 2022.* https://digital-strategy.ec.europa.eu/es/policies/code-practice-disinformation

Unión Europea. (6 de abril, 2022). Ley Europea de Gobernanza de Datos. https://digital-strategy.ec.europa.eu/es/policies/data-governance-act

Unión Europea. (19 de febrero de 2020). *Una estrategia europea de datos.* https://digital-strategy.ec.europa.eu/es/policies/strategy-data

Unión Europea. (2019). Ley de Ciberseguridad de la UE. https://digital-strategy.ec.europa.eu/es/policies/cybersecurity-act

Unión Europea. (2016). *Reglamento General de Protección de Datos (216/679).* https://eur-lex.europa.eu/ES/legal-content/summary/general-data-protection-regulation-gdpr.html

Unión Europea. (19 de octubre de 2022). *Ley de Mercados digitales.* https://eur-lex.europa.eu/legal-content/ES/TXT/HTML/?uri=CELEX:32022R1925

Unión Internacional de Telecomunicaciones [UIT]. (2021). *Índice Mundial de Ciberseguridad 2020.* https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-S.pdf

Unión Internacional de Telecomunicaciones [UIT]. (29 de junio 2021). *Los países refuerzan sus estrategias de ciberseguridad.* https://www.itu.int/es/mediacentre/Pages/pr06-2021-global-cybersecurity-index-fourth-edition.aspx

United Kingdom Government. (29 June 2023). *The government's code of practice on copyright and AI. Intellectual Property Office.* https://www.gov.uk/guidance/the-governments-code-of-practice-on-copyright-and-ai

United Kingdom Government. (1 y 2 de noviembre de 2023). *Declaración de Bletchley de los países que asisten a la Cumbre de seguridad de la IA.* https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/dbc58681-1b68-47e0-8e3f-f91435fdf8ce

United Kingdom Government. (29 March 2023). *A pro-innovation approach to AI regulation.* https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper

United Kingdom Government. (18 December 2022). *National AI Strategy: Our ten-year plan to make Britain a global AI superpower.* https://www.gov.uk/government/publications/national-ai-strategy/national-ai-strategy-html-version

United Kingdom Parliament. (18th July 2022). *Data Protection and Digital Information Bill.* https://publications.parliament.uk/pa/bills/cbill/58-03/0143/220143.pdf

V

Velázquez, J., A. (6 de diciembre de 2023). *Avances tecnológicos que marcaron al 2023: un año dominado por la Inteligencia Artificial.* Reporte Índigo. https://www.reporteindigo.com/piensa/avances-tecnologicos-que-marcaron-al-2023-un-ano-dominado-por-la-inteligencia-artificial/

Vía Libre. (14 de marzo de 2023). *Declaración Montevideo IA: por una IA que refleje la realidad latinoamericana y al servicio de las personas.* https://www.vialibre.org.ar/una-inteligencia-artificial-latinoamericana-y-al-servicio-de-las-personas/

Vicente, S., P. (14 de noviembre de 2023). *UE: La Comisión Europea analiza el impacto económico, social y cultural de los videojuegos en Europa.* Instituto de Derecho de Autor (Instituto Autor). https://www.institutoautor.com/ue-la-comision-europea-analiza-el-impacto-economico-social-y-cultural-de-los-videojuegos-en-europa/

Vidal L., M. (31 de enero de 2024). *Tienen sangre en sus manos: los senadores de EE. UU. arremeten contra las redes sociales por no proteger a los menores.* El País, Tecnología, Washington. https://elpais.com/tecnologia/2024-01-31/tienen-sangre-en-sus-manos-los-senadores-de-ee-uu-arremeten-contra-las-redes-sociales-por-no-proteger-a-los-menores.html

W

Wagstaff, J. (diciembre de 2023). Un nuevo modelo de ejército. Fondo Monetario Internacional, Finanzas y Desarrollo. https://www.imf.org/es/Publications/fandd/issues/2023/12/Case-Studies-New-model-army-Jeremy-Wagstaff

Webb, A. (s.f.). *FTI Annual Letter, 2024 Macro Themes + 2023 Signals Review.* https://mailchi.mp/futuretodayinstitute/2023-annual-letter#themes

Webster, G. (28 February 2022). *Translation: Internet Information Service Algorithmic Recommen-dation Management Provisions.* DigiChina, Stanford University. https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/

World Economic Forum. (10 de enero 2024). Informe de riesgos globales 2024. https://www3.weforum.org/docs/WEF_GRR24_Press%20release_ES.pdf

Y

Yanling, H. (28 de octubre de 2021). *China fortalecerá la gobernanza de los algoritmos.* Observador de Justicia de China. https://es.chinajusticeobserver.com/a/china-to-strengthen-governance-of-algorithms

DESAFÍOS PARA TENER MAYOR SEGURIDAD ANTE LA INTELIGENCIA ARTIFICIAL

Claudio Manuel de Rosa Ferreira es doctor en Economía, investigador económico del Observatorio de Políticas Públicas de la Universidad Francisco Gavidia (OPP-UFG), con amplia experiencia en el diseño de planes de gobierno, de políticas públicas y proyectos socioeconómicos en Centroamérica. Trabajó en el Fondo Monetario Internacional (FMI), Agencia de los Estados Unidos para el Desarrollo Internacional (USAID) El Salvador; además, gobernador de la Federación Latinoamericana de Bancos (FELABAN). Ha sido consultor del Banco Mundial (BM) y del Programa de las Naciones Unidas para el Desarrollo (PNUD). Conferencista y moderador en foros nacionales e internacionales. Docente de posgrado. Economista Distinguido 2021.

OBSERVATORIO DE POLÍTICAS PÚBLICAS
UNIVERSIDAD FRANCISCO GAVIDIA

UFG
UNIVERSIDAD FRANCISCO GAVIDIA
Powered by Arizona State University®

ISBN: 978-99983-906-2-1

ISBN: 978-99983-906-2-1