ACUERDO 5038/SO/03-10/2024

ACUERDO MEDIANTE EL CUAL SE APRUEBA LA INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY PARA EL USO DE INTELIGENCIA ARTIFICIAL Y EL TRATAMIENTO DE DATOS PERSONALES POR SUJETOS OBLIGADOS EN LA CIUDAD DE MÉXICO.

Acordado en Sesión Ordinaria celebrada el **tres de octubre de dos mil veinticuatro,** por **unanimidad de votos**, de los integrantes del Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, conformado por las Comisionadas y los Comisionados Ciudadanos, que firman al calce, con el voto concurrente de la Comisionada Ciudadana María del Carmen Nava Polina, ante Miriam Soto Domínguez, Secretaria Técnica, de conformidad con lo dispuesto en el artículo 15, fracción IX del Reglamento Interior de este Instituto, para todos los efectos legales a que haya lugar.

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
d3a4dc2cef4c2206d170bd6ad682599b

ARÍSTIDES RODRIGO GUERRERO GARCÍA
COMISIONADO PRESIDENTE

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
3e9e21058254ea360560acf6b2545013

JULIO CÉSAR BONILLA GUTIÉRREZ
COMISIONADO CIUDADANO

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
292f98a11437541c27dadc49ac498eee

LAURA LIZETTE ENRÍQUEZ RODRÍGUEZ
COMISIONADA CIUDADANA

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
c3f567df648d10050160ed902052e3d5

MARÍA DEL CARMEN NAVA POLINA
COMISIONADA CIUDADANA

MIRIAM SOTO DOMÍNGUEZ
SECRETARIA TÉCNICA

Firmado con FIRMA CDMX
llave.cdmx.gob.mx
2c9079dc1673b4e650e10478619ce0bb

ACUERDO MEDIANTE EL CUAL SE APRUEBA LA INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY PARA EL USO DE INTELIGENCIA ARTIFICIAL Y EL TRATAMIENTO DE DATOS PERSONALES POR SUJETOS OBLIGADOS EN LA CIUDAD DE MÉXICO.

CONSIDERANDOS

1. Que el artículo 116, fracción VIII, de la Constitución Política de los Estados Unidos Mexicanos (Constitución Federal), prevé que, en las Constituciones de las Entidades Federativas, se establecerá la creación de organismos autónomos, especializados, imparciales y colegiados, responsables de garantizar los derechos de acceso a la información y de protección de datos personales en posesión de los sujetos obligados, conforme a los principios y bases establecidos por el artículo 6°, párrafo segundo de la Constitución Federal.

2. Que de conformidad con lo establecido en los artículos 46, Apartado A, inciso d) y 49 de la Constitución Política de la Ciudad de México (Constitución local); 37, primer párrafo de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México (Ley de Transparencia) y 78 de la Ley de Protección de Datos Personales en Posesión de los Sujetos Obligados de la Ciudad de México (Ley de Datos), el Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (Instituto) es un Órgano Autónomo, de carácter especializado, independiente, imparcial y colegiado, con personalidad jurídica y patrimonio propio, cuenta con plena autonomía técnica, de gestión y financiera, con capacidad para decidir sobre el ejercicio de su presupuesto y determinar su organización interna, funcionamiento y resoluciones; es responsable de garantizar el cumplimiento de la Ley de Transparencia, dirigir y vigilar el ejercicio de los Derechos de Acceso a la Información y la Protección de Datos Personales,

conforme a los principios y bases establecidos por el artículo 6º párrafo segundo y 16 de la Constitución Federal; y demás preceptos aplicables de la Ley General de Transparencia y Acceso a la Información Pública (Ley General de Transparencia) y la propia Ley de Transparencia.

3. Que en el artículo 79, fracciones IV y X de la Ley de Datos se establece que el Instituto, entre otras, tendrá las atribuciones de promover y difundir el ejercicio del derecho a la protección de datos personales, así como, llevar a cabo acciones y actividades que promuevan el conocimiento del aludido derecho, así como de sus prerrogativas.

4. Que de acuerdo con lo establecido en el artículo 62 de la Ley de Transparencia, el Pleno de este Instituto es el órgano superior de dirección que tiene la responsabilidad de vigilar el cumplimiento de las disposiciones constitucionales y legales en materia de transparencia, acceso a la información y protección de datos personales en la Ciudad de México.

5. Que de acuerdo con lo establecido en los artículos 57, párrafo primero; 67, inciso a) de la fracción II; y, 71, fracción XVIII, de la Ley de Transparencia, el Instituto podrá en todo momento presentar iniciativas de leyes o decretos ante el Congreso de la Ciudad de México en las materias de su competencia; en ese sentido, el Pleno del Instituto cuenta con la facultad, en materia regulatoria, de aprobar dichas iniciativas de leyes o decretos, para después presentarlas al Poder Legislativo Local, por conducto de su Comisionado Presidente.

6. Que el veintisiete de febrero de dos mil diecinueve, el Pleno de este órgano garante aprobó su Reglamento Interior mediante acuerdo de clave alfanumérica 0313/SO/27-02/2019; el cual es de observancia general y obligatoria para las unidades administrativas y personal del Instituto, el cual tiene por objeto establecer

normas que regulan el funcionamiento y operación de la estructura orgánica para el correcto ejercicio de sus atribuciones.

7. Que de conformidad con lo señalado en los artículos 9 y 10 del Reglamento Interior del Instituto de Transparencia, Acceso a la Información, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México (Reglamento interior), el Pleno del Instituto funcionará y tomará sus decisiones de manera colegiada ajustándose al principio de igualdad entre sus integrantes, siendo la autoridad frente a las Comisionadas y Comisionados en su conjunto y en lo particular, sus resoluciones son obligatorias para estos, aunque estén ausentes o sean disidentes al momento de tomarlas. Las decisiones y resoluciones se adoptarán por mayoría simple. En caso de empate, el Comisionado Presidente resolverá con voto de calidad en términos de lo señalado por el artículo 63 de la Ley de Transparencia.

8. Que de conformidad con el artículo 14, Fracción XVI, es atribución de las Comisionadas y los Comisionados Ciudadanos proponer previamente a la Comisionada Presidenta o al Comisionado Presidente asuntos para integrarlos en el orden del día, en los términos del Reglamento de Sesiones del Pleno del Instituto, y de conformidad con el artículo 7 Fracción IV, V y VI del Reglamento de Sesiones del Pleno de este Instituto, corresponde a las Comisionadas y Comisionados r emitir previamente a las demás personas integrantes del Pleno, a la Secretaría Técnica, y en su caso a las Unidades Administrativas, los proyectos que serán sometidos a consideración del Pleno, así como Someter a consideración del Pleno cualquier asunto de la competencia del Instituto e instruir a la persona titular de la Secretaría Técnica, la inclusión, retiro o diferimiento de asuntos en el proyecto de orden del día, de conformidad con la Ley de Transparencia, el Reglamento Interior y este Reglamento de Sesiones.

9. Que de conformidad con los numerales 5, 6, 7 y 8 de los Considerandos de este acuerdo, el Comisionado Julio César Bonilla Gutiérrez presenta la **“INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY PARA EL USO DE INTELIGENCIA ARTIFICIAL Y EL TRATAMIENTO DE DATOS PERSONALES POR SUJETOS OBLIGADOS EN LA CIUDAD DE MÉXICO’’** para ser presentada ante el Poder Legislativo de la Ciudad de México, por conducto del Comisionado Presidente del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

Por las consideraciones y fundamentos anteriormente expuestos, el Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México emite el siguiente:

ACUERDO

PRIMERO. Se aprueba la **‘’INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY PARA EL USO DE INTELIGENCIA ARTIFICIAL Y EL TRATAMIENTO DE DATOS PERSONALES POR SUJETOS OBLIGADOS EN LA CIUDAD DE MÉXICO’’,** misma que se integra al presente acuerdo como **ANEXO ÚNICO**, formando parte integral del mismo.

SEGUNDO. Se aprueba la presentación de la **‘’INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY PARA EL USO DE INTELIGENCIA ARTIFICIAL Y EL TRATAMIENTO DE DATOS PERSONALES POR SUJETOS OBLIGADOS EN LA CIUDAD DE MÉXICO’’** ante el Poder Legislativo de la Ciudad de México, por conducto del Comisionado Presidente del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, **Dr. Arístides Rodrigo Guerrero García**.

TERCERO. El presente Acuerdo entrará en vigor el día de su aprobación por el Pleno del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

CUARTO. Se instruye a la Secretaría Técnica para que el presente Acuerdo sea incorporado al portal de Internet del Instituto.

Ciudad de México, 03 de octubre de 2024

VOTO CONCURRENTE AL ACUERDO MEDIANTE EL CUAL SE APRUEBA LA INICIATIVA CON PROYECTO DE DECRETO PARA EXPEDIR LA LEY PARA EL USO DE INTELIGENCIA ARTIFICIAL Y EL TRATAMIENTO DE DATOS PERSONALES POR SUJETOS OBLIGADOS EN LA CIUDAD DE MÉXICO.

Con fundamento en los artículos 63, segundo párrafo; 65, fracción V; 73, fracciones I y II, de la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México; 14, fracción VIII, del Reglamento Interior del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México y el artículo 7, fracción XVI y 42 del Reglamento de sesiones del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, emito el siguiente voto:

Si bien reconozco que este Instituto se sume a la discusión internacional sobre cómo regular el desarrollo y operación de los sistemas de inteligencia artificial para asegurar a las personas el disfrute de sus beneficios, a la vez que se prevean sus riesgos. La propuesta que se pone a nuestra consideración busca salvaguardar la protección de datos personales asociados al desarrollo, entrenamiento y uso de estas tecnologías cuando las empleen los actores públicos institucionales de la Ciudad de México. Y hablo de tecnologías, pues así se las acota y define en el glosario de la iniciativa que se nos propone, siguiendo definiciones internacionales. La preocupación es válida, oportuna y pertinente. Pero quiero considerar, en el curso de mi participación, si corresponde o no a este Instituto e incluso al órgano legislativo de esta entidad federativa resolver las preocupaciones que el proyecto pone a nuestra consideración.

En la **Recomendación sobre la ética de la inteligencia artificial de** la Unesco, se define a la IA, en sentido amplio como *"tecnologías de procesamiento de la información que integran modelos y algoritmos que producen una capacidad para aprender y realizar tareas cognitivas, dando lugar a resultados como predicción y la adopción de decisiones en entornos materiales y virtuales."* Esa recomendación señala que, para estar basado en derechos humanos, el enfoque de IA debe contemplar diez principios básicos, a saber:

1. Proporcionalidad e inocuidad,
2. Seguridad y protección,
3. Derecho a la intimidad y protección de datos,
4. Gobernanza y colaboración adaptativas y de múltiples partes interesadas,
5. Responsabilidad y rendición de cuentas,
6. Transparencia y explicabilidad,
7. Supervisión y decisión humanas,
8. Sostenibilidad,
9. Sensibilización y educación, así como
10. Equidad y no discriminación.

Por ello, una eficaz regulación del desarrollo, entrenamiento y uso de los sistemas de Inteligencia Artificial debe considerar al menos estos diez aspectos mencionados, y requeriría prever su uso tanto por actores del sector público, como, quizá de manera principal, por los actores del sector privado. Algunos de los diez aspectos señalados involucran derechos salvaguardados por este instituto, como lo son el derecho a la protección de datos, la rendición de cuentas, la transparencia. Otros, sin embargo, exceden la competencia y los alcances que tenemos como garante local de los derechos de protección de datos y acceso a la información pública y son probablemente ajenos a la naturaleza de este organismo.

Tras revisar la normativa aplicable a la materia, veo que un organismo garante de la naturaleza del INFO es ajeno a la regulación de este tema más allá de los aspectos previstos por la normativa vigente en materia de protección de datos personales. Y sostengo que es ese marco, tanto en el ámbito nacional como en el local, el que será necesario actualizar. En la actualidad las entidades competentes para proponer y conocer sobre Inteligencia Artificial son instancias federales, puesto que los desarrolladores de estos sistemas pueden incluso ser empresas privadas extranjeras.

La Ley General de Protección de Datos Personales en Posesión de los Sujetos Obligados prevé, en su artículo 30, que "Entre los mecanismos que deberá adoptar el responsable para cumplir con el principio de responsabilidad establecido en la presente Ley están, al menos, los siguientes:

VII. Diseñar, desarrollar e implementar sus políticas públicas, programas, servicios,

sistemas o plataformas informáticas, ***aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, de conformidad con las disposiciones previstas en la presente Ley y las demás que resulten aplicables en la materia****, y*

VIII. Garantizar que sus políticas públicas, programas, servicios, sistemas o plataformas informáticas, ***aplicaciones electrónicas o cualquier otra tecnología que implique el tratamiento de datos personales, cumplan por defecto con las obligaciones previstas en la presente Ley y las demás que resulten aplicables en la materia****."*

Y en su artículo 74, la misma norma dispone "Cuando el responsable pretenda poner en operación o modificar políticas públicas, sistemas o plataformas informáticas, **aplicaciones electrónicas o cualquier otra tecnología que a su juicio y de conformidad con esta Ley impliquen el tratamiento intensivo o relevante de datos personales, deberá realizar una Evaluación de impacto en la protección de datos personales, y presentarla ante el Instituto o los Organismos garantes, según corresponda**, los cuales podrán emitir recomendaciones no vinculantes especializadas en la materia de protección de datos personales.

Por lo anterior, tengo la convicción de que la materia que se busca regular para la protección de datos personales en los sistemas de inteligencia artificial mediante una norma específica, resulta redundante en relación con las disposiciones asociadas a la normativa en materia de protección de datos personales.

Por su parte, la Ley General en Materia de Humanidades, Ciencias, Tecnologías e Innovación, prevé (art. 18) como una responsabilidad de los gobiernos de las entidades federativas la elaboración de "sus respectivos programas en materia de humanidades, ciencias, **tecnologías e innovación contemplando las propuestas que presenten las dependencias y entidades de la administración pública local que fomenten, realicen o apoyen actividades de** [...] **desarrollo tecnológico e innovación**", para lo que considerarán las opiniones que emitan los órganos internos consultivos, las universidades, las instituciones de educación superior, los centros de investigación y la comunidad en general, así como los sectores social y privado, de la entidad federativa correspondiente.

Esa misma disposición contempla que "el diseño e implementación de los programas de las entidades federativas deberán contemplar como punto de partida las necesidades, problemáticas, capacidades y vocaciones de los municipios y de las demarcaciones, según corresponda, de conformidad con la legislación aplicable. Asimismo, los programas de las entidades federativas deberán ser congruentes con los fines, principios y bases de las políticas públicas." Esa misma norma reserva como competencia federal (artículo 22, fracción I) la facultad de integrar, formular, conducir, ejecutar y evaluar la política nacional en materia de humanidades, ciencias, tecnologías e innovación, conforme a los fines, principios y bases de las políticas públicas previstos en dicha Ley.

La legislación en materia de ciencia y tecnología de esta ciudad está pendiente de armonizarse con la norma general vigente, y esa es una buena oportunidad para detallar los aspectos relativos a la regulación de los sistemas de inteligencia artificial en los aspectos señalados por las orientaciones internacionales, ajenos a la protección de datos personales, previstos por la norma especializada en esa materia.

Sin duda, la protección de la privacidad y las garantías del uso legítimo de los datos personales en manos de los actores públicos institucionales y del sector privado debe actualizarse y robustecerse en consideración del acelerado avance de los desarrollos tecnológicos que observamos, a fin de atender con oportunidad y eficacia los desafíos que nos ofrecen.

Sin embargo, creo que para que esta regulación sea eficaz, robusta y apropiada, debe provenir del ámbito nacional, a fin de asegurar un estándar común de protección, clara definición de competencias y responsabilidades, así como claridad en los principios, bases y metodologías que se emplearán para estos fines.

Por ello, en **atención a los principios de certeza, legalidad, eficacia y profesionalismo que la ley local de transparencia pide al Pleno que guíen las actividades de este Instituto, me aparto, respetuosamente, del proyecto que se pone a nuestra consideración**. Reitero, sin embargo, mi felicitación por traer a la discusión un tema que requiere pronto examen por parte de los órganos legislativos competentes de nuestro país.

Confío en que pronto las normas nacionales correspondientes se adecuen para atender las

preocupaciones señaladas por los organismos internacionales y de las que el proyecto de nuestro colega, el Comisionado Bonilla, hace eco. Gracias.

María del Carmen Nava Polina

Comisionada del InfoCDMX

www.infocdmx.org.mx La Morena 865, Col. Narvarte Poniente, Alcaldía Benito Juárez, C.P. 03020, CDMX Tel. +52 (55) 5636-2120


SIN TEXTO

Iniciativa con proyecto de Decreto para Expedir la Ley para el uso de inteligencia artificial y el tratamiento de datos personales por sujetos obligados en la Ciudad de México.

Quienes suscriben, las personas Comisionadas Ciudadanas del Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México, con fundamento en lo dispuesto por los artículos 6º, 16, 71 y 116 fracción VIII de la Constitución Política de los Estados Unidos Mexicanos; 30, numeral 1, inciso g), 46, inciso d) y 49 de la Constitución Política de la Ciudad de México; así como 12, fracción VI y 13, fracciones LXIV y LXVII de la Ley Orgánica del Congreso de la Ciudad de México, sometemos a consideración de ese H. Congreso de la Ciudad de México, la presente Iniciativa con proyecto de Decreto para expedir la **Ley para el uso de inteligencia artificial y el tratamiento de datos personales por sujetos obligados en la Ciudad de México**.

EXPOSICIÓN DE MOTIVOS

I. El uso de las Tecnologías de la Información y la Comunicación como Derecho Humano

La expansión acelerada de las tecnologías ha traído consigo oportunidades para el desarrollo económico, social y cultural del país, pues ha puesto a nuestra disposición herramientas para acceder y difundir de forma fácil y rápida una gran cantidad de información, lo que ha permitido hacer frente a diversas problemáticas o bien la creación de políticas públicas para una mejor gobernanza.

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

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

"(...)

Artículo 6º. *La manifestación de ideas no será objeto de ninguna inquisición judicial o administrativa, sino en el caso de que ataque a la moral, la vida privada o los derechos de terceros, provoque algún delito, o perturbe el orden público; el derecho de réplica será ejercido en los términos dispuestos por la ley. El derecho a la información será garantizado por el Estado.*
Toda persona tiene derecho al libre acceso a información plural y oportuna, así como a buscar, recibir y difundir información e ideas de toda índole por cualquier medio de expresión.
El Estado garantizará el derecho de acceso a las tecnologías de la información y comunicación, así como a los servicios de radiodifusión y telecomunicaciones, incluido el de banda ancha e internet. Para tales efectos, el Estado establecerá condiciones de competencia efectiva en la prestación de dichos servicios*.*

(...)"[1]

Por su parte, la Relatoría Especial para la Libertad de Expresión e Internet de la Comisión Interamericana de Derechos Humanos, señala 4 criterios orientadores relacionados con el acceso a internet y a las tecnologías de la información, al respecto:

"(...)

1. Acceso

(...)

16. ***El principio de acceso universal se refiere a la necesidad de garantizar la conectividad y el acceso universal, ubicuo, equitativo, verdaderamente asequible y de calidad adecuada, a la infraestructura de Internet y a los servicios de las TIC, en todo el territorio del Estado****, tal como ha sido reconocido por los jefes de Estado en las Cumbres de las Américas.* ***Le corresponde al Estado decidir cuáles son los medios más adecuados, bajo las circunstancias, para asegurar la implementación de este principio****. Sin embargo, como se explica adelante, esta oficina otorga este principio. Sin embargo, como se explica adelante, esta oficina otorga particular importancia a aquellas medidas que buscan asegurar que las estructuras de precios sean inclusivas, para no dificultar el acceso; que la conectividad se extienda a todo el territorio, para promover de manera efectiva el acceso de los usuarios rurales y de comunidades marginales; que las comunidades tengan acceso a centros de tecnologías de la información y comunicación comunitarios y otras opciones de acceso; y que los esfuerzos de capacitación y educación sean reforzados, en especial en sectores pobres, rurales y entre la población mayor.* ***El acceso universal supone también, de manera prioritaria, asegurar el acceso equitativo en términos de género, así como el acceso incluyente de personas en situación de discapacidad y/o pertenecientes a comunidades marginadas****.*

(...)

2. Pluralismo

(...)

19. ***Le corresponde al Estado preservar las condiciones inmejorables que posee Internet para promover y mantener el pluralismo informativo. Esto implica asegurar que no se introduzcan en Internet cambios***

[1] Constitución Política de los Estados Unidos Mexicanos, artículo 6º, p. 12, Constitución Política de los Estados Unidos Mexicanos (diputados.gob.mx)

***que tengan como consecuencia la reducción de voces y contenidos. Las políticas públicas sobre la materia deben proteger la naturaleza multidireccional de Internet y promover las plataformas que permitan la búsqueda y difusión de informaciones e ideas de toda índole**, sin consideración de fronteras, en los términos del artículo 13 de la Convención Americana.*

(…)

3. No discriminación

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

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

4. Privacidad

(…)

*23. Tal y como fue observado por la Asamblea General de las Naciones Unidas en la resolución "El derecho a la privacidad en la era digital", adoptada por consenso, **los Estados tienen la obligación de respetar y proteger el derecho a la privacidad de conformidad con el derecho internacional de los derechos humanos, incluyendo en el contexto de las comunicaciones digitales…las autoridades deben, de una parte, abstenerse de hacer intromisiones arbitrarias en la órbita del individuo, su información personal y sus comunicaciones y… deben garantizar que otros actores se abstengan de realizar tales conductas abusivas**. Por ejemplo, se debe promover la existencia de espacios en línea libres de observación o documentación de la actividad e identidad de los ciudadanos. Esto incluye, por ejemplo, la preservación de plataformas anónimas para el intercambio de contenidos y el uso de servicios de autenticación proporcionales…*

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

(…)"[2]

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

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

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

El tercer principio, el cual está relacionado con nuestro artículo primero constitucional, y el principio de neutralidad de la red, se refiere a la no discriminación, en donde se garantice el acceso a las tecnologías de la información en igualdad de condiciones, aplicando medidas de inclusión, nivelación y acciones afirmativas en favor de personas en situación de vulnerabilidad.

Al respecto, en la Declaración conjunta sobre libertad de expresión e Internet[3], se señaló que la neutralidad de la red es un principio según el cual el tratamiento de los datos y el tráfico de Internet no debe ser objeto de ningún tipo de discriminación en función de factores como dispositivos, contenido, autor, origen o destino del material, servicio o aplicación.

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

Por lo que hace a la privacidad de las personas, contenido en el cuarto principio, contempla tanto la obligación de los Estados de respetar y proteger este derecho, incluyendo incluso el contexto de las comunicaciones digitales, absteniéndose de hacer intromisiones arbitrarias en su información

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

personal y sus comunicaciones, promoviendo la existencia de espacios en línea libres de observación o documentación de la actividad e identidad de las personas.

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

"(...)

Artículo 8
Ciudad educadora y del conocimiento

"(...)

C. Derecho a la ciencia y a la innovación tecnológica

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

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

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

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

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

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

6. ***En el presupuesto de la Ciudad de México, se considerará una partida específica para el desarrollo de la ciencia y la tecnología****, que no podrá ser inferior al dos por ciento del Presupuesto de la Ciudad.*

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

(...)"[4]

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

Asimismo, se establece que las autoridades fortalecerán y apoyarán la generación, ejecución y difusión de proyectos de investigación científica y tecnológica, así como la vinculación de estos con los sectores productivos, sociales y de servicios, a fin de resolver problemas y necesidades de la Ciudad, contribuir a su desarrollo económico y social, elevar el bienestar de la población y reducir la desigualdad.

Tanto en el ámbito local, federal e internacional se reconoce a toda persona el derecho a acceder a las tecnologías de la información y comunicación, como es el caso de la inteligencia artificial, en un sentido de progresividad.

Por lo que garantizar este derecho resulta trascendental, ya que su importancia radica en que las plataformas digitales e incluso ya las inteligencias artificiales que habitan el espacio digital conviven todas las personas y son participes de nuestras actividades diarias. Por lo que hacer accesible y posible este derecho en concordancia con la protección de nuestros datos personales, permitirá una mejor interacción y comunicación humana, buscando eliminar cualquier barrera física que nos imponían el tiempo y la distancia.

En México las tecnologías de la información y el Internet han experimentado una transformación significativa en las últimas décadas, impulsada por el crecimiento de la infraestructura digital, sin embargo, a pesar de los avances, el país aún enfrenta retos considerables como la brecha digital, los riesgos a la privacidad y la ciberseguridad, entre otras.

[4] Constitución Política de la Ciudad de México, artículo 8º, p. 14, CONSTITUCION_POLITICA_DE_LA_CDMX_9.pdf

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

II. Inteligencia Artificial, protección de datos personales y privacidad

Los desarrollos tecnológicos, como la Inteligencia Artificial (IA), no sólo mejoran muchas de nuestras experiencias, sino que su indebida utilización traducida en una violación a la intimidad y privacidad de las personas puede acarrear graves consecuencias para las sociedades tanto en lo colectivo como en lo individual (Brexit, asalto al capitolio, desinformación en tiempos de pandemia, violencia digital, ciberacoso, etc.).

Lo anterior, porque la fortaleza de la IA radica en los datos, pero también representan el eslabón más débil que se debe proteger cuando esos datos pertenecen a las personas e impactan su vida privada. La magnitud de las consecuencias adversas de un sistema de IA para los derechos humanos es de gran relevancia al momento de proteger a las personas y a sus libertades.

Su impacto es tan importante que, en todo el mundo existe un debate sobre si las empresas tecnológicas y los gobiernos deben permitir que las personas asuman de nueva cuenta su control, o si su tratamiento, al ser parte del derecho a la privacidad de las personas, tiene que ser modificado tomando en cuenta los diversos casos problemáticos. Lo cierto es que, durante la última década se han presentado diversos casos que han producido que los gobiernos legislen e impongan prohibiciones, multas y hasta el grado de discutir si los algoritmos pueden ser considerados como "agencia" sujeta a responsabilidad legal.

De esta manera, gobiernos, empresas y la academia están buscando cómo proteger los datos personales, la libertad de expresión y de información, el derecho a la no discriminación, el derecho a la educación, la protección de mercado, los derechos laborales, los grupos vulnerables (niñez, adultos mayores, mujeres, personas LGBTTTIQ+, entre otros), la propiedad intelectual, la dignidad de las personas, la democracia, el estado de Derecho y el medio ambiente.

Estamos entrando a una etapa nueva de “revolución digital por el uso de IA” en la que la privacidad, la rendición de cuentas y los derechos humanos se están interconectando en cada Poder Legislativo como un tema de agenda prioritaria para su regulación. Las empresas y organizaciones responsables de emisión de normas para la aplicación de estándares también se han sumado a esta actividad, aportando metodologías para la gestión de riesgos por el uso de IA.

Hoy tenemos algoritmos que toman decisiones en tiempo real y sin intervención humana, que son sometidos a auditorías algorítmicas para prevenir impactos adversos y brindar a las personas usuarias sistemas de IA cuyos datos de entrenamiento, validación, prueba y puesta en operación tienen un grado de fiabilidad que se registra en bases de datos gubernamentales que permiten cuidar a las personas y a la sociedad en su conjunto. Existen también modelos de IA que son entrenados con grandes volúmenes de datos cuyo origen no ha sido revelado y, al igual que con las auditorías financieras, la auditoría de algoritmos se está convirtiendo en un requisito indispensable que guía el panorama de la protección de datos.

Por lo que, como Estado debemos pensar en diseños normativos que, sin afectar la libertad de expresión u otros derechos, constriñan a quienes proveen de servicios digitales, así como a las instituciones que hacen uso de la IA, a realizar evaluaciones de impactos potenciales, cortes analíticos periódicos de sus desarrollos y, sobre todo, dotar de información clara a las personas, acerca de lo que se hará con sus datos por parte de las inteligencias artificiales que operan.

Del mismo modo, debemos generar controles efectivos para que las personas se autodeterminen informativamente en lo digital y podamos incluso apagar aquellas inteligencias artificiales que, tras ser auditadas conforme a procedimientos normados y razonables, descubramos que han aprendido lo que no debían aprender de nosotras y nosotros.

Para ello, debemos centrarnos en la confiabilidad, asegurando que la IA sea legal, ética y robusta desde un punto de vista técnico, implementando estrategias dirigidas especialmente en lo que respecta a la privacidad y la protección de datos personales, centradas en la ética, la innovación y el apoyo a la investigación y el desarrollo en el campo de la IA.

Si bien, son muchas las ventajas del uso de las tecnologías y la inteligencia artificial, no debemos olvidar que requieren datos de las y los usuarios, lo que representa riesgos en su tratamiento, manejo, transferencia y seguridad.

Sin el conocimiento o la autorización de la persona titular de los datos respectivos pueden predecir nuestras actuaciones, gustos e intereses, a partir de los datos que compartimos y se someten a su análisis. En este sentido, desde el Instituto, facultado constitucionalmente como Órgano Garante en materia de protección de datos personales, existe una constante preocupación respecto del uso masivo de sistemas de IA que para su funcionamiento requieran de información que identifique o haga identificable a la persona detrás del dato personal; ya que ello puede implicar afectaciones graves a la autodeterminación informativa, intimidad, privacidad y dignidad de las personas, porque la IA recaba grandes cúmulos de información en tiempo real, las procesa y toma decisiones, lo cual expone aspectos privados de la vida de las personas, como los hábitos de consumo de un hogar, los ingresos económicos o su ideología política o religiosa, por mencionar algunos.

Esta sobreexposición y concentración de información, deja a las personas usuarias de sistemas de inteligencia artificial desprotegidas frente al poder acumulado por las corporaciones. Ejemplos como el de Cambridge Analytical hacen evidente la necesidad de vigilar el comportamiento de tecnologías como la inteligencia artificial.

En este contexto, tal y como sucede en otras parte del mundo como China, Estados Unidos, así como la reciente Ley Europea sobre la IA, debe regularse el alcance y contenido de los sujetos obligados a quienes aplicaría la normativa y su respectivo grado de responsabilidad, específicamente en la Ciudad de México.

De igual forma, debe prever los requisitos claros que deberán reunir las IA para poder operar en la capital del país sin que menoscabe los derechos y dignidad de las personas y promueva la innovación tecnológica en un marco de ética y responsabilidad.

Deben establecerse también procedimientos sancionatorios y sanciones para quienes infrinjan la normativa en materia de IA, pues con ello estaríamos cumpliendo a cabalidad la tutela judicial efectiva de las personas, misma que prevé contar con un recurso efectivo que garantice sus derechos respetando todas las reglas del debido proceso y sobre todo contar con sanciones que lo hagan efectivo.

III. Uso de las Tecnologías en la administración pública en la Ciudad de México

En la capital del país, tenemos a la Agencia Digital de Innovación Pública[5], que de 2019 a 2023 simplificó 2,100 trámites gubernamentales para facilitar la vida de quienes habitan la Ciudad de México y con ello reducir el tiempo de respuesta. También trasladó el 70% de los trámites a un portal en Internet y logró el impulso de Wi-Fi gratuito en lugares públicos y escuelas para ayudar a familias de bajos recursos y jóvenes a contar con la posibilidad de acceder a herramientas de IA.

Desde 2021, la Ciudad de México es la más conectada del mundo con 32, 947 puntos de acceso al que se han conectado en total 20 millones de personas usuarias. La estrategia de conectividad en la capital está diseñada para garantizar que las personas puedan ejercer su derecho al acceso al Internet, fomentando un acceso progresivo a las tecnologías de información y comunicación.

También, se ha puesto en operación la "Llave CDMX Expediente" con la que acceden más de 6 millones de personas usuarias, equivalentes a 14 millones 300 mil "log-ins". Con la cuenta Llave CDMX Expediente las personas tienen acceso a todos los trámites digitales que existen en la Ciudad, pueden guardar sus documentos personales y reutilizarlos para nuevos trámites o consultar el estado de cada uno. Esta iniciativa forma parte de uno de los pilares fundamentales dentro de la estrategia de transformación digital de la ciudad y ha significado un cambio en el modelo de administración pública.

La Ciudad de México, ha ganado varios premios de innovación a nivel internacional, por ejemplo, por el programa PILARES (Puntos de Innovación. Libertad, Arte, Educación y Saberes) con 294 centros comunitarios establecidos en toda la ciudad para ofrecer a las personas programas sociales

[5] Los datos que a continuación se narran son tomados del sitio: https://adip.cdmx.gob.mx/

que fomentan vínculos comunitarios y ayuda a grupos vulnerables a obtener habilidades útiles para la vida.

También, la ciudad cuenta con una tarjeta digital de transporte urbano para consolidar servicios de múltiples proveedores y brindar acceso sin inconvenientes al Metro, Metro Bus, Trolebús, Cablebús y al teleférico más largo del mundo. Cuenta con una red de bibilotecas públicas, como espacios en los que miles de personas acuden y utilizan el servicio de Internet para mejorar sus vidas. Existe la digitalización de las tarjetas de circulación vehicular, de las licencias de conducir, de las actas de nacimiento, así como la posibilidad de hacer trámites para la apertura de negocios en los que se suben datos de las personas.

Se ha desarrollado por la Agencia Digital de Innovación Pública más de 200 aplicaciones en beneficio de la población, que no solamente se utilizan en la Ciudad de México, sino que también se comparten con algunas entidades federativas y municipios; con ellas, se pueden solicitar taxis públicos, llamar a la policía, activar un botón de auxilio, renovar trámites para restaurantes.

Se cuenta con la plataforma denominada “Tianguis Digital” creada para planear, conducir y vigilar los procedimientos de contratación pública. Gracias a esta plataforma es posible dar seguimiento a los procedimientos de contratación pública, de forma abierta y transparente, y asegurar que los recursos destinados se inviertan adecuadamente. Los módulos se integran por información pública y privada y se puede consultar el padrón de proveedores, convocatorias de contratación, así como la conexión con sistemas fiscales y bancarios. A febrero de 2022 se habían registrado 6,188 proveedores y existían más de 4 mil convocatorias públicas.

En lo legislativo, se han hecho importantes avances como la creación de una Ley para Garantizar el Acceso Libre y Gratuito al Internet en la Ciudad de México que señala en su artículo 18, último párrafo que el “acceso gratuito al servicio público gratuito de internet que brinde la Administración Pública y Alcaldías, no recopilará datos personales de los usuarios” y una Ley de Operación e Innovación Digital para la Ciudad de México, en la que la gobernanza tecnológica regirá bajo los principios de apertura, escalabilidad, interoperabilidad, protección de datos personales y privacidad. La ley faculta a la Jefatura de Gobierno de la Ciudad para diseñar, implementar y supervisar la política de gobernanza tecnológica, diseñar la Plataforma de Inter operatividad Gubernamental, definir el modelo de gobernabilidad de tecnologías de la información y comunicaciones y dictaminar técnicamente la adquisición de tecnologías de la información así

como coordinar la participación de instituciones públicas y privadas en la realización de proyectos de tecnologías de la información y comunicaciones.

Además de contar con la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, la cual tiene por objeto establecer las bases, principios y procedimientos para garantizar el derecho que tiene toda persona al tratamiento lícito de sus datos personales, a la protección de los mismos, así como al ejercicio de los Derechos de Acceso, Rectificación, Cancelación y Oposición de sus datos personales en posesión de sujetos obligados, facultando al Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México su debida observancia.

El Instituto ha desarrollado diversos mecanismos tecnológicos, incluso usando la IA, para poder cumplir con sus atribuciones, ejemplo de ello es el SIVER, herramienta tecnológica que busca integrar los procesos operativos y facilitar la entrega de la información para verificar y gestionar de manera eficaz cada una de las etapas y los tiempos establecidos en la Ley de Datos local.

De igual forma, se desarrolló con IA "ATIC", como una herramienta tecnológica que tiene como finalidad establecer un canal de comunicación entre la ciudadanía y este órgano autónomo, brindando asesoría en las tareas relacionadas con las obligaciones de transparencia, mediante comunicaciones fluidas, ágiles y accesibles con disponibilidad las 24 horas y los 365 días del año, lo que ha permitido que las personas puedan obtener información pública en pocos segundos.

Como podemos advertir, la Ciudad de México tiene a todo el gobierno interconectado, razón por la cual es indispensable que contemos con instrumentos jurídicos adecuados que permitan cumplir las atribuciones que, como instituciones, marca la Constitución; pero al mismo tiempo se protejan los datos y derechos de las personas.

Así, la Ley que proponemos coadyuvará al perfeccionamiento del marco normativo que da gobernanza digital a la Ciudad de México, específicamente, en materia de protección de datos personales ante el desarrollo y utilización de sistemas de inteligencia artificial por parte de las instituciones públicas en la capital del país.

IV. Contenido de la Iniciativa

La propuesta que presentamos ante ese H. Congreso de la Ciudad de México está en consonancia con el enfoque adoptado por diversos organismos internacionales y nacionales como, por ejemplo:

a) *Recomendación del Consejo de la OCDE sobre Inteligencia Artificial (actualizada a mayo 2024)*[6], la cual es considerada como documento pionero en delimitar este tema, siendo sus principios un eje rector reconocido por académicos, gobiernos y empresas.

b) *Recomendación sobre la Ética de la Inteligencia Artificial*[7] de la UNESCO, en la que se exhorta a los gobiernos su suscripción y recomendando una regulación siguiendo las buenas prácticas que han emitido organizaciones de la sociedad civil pioneras en el tema del uso del internet, los datos y la inteligencia artificial. Lo que hace excepcional a esta recomendación es que permiten a los responsables políticos "traducir los valores y principios fundamentales en acciones con respecto a la gobernanza de datos, el medio ambiente y los ecosistemas, el género, la educación, la investigación, la salud y el bienestar social, entre otros muchos"[8].

c) *Recomendaciones* del *Open Data Institute* (ODI) y su programa "IA centrada en los datos", el cual fomenta la innovación y los compromisos de la Declaración de Bletchley[9] haciendo que los sistemas de IA utilicen los datos de forma responsable. Esto incluye creación de marcos regulatorios para definir y evaluar el valor de los datos y de los modelos de negocio que utilizan IA, aprendizaje federado, programas de innovación que apoyen a MiPyMes y cursos de capacitación sobre ética para el uso de los datos y la IA[10]:

En todo este trayecto, el ODI, organismo de gran renombre no sólo por el prestigio de quienes lo fundaron, sino también por la calidad de sus investigaciones, ha desarrollado un programa de trabajo sobre IA centrada en los datos, diseñado para crear un ecosistema de IA basado en prácticas de datos responsables que se está promoviendo como una salida alterna entre el rigor de la legislación Europea o de los Estados Unidos y la exigencia de evitar la regulación del tema.

[6] Consúltese en: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449
[7] Consúltese en https://www.unesco.org/es/artificial-intelligence/recommendation-ethics?hub=32618
[8] Para más datos sobre la recomendación, consúltese: https://www.unesco.org/es/artificial-intelligence/recommendation-ethics?hub=32618
[9] Existen las valiosas aportaciones que el gobierno del Reino Unido ha compartido con los países que asistieron a la Cumbre de seguridad de la IA, el 1 y 2 de noviembre de 2023 y que hacen hincapié en un enfoque alterno al modelo de la Unión Europea, basado en un criterio de la creación de regulación por sector o sectorizado. Consúltese el texto de la Declaración de Bletchely en: https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/dbc58681-1b68-47e0-8e3f-f91435fdf8ce
[10] Consúltese más información en: https://theodi.org/insights/projects/data-centric-ai/

Consideramos que en materia de datos personales, se debe de actualizar la legislación y esta propuesta fue construida para ser un ejemplo de equilibro entre los diferentes modelos regulatorios. A decir del ODI, los gobiernos "tienen un papel importante que desempeñar en este sentido, desde la introducción de nuevas leyes que regulen el uso de los datos para entrenar a la IA, hasta el estímulo de la inversión y la innovación en la garantía y el intercambio de datos, pasando por el uso de los datos y la propia IA de manera transparente para prestar servicios públicos"[11].

Respecto a la generación de nuevas normas para la protección de datos que se utilizan para entrenar a la IA, recomienda que la legislación garantice la innovación de estas nuevas tecnologías, continuando el desarrollo y el despliegue de la IA, pero con un beneficio a personas, empresas y la sociedad en su conjunto.

Cabe señalar en este tema, que los datos personales que son utilizados por los sistemas de IA para su desarrollo o uso, no deben ser secretos para las personas dueñas de esa información ni para las organizaciones a las que el gobierno les asigna la responsabilidad de su protección. Por esta razón, en muchos países del mundo se están regulando los datos que se utilizan para el desarrollo o uso de modelos de inteligencia artificial y cuyo procesamiento se caracteriza por un alto volumen de información que sirve para realizar interacciones complejas y generar a los usuarios resultados que gran calidad que de otra manera no hubieran sido posibles de aportar.

Además las tres recomendaciones comentadas, debemos mencionar que el 1º de agosto de 2024 entró en vigor el *Reglamento de Inteligencia Artificial de la Unión Europea*[12], cuyo modelo se basa en el "enfoque basado en riesgos" y las Directrices éticas para una IA confiable (2019) elaboradas por el Grupo independiente de expertos de alto nivel creado por la Comisión Europea, las cuales buscan dar seguridad jurídica a las personas pero ha sido cuestionada por la alta carga regulatoria que contiene y que puede transformarse en una carga que inhiba el uso de modelos de IA.

Creemos que la Ciudad de México, en materia de privacidad y uso de datos para el desarrollo o utilización de modelos de IA, debe tomar una regulación sectorizada que tenga como base el contenido que se propone en esta legislación, pero que cada sujeto obligado, según sus necesidades

[11] Intervención política 1: Aumentar la transparencia en torno a los datos utilizados para entrenar modelos de IA | La ODI (theodi.org)

[12] Diario Oficial de la Unión Europea del 12 de julio de 2024.

y etapas de implementación de la IA, esté acompañado de la experiencia que tiene el Instituto en materia de protección de datos personales.[13]

En México, la sociedad civil también ha estado activa a través de organizaciones especializadas en el desarrollo de políticas públicas y tecnología tales como EON INSTITUTE, CMINDS, el Centro México Digital y la Alianza Nacional de Inteligencia Artificial, generándose diferentes documentos durante los últimos seis años de actividad. Quizás el de mayor relevancia es la "Propuesta de Agenda Nacional de la IA para México 2024-2030", que busca poner los cimientos del rumbo en materia de políticas públicas para el próximo sexenio.[14] La iniciativa transforma muchas de esas ideas en norma jurídica y también incluye las reflexiones de este sector en materia de protección de datos y respeto al derecho humano a la privacidad.

El Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México ha venido trabajando en la revisión de los diferentes modelos regulatorios que se están generando, la legislación que hoy se presenta se preparó bajo 5 criterios generales básicos que sirvan de base para que en un futuro puedan ser utilizados por otras entidades del país y la misma federación para su implementación desde sus diferentes ámbitos de competencia. Los 5 criterios son los siguientes:

1. Regulación por sector basada en las facultades de cada unidad administrativa: La iniciativa únicamente atiende temas de privacidad y uso de datos personales que sirve para el desarrollo de modelos de IA o para la toma de decisiones derivadas de los mismos por parte de las instituciones públicas de la capital del país.
2. Coherencia con el enfoque regulatorio nacional e internacional: La iniciativa se construyó tomando en consideración que, si bien, ni en la Constitución Federal o alguna Ley de carácter General y Federal se prevén atribuciones exclusivas para presentar iniciativas en materia de IA, lo cierto es que con la finalidad de no dejar desprotegida a la población en

[13] En 2023, el Gobierno del Reino Unido también creo el Instituto de Seguridad de la IA para centrarse en la "seguridad avanzada de la IA para el interés público". Una de sus funciones clave es facilitar el intercambio de información con entidades nacionales e internacionales, adhiriéndose a las regulaciones de privacidad y datos existentes. Esto incluye el intercambio de datos sobre el entrenamiento y el ajuste de los sistemas de IA, que es crucial para la función del Instituto de realizar evaluaciones de sistemas de IA. En marzo de 2024, se presentó en la Cámara de los Lores un proyecto de ley de miembros privados que exige a los proveedores de IA que compartan información sobre sus datos de entrenamiento con una "Autoridad de IA central", garanticen el consentimiento informado al recopilar datos de entrenamiento y se sometan a auditorías obligatorias. Sin embargo, el proyecto de ley no avanzó, es probable que se obligue a las empresas de IA a compartir sus datos de prueba con el gobierno del Reino Unido para evitar que su uso impacte de forma negativa a las personas.

[14] Consúltese ese y otros documentos en: https://www.ania.org.mx/documentos

la protección de sus datos personales como Órgano Garante, y constitucionalmente autónomo en esa materia, se cuenta con atribuciones constitucionales para que, desde lo local podamos presentar iniciativas relacionadas con las materias y derechos humanos que tutelamos en un sentido de progresividad. En el ámbito internacional hemos verificado que se adapte, atendiendo a nuestra realidad social, cultural, tecnológica y jurídica a los principios de la legislación propuesta por el Reino Unido e Israel. Sin omitir el estudio de otras como la de los Estados Unidos, la Unión Europea, Chile, Colombia y Perú. De tal forma que la persona legisladora tenga la certeza que se aprobará una ley con la profundidad de estudio adecuada para su entrada en vigor de manera valida y eficaz.

3. Adopción de un enfoque basado en riesgos: Si bien se utiliza el modelo de gestión de riesgos de privacidad para medir el impacto al sistema de IA (tal como ahora se hace en temas alejados de lo digital), no se cae en el extremo de la gestión de riesgos abierta a cualquier tipo de riesgo, pues, de lo contrario, la convertiría en una carga regulatoria innecesaria.
4. Uso de herramientas de "soft law": La Ley permite a los sujetos obligados que están utilizando IA guiar el cumplimiento de la misma a través de normas ISO y normas de la IEEE relacionadas con riesgos de privacidad y uso de IA. Esto permitirá que la Ciudad de México sea punto de referencia para el desarrollo y uso de modelos de inteligencia artificial innovadores sin una carga regulatoria excesiva.
5. Fomento de la cooperación entre los sectores público, privado y académico: La ley se desarrolló con la colaboración del sector privado, la academia y la vinculación internacional que hizo la Embajada del Reino Unido para que expertos de México y la Gran Bretaña intercambiaran consejos y buenas prácticas que hoy están plasmados en esta iniciativa de Ley.

En consecuencia, la "**Ley para el uso de inteligencia artificial y el tratamiento de datos personales por sujetos obligados en la Ciudad de México**" actualizará y se complementará con nuestra legislación que protege los datos personales en Posesión de sujetos obligados de esta capital y demás normas secundarias que regulan la privacidad con base en la Constitución Política de la Ciudad de México.

La iniciativa busca proteger a las personas y el uso de sus datos, ya sea para actividades de entrenamiento de modelos de inteligencia artificial, para el uso de la IA en la comercialización de

servicios o productos. Su contenido es un referente para que las empresas que están trabajando con sistemas de inteligencia artificial conozcan, entiendan y apliquen las reglas de la privacidad y las reglas de la transparencia de la información que existen en la Ciudad de México y con ello generar seguridad jurídica evitándose una afectación a los derechos de las personas sin inhibir la innovación.

Por tanto, existe un capítulo en el que se le pide a las empresas que están utilizando este tipo de inteligencia artificial que, desde antes de que el sistema inteligente se ponga en ambiente de producción, su personal esté capacitado en ética de la inteligencia artificial, regulación sobre privacidad y responsabilidad por el uso de algoritmos que se utilizan para la toma de decisiones. Creemos que las personas, físicas o jurídicas, deben conocer los casos de malas prácticas en los que se ven afectados los datos personales y, a la vez, entiendan la forma correcta de tratarlos, de cuidar su uso y almacenamiento hasta su destrucción.

Hay que decir que, si bien el concepto "transparencia" no se regula a profundidad, sí existe la posibilidad de que el Instituto intervenga ante alguna queja ciudadana, lo cual busca generar una cultura de la gobernanza de datos sin ser tan invasivo de la empresa. Si bien el concepto de transparencia se ha desarrollado de sobremanera en el sector público y en otras muchas actividades del hombre, el sector tecnológico y, más específicamente, el sector que la inteligencia artificial está apenas en construcción con reglas específicas de las cuales el Congreso de la Ciudad de México tendrá que incorporar en algún momento para evitar la manipulación de los datos.

Está demostrado que existen casos de manipulación de la información relacionados con el uso de algoritmos de inteligencia artificial, tanto en el sector público como en el sector privado, y esta manipulación deriva de a) razones reales o personales, b) razones legales o c) de falta de razones (por intereses personales o de grupo).

Existen *razones reales o personales* cuando, en calidad de empresas que entrenan modelos de IA o usuarios que tienen algún sistema de IA, se decide que nadie tenga accesos a los datos con los que entrenó el modelo o con el que usó el modelo y se evita compartirlos.

Las *razones legales* obligan a quienes tienen conocimiento de determinada información a mantenerla en secreto; por ejemplo, una persona que labora en un banco está obligada por la autoridad legal a no revelar los saldos de sus clientes.

Y, la *falta de razones* la encontramos en aquellos intentos deliberados de ocultar la información por una decisión personal o de un grupo ante el temor de que la revelación de la información genere

algún daño y se evita darla o se manipula la entrega. Por ejemplo, una empresa podría responder a una solicitud de información entregando 15 mil páginas de documentos mal testados y desordenados, lo cual obligaría a la persona solicitante a invertir mucho tiempo buscando la información requerida.

La doctrina indica que existen dos tipos de modelos algorítmicos*:* Uno abierto, interpretable y explicable. Otro que se considera de caja negra, porque se conocen los datos de entrada y los de salida, pero no cómo se generaron; no se sabe cómo se entrenan ni cómo llegan a la mejor solución o conclusión, aquí la transparencia se ve afectada. Así, la propuesta de ley busca regular el segundo tipo de algoritmos mediante el uso de auditorías algorítmicas.

Entendamos el contexto partiendo del concepto de responsabilidad en una sociedad informatizada. Hace más de 25 años, Helen Nissenbaum, hizo una reflexión muy novedosa respecto del concepto responsabilidad en una sociedad informatizada. Señaló cuatro tendencias que diluyen las líneas de responsabilidad: "Primero, los sistemas computarizados generalmente son diseñados y operados por "muchas manos". Como resultado, la responsabilidad se difunde entre muchas partes y se oscurece un análisis de quién o qué instituciones pueden rendir cuentas. En segundo lugar, la inevitabilidad de los errores en el software también parece proporcionar una especie de excusa para dejar de preocuparse por un software defectuoso en general. Esto tiende a ocultar un análisis adecuado de los errores en el software y dificulta la inversión de esfuerzos en su eliminación y prevención. En tercer lugar, cuando las cosas salen mal, con demasiada facilidad tendemos a culpar a la computadora en lugar de a las personas involucradas. Finalmente, no es útil que los desarrolladores de software se nieguen rotundamente a rendir cuentas por sus productos."[15]

Ibo van de Poel comenta que quizás fue Denise Thompson, la primera en utilizar la noción *The many hands problema,* en un artículo sobre la responsabilidad de las personas funcionarias públicas y lo describe de la siguiente manera: "Debido a que muchos funcionarios diferentes contribuyen de muchas maneras a las decisiones y políticas del gobierno, es difícil, incluso en principio, identificar quién es moralmente responsable de los resultados políticos"[16]

---

[15] Cfr. Helen Nissenbaum, "Accountability in a Computerized Society", en *Science and Engineering Ethics*, número 2, vol. 25, 1996. Consúltese en: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.40.77 [20 de julio de 2022]

[16] Cfr. van de Poel, I., Fahlquist, J. N., Doorn, N., Zwart, S., & Royakkers, L. (2012). The problem of many hands: climate change as an example. Science and engineering ethics, 18(1), 49–67, p. 50. Consúltese en: https://doi.org/10.1007/s11948-011-9276-0 [20 de julio de 2022] Para profundizar más sobre este tema puede consultarse: a Ibo van de Poel, Lambèr Royakkers, Sjoerd D. Zwart, *Moral Responsibility and the Problem of Many Hands*, Routledge, 2018.

Estas cuatro posturas pueden diluir la responsabilidad legal y, en consecuencia, la reparación del daño a una víctima. A partir de 2022, y con la entrada en funcionamiento de los *Large Language Models*, debemos adicionar ahora una quinta tendencia que tiene que ver con la creciente importancia de la toma de decisiones, respaldada por el uso de algoritmos de *Deep Learning* en los que la voluntad del ser humano no necesariamente participa. Tales algoritmos están guiando nuestras vidas a cada momento y, desafortunadamente, estamos viendo que algunos de sus resultados traen sesgos que impactan la privacidad de las personas. A nivel colectivo, los resultados pueden estar sesgados en función del género, la etnia u otras características o circunstancias.

Desde el exterior, la caja negra se prueba, ya sea insertando varias entradas y observando las salidas o, si la entrada no se puede manipular, observando las salidas disponibles. Sin embargo, esta revisión supera las capacidades humanas tradicionales. La pregunta que se ha venido haciendo por diversas personas expertas en la materia es: ¿Cómo crear una cultura de responsabilidad algorítmica? Zarsky promotor de la transparencia algorítmica señala: "El análisis del nexo entre transparencia y rendición de cuentas solo puede proceder después de la introducción de dos distinciones importantes. Por un lado, se deben distinguir varias fases de la toma de decisiones: Primero es la recopilación de datos (conjuntos), posteriormente los datos se utilizan en el aprendizaje automático para desarrollar un modelo (desarrollo del modelo), y finalmente ese modelo se utiliza para la toma de decisiones (uso del modelo)". [17] En conjunto, estas dos distinciones implican que cualquier llamado a la transparencia debe ser específico sobre lo que se debe revelar y a quién se debe dar. El aprendizaje automático está muy relacionado entre sí en las etapas de recopilación de datos, construcción del modelo y uso del modelo. Cuando se llama a una organización a rendir cuentas se debe analizar todo para no afectarla. Conscientes de esto, la Ley contempla un capítulo de gestión de riesgos y otro de responsabilidad algorítmica por el uso de sistema inteligentes que se usan para la toma de decisiones en los que el uso de datos personales son la fuente que les da vida.

La postura del Instituto es buscar la transparencia de los modelos de IA, siempre y cuando sea una exigencia ciudadana justificada, derivada de un caso de impacto a la privacidad y cuidando que no se impacten de manera trascendente en el funcionamiento de las instituciones o en el orden público. En cuanto a la transparencia en el uso de datos, no sería prudente hacer que los conjuntos de datos estén disponibles para cualquiera, equivaldría a una invitación por violaciones de la privacidad. Es

[17] T. Z., Zarsky, "Transparent predictions", *University of Illinois Law Review*, número 4, 2013, pp. 1503-1570.

importante, por tanto, excluir al público en general de obtener una transparencia total cuando el caso no lo requiera y sin cuidar las reglas que existen actualmente para el tratamiento de la información.

Como regla general, las empresas hacen énfasis en sus derechos de propiedad sobre el uso de sus modelos algorítmicos, lo cual se debe de respetar, pero a la vez, estos modelos algorítmicos no deben de ser utilizados para su entrenamiento sin que se verifique: a) la fuente de los datos (persona física o moral); b) la licitud de los datos, c) la forma en la que se crearon esos datos; d) el mecanismo de filtrado, incremento o disminución del tamaño de los datos; e) la detección de aquellos que estén sujetos a regulaciones específicas (derechos de autor); y, f) la persona (física o jurídica) que hace el licenciamiento de los datos. Esta postura debe tomarse en cuenta ya que busca reducir la opacidad en el uso de datos.

Una segunda reflexión en este tema, como afirma Laat[18] es que, en conjunto, las personas afectadas en el uso de sus datos deben tener el derecho de obtener una explicación completa sobre todo lo que les concierne. Los organismos de protección de datos son el mecanismo garante para que la persona afectada y la persona física o jurídica que hizo el impacto, tomen el camino de la legalidad y lleguen a una rendición de cuentas que inhiba este tipo de conductas.

La capacidad de interpretación de los algoritmos sigue siendo aquí un tema de la mayor relevancia. Por eso la ley se orienta también hacia la responsabilidad algorítmica o el uso de algoritmos que generan IA y que esta, al impactar de forma negativa a los derechos humanos, sin intervención de estos últimos, debe ser modificada o, en su caso, suspender su desarrollo o utilización.

Las posibles soluciones que se generen con motivo de la transparencia y el uso de datos, así como los problemas de algoritmos de caja negra, deben tener en cuenta tres preguntas clave: 1. ¿Cuánto tiene que revelar la empresa que usa los algoritmos de caja negra? 2. ¿A quién debe revelarlo? y 3. ¿Y qué tan rápido debe ocurrir la revelación? En mayo de 2017, la Association for Computing Machinery (ACM) aprobó una declaración sobre "Transparencia y responsabilidad algorítmica". La declaración de ACM presenta siete principios para promover la transparencia algorítmica:

Principios para la transparencia y la responsabilidad algorítmica

[18] P.B. Laat, "Algorithmic Decision-Making Based on *Machine Learning* from Big Data: Can Transparency Restore Accountability?" *op. cit.,* pp. 525–541 [20 de julio de 2022]

1. Conciencia: Las personas propietarias, diseñadoras, constructoras, usuarias y otras partes interesadas de los sistemas analíticos deben ser conscientes de los posibles sesgos involucrados en su diseño, implementación y uso, así como del daño potencial que los sesgos pueden causar a la sociedad.

2. Acceso y reparación: Quienes regulan deben fomentar la adopción de mecanismos que permitan interrogar y compensar a las personas y grupos que se ven afectados negativamente por decisiones tomadas algorítmicamente.

3. Responsabilidad: Las instituciones deben ser responsables de las decisiones tomadas por los algoritmos que utilizan, incluso si no es factible explicar en detalle cómo los algoritmos producen sus resultados.

4. Explicación: Se anima a los sistemas e instituciones que utilizan la toma de decisiones algorítmica a producir explicaciones sobre los procedimientos seguidos por el algoritmo y las decisiones específicas que se toman. Esto es particularmente importante en contextos de políticas públicas.

5. Procedencia de los datos: Quienes crean los algoritmos deben mantener una descripción de la forma en que se recopilaron los datos de entrenamiento, acompañada de una exploración de los posibles sesgos inducidos por el proceso de recopilación de datos humanos o algorítmicos. El escrutinio público de los datos brinda la máxima oportunidad de realizar correcciones. Sin embargo, las preocupaciones sobre la privacidad, la protección de secretos comerciales o la revelación de análisis que podrían permitir a actores malintencionados engañar al sistema pueden justificar la restricción del acceso a personas calificadas y autorizadas.

6. Auditabilidad: Los modelos, algoritmos, datos y decisiones deben registrarse para que puedan ser auditados en los casos en que se sospeche de daño.

7. Validación y pruebas: Las instituciones deben utilizar métodos rigurosos para validar sus modelos y documentar esos métodos y resultados. En particular, deberían realizar pruebas de forma rutinaria para evaluar y determinar si el modelo genera daño discriminatorio. Se anima a las instituciones a hacer públicos los resultados de dichas pruebas.[19]

El Instituto, consciente de lo anterior y tomando en consideración la responsabilidad de actualizar su marco normativo siguiendo las recomendaciones de la *Global Privacy Assembly (GPA)*, emitidas en la XLII sesión de la Asamblea Global de Privacidad (octubre de 2020), hace suya la

[19] http://www.acm.org/binaries/content/assets/public-policy/2017_joint_statement_algorithms.pdf

"Resolución sobre la rendición de cuentas en el desarrollo y uso de la inteligencia artificial", la cual busca promover la "fiabilidad" de las empresas que ***desarrollan y utilizan*** sistemas de IA, para que colaboren estrechamente con los responsables de la formulación de políticas públicas de los gobiernos, para resolver las preocupaciones y corregir los sesgos en materia de Derechos Humanos. Para la elaboración de la iniciativa que hoy presentamos se tomó en cuenta las recomendaciones siguientes:

(1) Evaluar el impacto potencial en los Derechos Humanos (incluidos los derechos de protección de datos y privacidad) antes del desarrollo o uso de la IA;
(2) Pruebe la robustez, fiabilidad, precisión y seguridad de los datos de la IA antes de ponerla en uso, incluida la identificación y el abordamiento del sesgo en los sistemas y los datos que utilizan que pueden conducir a resultados injustos;
(3) Mantener registros de evaluación de impacto, diseño, desarrollo, pruebas y uso de IA;
(4) Divulgar los resultados de la evaluación de impacto en la protección de datos, la privacidad y los Derechos Humanos de la IA;
(5) Garantizar la transparencia y la apertura mediante la divulgación del uso de la IA, los datos que se utilizan y la lógica implicada en la IA;
(6) Asegurar que se identifique a un actor humano responsable (a) con el que se puedan plantear preocupaciones relacionadas con decisiones automatizadas y se puedan ejercer derechos, y b) quién puede desencadenar una evaluación del proceso de decisión y la intervención humana;
(7) Proporcionar explicaciones en un lenguaje claro y comprensible para las decisiones automatizadas tomadas por la IA bajo demanda;
(8) Hacer la intervención humana sobre la decisión automatizada tomada por la IA bajo demanda;
(9) Monitorear y evaluar continuamente el desempeño y los impactos de la IA por parte de los seres humanos, y actuar con prontitud y firmeza para abordar los problemas identificados;
(10) Implementar mecanismos de denuncia/presentación de informes sobre el incumplimiento o el riesgo significativo en el uso de la IA;
(11) Garantizar la auditabilidad de los sistemas de IA y estar preparado para demostrar la rendición de cuentas ante las autoridades de protección de datos a petición;

(12) Participar en debates con múltiples partes interesadas (incluidas las organizaciones no gubernamentales, las autoridades públicas y el mundo académico) para identificar y abordar el impacto socioeconómico más amplio de la IA y garantizar la vigilancia algorítmica.

(13) Instar a las organizaciones que desarrollan o utilizan sistemas de IA a implementar medidas de rendición de cuentas que sean apropiadas con respecto a los riesgos de interferencia en los Derechos Humanos.

(14) Exhortar a todos los miembros de la Asamblea Mundial de la Privacidad a que colaboren con organizaciones que desarrollen o utilicen sistemas de IA en sus jurisdicciones y a nivel mundial para promover los principios adoptados en su resolución de 2018, y la rendición de cuentas en el desarrollo y uso de la IA, y la adopción de medidas de rendición de cuentas;

(15) Alentar a los gobiernos a considerar la necesidad de realizar cambios legislativos en las leyes de protección de datos personales, a fin de dejar claras las obligaciones legales relativas a la rendición de cuentas en el desarrollo y uso de la IA, cuando dichas disposiciones aún no estén en vigor; y

(16) Alentar a los gobiernos, a los organismos que supervisan o regulan, a las organizaciones que desarrollan o utilizan sistemas de IA y todas las demás partes interesadas pertinentes a que colaboren con las autoridades de protección de datos en el establecimiento de principios, normas y mecanismos de rendición de cuentas, como la certificación, con el fin de demostrar el cumplimiento legal, la rendición de cuentas y la Ética en el desarrollo y uso de los sistemas de IA.[20]

Para finalizar, no podemos omitir lo que Margaret Hu[21], comenta en el famoso caso *Cambridge Analytica-Facebook* (que involucró datos de millones de personas usuarias que fueron liberados y explotados sin la debida autorización) analizando una variedad de soluciones legales y políticas

[20] Cfr. XLII sesión de la Asamblea Global de Privacidad (octubre de 2020) https://globalprivacyassembly.org/document-archive/adopted-resolutions/

[21] Hu, Margaret. "Cambridge Analytica's Black Box" en *Big Data & Society*, julio 2020. https://doi.org/10.1177/2053951720938091. La autora comenta que el escándalo Cambridge Analytica-Facebook generó una preocupación generalizada sobre los métodos implementados para apuntar a los votantes a través de algoritmos de perfiles basados en datos de usuarios de Facebook. El escándalo finalmente condujo a una multa de $ 5 mil millones impuesta a Facebook por la Comisión Federal de Comercio (FTC) en julio de 2019. Sin embargo, la acción de la FTC ha sido criticada por no abordar adecuadamente la privacidad y otros daños que emanan de la liberación de Facebook de aproximadamente 87 millones de datos de usuarios de Facebook, que fueron explotados sin la autorización. El ensayo resume la respuesta de la FTC y concluye que en la necesidad de explorar "protecciones del tipo de debido proceso dentro de las acciones de aplicación de las agencias reguladoras como la FTC".

que se han propuesto para mejorar la privacidad de la información (una reforma a la Comisión Federal de Comercio e imponer requisitos procesales para respetar el debido proceso a actores privados). Carissa Véliz, profesora en la Universidad de Oxford, ubica este evento como el que nos alertó a todos en el tema de la privacidad:

> "Después del escándalo de Cambridge Analytica, y de experimentar casos de humillación pública o robo de identidad de nosotros mismos, ahora entendemos que las consecuencias de la falta de privacidad actual son tan graves como lo eran antes de que apareciera Internet. Políticamente, comprometer nuestra privacidad es más peligroso que nunca. Nunca habíamos acumulado tantos datos personales sobre ciudadanos. Y hemos permitido que la vigilancia crezca en un momento en que los estándares de ciberseguridad son deficientes, las democracias son débiles y los regímenes autoritarios con un don para la piratería están en aumento. La tecnología digital utilizó el manto de la invisibilidad de los datos para erosionar nuestra privacidad. […] Los bloqueos para esos datos no solo deben ser legales (ya que las leyes cambian y se infringen), sino también técnicos (por ejemplo, mediante cifrado) y prácticos. […] Es cuestionable que empresas privadas sean los árbitros de si una solicitud para hacer algo menos accesible tiene mérito, incluso si la decisión puede ser apelada y remitida a una Agencia de Protección de Datos."[22]

En síntesis, esta iniciativa busca que las personas sean dueñas de sus datos en entornos digitales y que las instituciones públicas que utilizan sistemas de inteligencia artificial, cuando involucren información personal o tomen decisiones automatizadas con la misma, realicen evaluaciones de impacto a sus algoritmos.

Específicamente cuando los sistemas automatizados puedan facilitar la toma de decisiones sobre aspectos sensibles de la vida de las personas mediante, como, por ejemplo, el uso de datos personales para evaluar comportamientos. Un sistema inteligente o un sistema que utiliza inteligencia artificial puede generar un impacto adverso a la privacidad de las personas cuando: 1. plantea problemas de seguridad o privacidad; 2. involucra la información personal de un número

[22] Carissa, Véliz, *Privacy is Power*, Transworld, Edición de Kindle, 2020. [La traducción fue hecha con https://translate.google.com.mx/?hl=es&sl=en&tl=es&op=translate]

significativo de personas; o 3. sistemáticamente supervisa una gran cantidad de personas con su ubicación física para determinar hábitos comerciales o de vida cotidiana.

Las evaluaciones de impacto de los sistemas de decisión automatizada de este tipo son consideradas de alto riesgo y, por tanto, deben de ser supervisadas por el Instituto como órgano facultado para garantizar y tutelar la protección de datos personales en posesión de sujetos obligados en la capital del país. Para ello, se prevén medidas de apremio y sanciones en caso de que el responsable del sistema de inteligencia artificial no atienda alguna determinación del Instituto. También se establece cómo las personas podrán hacer valer sus derechos ARCOP y el recurso de revisión para impugnar una respuesta de los sujetos obligados.

En particular la ley tiene como desafíos éticos y regulatorios en su aplicación y futura generación de política pública para la Ciudad de México:

1. Combatir la discriminación: Mediante la regulación de los sesgos existentes en los datos que se utilizan para el entrenamiento o uso de modelos de IA, los cuales pueden conducir a resultados discriminatorios para personas, grupos en situación de vulnerabilidad o determinados sectores de la economía. Por ello, tanto desarrolladores como personas usuarias deben saber que existen problemas con los datos de entrenamiento y con las inferencias de los sistemas y su correlación con ciertas variables, por ejemplo el lugar de residencia, dirección o código postal, los cuales pueden ser un indicador para que el sistema de IA haga una agrupación por zona geográfica (afiliación grupal); también existen características étnicas o de nivel socioeconómico que están presentes y que pueden impactar de forma negativa a las personas. Esto se pude corregir o mitigar mediante enfoques algorítmicos o metodológicos conducidos por un supervisor humano.
2. Supervisión humana: La ausencia de supervisión humana en el ciclo de decisión de un sistema de IA puede afectar a las personas, sobre todo cuando el algoritmo toma decisiones en temas relacionados con actividades laborales, educativas, salud, reclutamiento de personal, políticas públicas, entre otros. Esto puede generar responsabilidades para el desarrollador, la empresa, el comercializador, entre otros. Sin supervisión humana, las decisiones perjudiciales y los errores del sistema podrían pasar desapercibidos, por esta razón la ley obliga a que exista dentro de la organización un supervisor humano de los modelos de IA. A mayor nivel de autonomía, mayor nivel de supervisión y del uso de sistemas para la gestión de riesgos ya que los sistemas de IA obtienen su eficacia, en general, de la automatización.

3. Explicabilidad algorítmica: Los sistemas de inteligencia artificial se basan en modelos para hacer predicciones, generar contenido y tomar decisiones que muchas veces sustituyen a los seres humanos. Sin embargo, ocurre a menudo que la lógica de estos modelos no puede explicarse fácilmente, ni extraerse en un formato entendible por seres humanos (por eso se llaman algoritmos de "caja negra"). Los sujetos Obligados y las personas deben estar conscientes de ello y buscar algún mecanismo para transparentar el proceso de toma de decisiones basado en IA. La falta de explicabilidad de los modelos de IA puede afectar la confianza en esos sistemas al desconocer el ser humano los parámetros por los cuales el sistema de IA tomó determinada decisión.

4. Monitoreo de las decisiones que toma la IA: Los sistemas de IA se utilizan cada vez más para apoyar o asistir en la toma de decisiones humanas. Algunos sistemas de IA pueden sustituir por completo la participación del ser humano e interactuar con usuarios o clientes generando todo tipo de soluciones. Este nivel de autonomía es parte de lo que se busca para crear la Inteligencia Artificial General y puede ser posible que las personas no siempre sepan si se está utilizando un sistema de IA. Esto pone en desventaja al ser humano ante actos que pueden hacerlo responsable, en los cuales o no tiene el conocimiento para tomar decisiones o el propio sistema no le genera información necesaria para solucionar la problemática (especialmente puede generar responsabilidad legal hacia la persona más cercana al uso del sistema de IA, a grupos vulnerables o aquellos con menor alfabetización digital). Además, en algunos casos, una organización que utiliza un sistema de IA puede ocultar el uso de esta a los usuarios finales, lo que genera diversas preocupaciones (proliferación de noticias falsas y desinformación), con los consiguientes riesgos para la democracia, el Estado de Derecho o los derechos humanos. Existen también casos de uso en los que las organizaciones utilizan los datos de las personas sin su consentimiento para la manipulación a gran escala del consumidor. Esto ha sido prohibido a nivel internacional con sanciones que van desde multas hasta la suspensión de operaciones en el lugar que se dio la afectación.

5. Ciberseguridad: los sistemas de IA son susceptibles a fallas técnicas y manipulaciones intencionales de los datos de entrenamiento o del propio sistema. Esto se puede generar tanto de manera intencional o no intencional, directa o indirectamente y lleva a preocupaciones sobre la falta de precisión del sistema y su protección con herramienta que detecten ataques o manipulaciones de terceros. Se debe de requerir tanto a los desarrolladores como a los usuarios

una política de ciberseguridad básica ya sea implementada por un tercero o ya sea desarrollada internamente que siga estándares internacionales.

6. Responsabilidad algorítmica: Los marcos de responsabilidad civil y penal presuponen la agencia por parte de una persona, sin embargo, la tendencia global nos lleva a la proyección de un nuevo tipo de responsabilidad que surge de los sistemas autónomos basados en Deep Learning y otras tecnologías cuyo actuar cambia el entorno y los convierte en agentes autónomos que están cambiando el mundo sin intervención directa de los seres humanos. Si estos sistemas están utilizando datos personales para la toma de decisiones sin intervención del ser humano y sin el consentimiento de sus dueños se genera un nuevo tipo de responsabilidad denominada "responsabilidad algorítmica". Es decir, aquella que deriva del uso de algoritmos de IA que impactan de forma adversa a los derechos humanos, sin intervención de estos últimos. Esta nueva responsabilidad lleva al responsable del desarrollo, uso o despliegue de la IA a su corrección o, en su caso, a la suspensión de su desarrollo o uso. También debe ser tomada en cuenta para la imposición de sanciones por generar un impacto adverso a la privacidad y al uso de datos personales. Este tipo de responsabilidad se debe de determinar por Instituto con base en las evidencias que entreguen los Sujetos Obligados, a través de estructuras de gobernanza interna y evaluaciones periódicas de riesgos de privacidad. Dada la gran cantidad de empresas de IA en sectores regulados, es importante diseñar enfoques personalizados que en cada caso se determinarán.

7. Respeto a la privacidad de las personas: El desarrollo y uso de sistemas de inteligencia artificial requiere invariablemente de grandes cantidades de datos, algunos de los cuales tienen información personal. La recopilación y el procesamiento de información personal están regulados por leyes de protección de la privacidad que existen desde hace décadas, pero han surgido desafíos que no están en la legislación actual y que nos lleva a su regulación particular, entendiendo el contexto de la IA. Es común que los desarrolladores olviden las reglas que existen para el uso de datos personales y utilicen datos personales que no se compartieron inicialmente para ese fin. Por ello, la ley busca generar una cultura de alfabetización digital en la que se capacite sobre el uso de datos personales en sistemas de IA, siendo este un requisito obligatorio para el desarrollo o utilización de la misma. También es obligatorio que los Sujetos Obligados hagan una manifestación de cumplimiento voluntario de la legislación que protege los datos personales y la privacidad de las personas y que toda la información que se tenga previa a la entrada en vigor de

esta ley con fines de entrenamiento o uso de un sistema sea borrada o regularizada con el consentimiento de cada usuario con el fin de obligar a las organizaciones a regularizar o, en su caso, eliminar información personal. Se debe contar con un sistema de gestión de riesgos para evitar impactos a la privacidad de las personas.

Para finalizar, consideramos importante manifestar que el Instituto, como organismo constitucional autónomo, especializado, imparcial, con personalidad jurídica y patrimonio propios, con autonomía técnica y de gestión[23] cuenta con facultades para presentar esta iniciativa, ya que es el encargado de garantizar la protección y el tratamiento lícito de los datos personales y de que se respete el derecho humano a la privacidad, de conformidad con el inciso E., del artículo 7 de la Constitución Política de la Ciudad de México. En este sentido, toda información relacionada con los datos personales y la privacidad de las personas que se encuentran en la Ciudad de México y que se encuentre en posesión de sujetos obligados debe ser protegida por el Instituto, en términos y con las excepciones que establece la Constitución Federal y las leyes de la materia señalan, rigiendo los principios de veracidad, licitud, consentimiento, información, calidad, finalidad, lealtad, proporcionalidad y responsabilidad.[24]

Adicional a ello, actualmente no existe una regulación específica sobre el uso de datos para el desarrollo y utilización de modelos de inteligencia artificial, ni desde el enfoque de la Constitución Federal o desde las leyes federales que regulan a los entes obligados o a las personas (físicas y jurídicas). Esto ofrece una oportunidad única para que la Ciudad de México lidere la regulación de la IA a nivel local y a nivel América Latina, estableciendo una legislación que proteja a la población partiendo desde el ámbito de los entes públicos. No podemos imponer a las empresas cargas regulatorias, sin que primero todas las personas servidoras públicas nos preparemos para entender los tipos de inteligencia artificial que existen, sus usos, impactos positivos y negativos y, principalmente, las reglas que se deben de seguir para proteger el uso de los datos personales en posesión de sujetos obligados que estén utilizando IA.

La IA es una tecnología de carácter general que tiene una aplicabilidad transversal o multisectorial que hace difícil su regulación. La IA impulsa la innovación en diversas disciplinas del conocimiento, incrementa la productividad y la eficiencia de los mercados, facilita la creación de nuevos modelos de negocio; las empresas de todos tamaños pueden utilizarla, tiene un impacto

[23] Artículo 46, inciso A., subinciso d) de la Constitución Política de la Ciudad de México.
[24] Artículo 7, inciso E. de la Constitución Política de la Ciudad de México.

social con un potencial enorme para reducir la brecha digital, acercar los servicios públicos, lograr mayor inclusión y hacer más eficiente el uso de los recursos públicos. Aprovechemos todas estas ventajas, protegiendo la privacidad de las personas desde el sector de la administración pública tal como la Constitución de la Ciudad de México mandata.

Por lo anteriormente expuesto, se pone a consideración de este H. Congreso de la Ciudad de México la Iniciativa con proyecto de Decreto para expedir la **Ley para el uso de inteligencia artificial y el tratamiento de datos personales por sujetos obligados en la Ciudad de México**, para quedar como sigue:

Ley para el uso de inteligencia artificial y el tratamiento de datos personales por sujetos obligados en la Ciudad de México

TÍTULO PRIMERO
DISPOSICIONES GENERALES

Capítulo Único
Del objeto de la Ley

Artículo 1. La presente Ley es de orden público y de observancia general en la Ciudad de México y tiene por objeto establecer los principios, reglas y procedimientos para el uso de inteligencia artificial y el tratamiento de los datos personas por sujetos obligados.

Son sujetos obligados por esta Ley, cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo y Judicial, Órganos Autónomos, partidos políticos, fideicomisos y fondos públicos.

Artículo 2. La aplicación e interpretación de la presente Ley se realizará conforme a lo dispuesto en la Constitución Política de los Estados Unidos Mexicanos, los Tratados Internacionales de los que el Estado mexicano sea parte, la Constitución Política de la Ciudad de México, la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México, así como las resoluciones, sentencias, determinaciones, decisiones, criterios y opiniones vinculantes que emitan los órganos nacionales e internacionales especializados, favoreciendo en todo momento, la protección más amplia.

Artículo 3. Ningún sistema de IA se desarrollará o utilizará en detrimento a los derechos de las personas, por lo que los sujetos obligados garantizarán que los grupos de atención prioritaria puedan ejercer, en igualdad de circunstancias, su derecho a la protección de sus datos personales y privacidad, observando en todo momento el principio pro persona.

Artículo 4. Para garantizar el derecho que tiene toda persona al tratamiento lícito de sus datos personales, a la protección de los mismos, así como al ejercicio de los Derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad de sus datos personales para el desarrollo o utilización de inteligencia artificial, los Sujetos Obligados deberán observar las disposiciones de esta ley, así como de la Ley de Datos y demás disposiciones aplicables en la materia.

Artículo 5. Los sindicatos y cualquier otra persona física o moral que reciba y ejerza recursos públicos o realice actos de autoridad en el ámbito federal, estatal y municipal serán responsables de los datos personales que se utilicen para el desarrollo o uso de un sistema de inteligencia artificial, de conformidad con la Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados y la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, respectivamente.

Artículo 6. Para los efectos de la presente Ley se entenderá por:

I. **Aviso de Privacidad:** Documento físico, electrónico o en cualquier otro formato generado por el responsable que es puesto a disposición del o la titular, previo al tratamiento de sus datos personales, de conformidad con la Ley de Datos.

II. **Comité de inteligencia artificial:** Órgano colegiado de los sujetos obligados cuya función es determinar los impactos adversos al derecho a la privacidad de las personas que pueden surgir por el desarrollo o uso de modelos de inteligencia artificial. Los Comités de transparencia a que hace referencia el artículo 88 de la Ley de Transparencia y el responsable del despliegue de la inteligencia artificial instarán los trabajos del Comité siguiendo los lineamientos internos para su integración y funcionamiento que para tal efecto emitan.

III. **Consentimiento:** Manifestación de la voluntad del o la titular de los datos mediante la cual se efectúa el tratamiento de los mismos.

IV. **Datos abiertos:** Aquellos datos digitales de carácter público bajo los supuestos que señala el artículo 6º, fracción XIII de la Ley de Operación e Innovación Digital para la Ciudad de México.

V. **Datos biométricos:** Datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física, como imágenes faciales o datos dactiloscópicos. Los datos biométricos pueden permitir la autenticación, la identificación o la categorización de las personas físicas y el reconocimiento de las emociones de las personas físicas.

VI. **Datos de entrada:** Datos proporcionados a un sistema de IA u obtenidos directamente por él a partir de los cuales produce un resultado de salida.

VII. **Datos de entrenamiento:** Datos utilizados para entrenar un sistema de IA mediante el ajuste de sus parámetros.

VIII. **Datos de prueba:** Datos para proporcionar una evaluación independiente del sistema de IA, con el fin de confirmar el funcionamiento previsto de dicho sistema antes de su introducción en el mercado o su puesta en servicio.

IX. **Datos de validación:** Datos utilizados para proporcionar una evaluación del sistema de IA entrenado y adaptar sus parámetros no entrenables y su proceso de aprendizaje para, entre otras cosas, evitar el subajuste o sobreajuste.

X. **Datos digitales:** Cualquier tipo de información que ha sido convertida a un formato digital y puede ser procesada por sistemas computacionales o dispositivos electrónicos. Esto incluye, datos textuales, imágenes, audio, video, datos estructurados y no estructurados, y cualquier otra información almacenada, procesada o transmitida electrónicamente.

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

XII. **Datos sintéticos:** Los datos sintéticos son generados mediante simulaciones y modelado computacional para representar fenómenos reales. Permiten la generación de grandes volúmenes de datos sin información personal identificable, imitando propiedades estadísticas reales. Estos datos ayudan a entrenar modelos de IA sin comprometer la privacidad.

XIII. **Datos personales:** Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona física es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información como puede ser nombre, número de identificación, datos de localización, identificador en línea o uno o varios elementos de la identidad física, fisiológica, genética, psíquica, patrimonial, económica, cultural o social de la persona.

XIV. **Desarrolladores**: Son las personas o entidades encargadas de crear, codificar y programar los sistemas de inteligencia artificial (IA). Involucran todo el proceso desde la conceptualización hasta la implementación técnica, incluyendo el diseño del software y la integración de los componentes necesarios para que el sistema de IA funcione adecuadamente.

XV. **Distribuidores**: Son aquellos que se encargan de la comercialización de los sistemas de IA. Aseguran que los productos cumplen con las regulaciones pertinentes antes de su venta y son responsables de la logística de distribución del producto final al consumidor o usuario final.

XVI. **Envenenamiento de datos:** Ataques que tratan de manipular al conjunto de datos que utiliza el modelo de inteligencia artificial o los componentes entrenados previamente utilizados en el entrenamiento, así como la generación de alucinaciones a través de la entrada de información diseñada para hacer que el modelo de inteligencia artificial comenta errores o salga de los parámetros establecidos.

XVII. **Gestión de riesgos de privacidad:** Actividad que busca asegurar que los sistemas de IA operen de manera que se proteja la privacidad de las personas en todo momento, integrando prácticas como la anonimización de datos, el cifrado y controles de acceso, entre otros, para minimizar los riesgos identificados.

XVIII. **Grupos de atención prioritaria**: Personas y colectivos que debido a la desigualdad estructural enfrentan discriminación, exclusión, maltrato, abuso, violencia y mayores obstáculos para el pleno ejercicio de sus derechos y libertades fundamentales, razón por lo cual se les debe garantizar una atención prioritaria.

XIX. **Identificación biométrica:** Reconocimiento automatizado de características humanas de tipo físico, fisiológico, conductual o psicológico que permite determinar la identidad de una persona física comparando sus datos biométricos con los datos biométricos de otras personas almacenados en una base de datos.

XX. **Incidentes:** Cualquier anomalía que afecte o pudiera afectar la seguridad de los datos personales.

XXI. **Inmovilización del sistema de inteligencia artificial:** Medida cautelar que consiste en la interrupción temporal en el uso de un sistema de inteligencia artificial ordenada por el Instituto en los supuestos de tratamiento ilícito de datos de carácter personal.

XXII. **Instituto o INFO CDMX:** Instituto de Transparencia, Acceso a la Información Pública, Protección de Datos Personales y Rendición de Cuentas de la Ciudad de México.

XXIII. **Inteligencia Artificial o IA:** Conjunto de tecnologías que funcionan a través de elementos interrelacionados que generan percepción, cognición, planificación, aprendizaje, comunicación o acción física similares a las humanas; y tecnologías de software, a veces hardware, que pueden aprender, crear conocimiento y actuar de forma autónoma, ya sea en forma de agentes de software o robots incorporados.

XXIV. **Interoperabilidad:** La capacidad de diferentes sistemas de IA y bases de datos para comunicarse, intercambiar datos y utilizar la información que ha sido intercambiada de manera licita, efectiva y coherente.

XXV. **Ley: Ley para el uso de inteligencia artificial y el tratamiento de datos personales por sujetos obligados en la Ciudad de México**.

XXVI. **Ley de Datos:** Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

XXVII. **Ley de transparencia:** Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

XXVIII. **Medidas de seguridad:** Conjunto de acciones, actividades, controles o mecanismos administrativos, técnicos y físicos que permitan proteger los datos personales y los sistemas de datos personales.

XXIX. **Minimización de datos:** El principio que establece que sólo deben recogerse y procesarse los datos personales que sean estrictamente necesarios para cumplir con un propósito específico y legítimo de un sistema de inteligencia artificial.

XXX. **Modelos de IA:** Representación matemática de un proceso de aprendizaje automático, aprendizaje profundo o inteligencia artificial generativa, que ha sido entrenada con datos y es capaz de realizar predicciones o tomar decisiones o crear nuevos conceptos. Los modelos de IA ejecutan tareas de predicción, clasificación y regresión. Los modelos de IA se desarrollan y se entrenan utilizando datos para crear patrones, relaciones o nuevos conceptos.

XXXI. **Privacidad desde el diseño y defecto:** Los modelos de inteligencia artificial deben tener una capa que los configure para ofrecer el máximo de privacidad de tal forma que el usuario no requiera tomar medidas adicionales para proteger sus datos personales, sino que dicha protección esté garantizada desde antes que se ponga en producción en un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva.

XXXII. **Procesamiento de datos:** Aquellas acciones de programación, con intervención o sin intervención humana, que permiten el desarrollo o utilización de un modelo de inteligencia artificial.

XXXIII. **Programadores**: Son los técnicos especializados en escribir, probar y mantener el código que constituye parte de los sistemas de IA. Su trabajo es esencial para el desarrollo de software y la ejecución eficiente de los sistemas de inteligencia artificial.

XXXIV. **Proveedores**: Se refieren a las entidades o individuos que suministran los sistemas de IA o sus componentes al mercado. Pueden ser también quienes ofrecen la tecnología necesaria para operar estos sistemas, incluyendo software y hardware. En algunos contextos, los proveedores son quienes ponen a disposición los sistemas de IA para su uso por terceros, responsabilizándose de mantener la funcionalidad y cumplimiento normativo del producto.

XXXV. **Reconocimiento de emociones:** Se refiere a emociones o intenciones como la felicidad, la tristeza, la indignación, la sorpresa, el asco, el apuro, el entusiasmo, la vergüenza, el desprecio, la satisfacción y la diversión que son detectados por sistemas de IA. No incluye los estados físicos, como el dolor o el cansancio. Tampoco incluye la mera detección de expresiones, gestos o movimientos que resulten obvios, salvo que se utilicen para distinguir o deducir emociones. Esas expresiones pueden ser expresiones faciales básicas, como un ceño fruncido o una sonrisa; gestos como el movimiento de las manos, los brazos o la cabeza, o características de la voz de una persona, como una voz alzada o un susurro. El reconocimiento de emociones sólo

está permitido cuando el dueño de los datos personales autoriza expresamente su consentimiento para su uso por los sujetos obligados.

XXXVI. **Responsable del despliegue de la inteligencia artificial:** Persona que utilice un modelo de inteligencia artificial por la función que realiza dentro del sujeto obligado, ya sea por decisión propia o a petición de un tercero y sobre la que recae la responsabilidad de asegurarse que los datos de entrada y salida respeten la privacidad de las personas, documentando las incidencias y solicitando, en su caso, la implementación de auditorías algorítmicas o acciones preventivas para evitar un impacto adverso al principio de privacidad.

XXXVII. **Responsable:** Aquellos que señala la fracción XXVIII, del artículo 3 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

XXXVIII. **Seguridad de la IA:** Los sistemas de IA se desarrollan y utilizan de manera que sean consistentes con los problemas que resuelven y resilientes frente a los intentos de alterar su uso o el funcionamiento para evitar su uso ilícito por terceros y reducir al mínimo los daños no deseados.

XXXIX. **Sesgos algorítmicos:** Aquellos producidos por personas, al momento de ingresar información al modelo de inteligencia artificial o por el propio modelo de inteligencia artificial al momento de procesar las entradas y salidas y cuyo resultado impacta de forma adversa a la privacidad, entendida esta como un derecho humano.

XL. **Sistema de IA:** Es una combinación de software y, en ocasiones, hardware que implementa uno o más modelos de IA. Un sistema de IA incluye una interfaz de usuario, los mecanismos de recopilación y procesamiento de datos y cualquier otro componente necesario para que la persona interactúe con el sistema en un contexto práctico, profesional o de vida cotidiana.

XLI. **Sujetos obligados:** Cualquier autoridad, entidad, órgano y organismo de los Poderes Ejecutivo, Legislativo, Judicial, órganos autónomos, partidos políticos, fideicomisos y fondos públicos de la Ciudad de México.

XLII. **Titular:** La persona física a quien corresponden los datos personales.

XLIII. **Toma de decisiones automatizadas:** Las decisiones automatizadas que puedan afectar significativamente los derechos y libertades de las personas deben ser revisables por un humano, y las personas deben tener el derecho a impugnar dichas decisiones y obtener explicaciones sobre el proceso.

XLIV. **Tratamiento:** El registro, estructuración, resguardo, adaptación, modificación, extracción, consulta, utilización, transmisión, difusión o entrenamiento que realizan los sujetos obligados con los datos personales o conjuntos de datos personales mediante el desarrollo o uso de modelos de inteligencia artificial.

XLV. **Unidad de transparencia:** Instancia a la que hace referencia la Ley de Transparencia, Acceso a la Información Pública y Rendición de Cuentas de la Ciudad de México.

TÍTULO SEGUNDO
PRINCIPIOS PARA GARANTIZAR UNA INTELIGENCIA ARTIFICIAL RESPONSABLE

Capítulo Único
Principios rectores de una IA responsable

Artículo 7. Para considerar que una inteligencia artificial es responsable con la privacidad de las personas en ambientes digitales, los sujetos obligados, dependiendo el sistema de IA o modelo de IA, deben verificar que se cumplan los siguientes principios rectores:

Ciberseguridad: Los sujetos obligados deben implementar medidas de ciberseguridad para proteger de las amenazas a los modelos de inteligencia artificial que utilicen para evitar una afectación a los datos personales; en particular, contra accesos o usos no autorizados, manipulación o la generación de alucinaciones. Esto incluye la implementación de estándares internacionales de ciberseguridad que no sean contrarios al sistema jurídico nacional.

Consentimiento de titulares de los datos: Las personas titulares de los datos deben ser informadas de manera clara y comprensible sobre cómo se utilizarán sus datos personales en modelos de inteligencia artificial mediante el aviso de privacidad respectivo y deben otorgar su consentimiento de manera libre y explícita antes de que sus datos sean procesados por sistemas de IA. Esta es una responsabilidad compartida que deberán cumplir los sujetos obligados, los responsables del despliegue de la inteligencia artificial, proveedores, distribuidores, programadores y todo aquel que pretenda utilizar datos personales para realizar alguna actividad con el gobierno de la Ciudad de México, para lo cual se sujetarán a las leyes en materia de datos personales respectivas. El consentimiento informado no da derecho al uso para fines comerciales, sin que medie un acuerdo de voluntades para tal fin.

Finalidad: Sólo se deben recolectar y procesar aquellos datos personales que sean estrictamente necesarios, adecuados y relevantes para la realización de la finalidad o finalidades para los cuales se obtuvieron y se ingresaron al modelo de inteligencia artificial. La finalidad de los datos ayuda a reducir los riesgos asociados con un mal uso, recopilación o almacenamiento que no sean compatibles.

No discriminación: Se deben implementar medidas para evitar que los modelos de inteligencia artificial reproduzcan o incrementen los sesgos que se producen en nuestra sociedad. Esto obliga al responsable del despliegue de la inteligencia artificial a la verificación del uso de los datos de entrenamiento y la aplicación de técnicas para minimizar sesgos algorítmicos; en particular, cuando se trate de datos de personas pertenecientes a los grupos de atención prioritaria, como son mujeres, personas mayores, personas no binarias, personas con discapacidad, niñas, niños y adolescentes.

Responsabilidad: Los sujetos obligados que implementan o utilizan modelos de inteligencia artificial deben asumir la responsabilidad de sus decisiones. Esto implica la implementación de

políticas y procedimientos para la gestión de riesgos que impacten de forma negativa a la privacidad y la realización de auditorías algorítmicas.

Transparencia: El responsable del despliegue de la inteligencia artificial deberá verificar con un portafolio de evidencias que las decisiones tomadas por los algoritmos que utilizan los modelos de inteligencia artificial sean posibles de explicar a los titulares de los datos. Esto incluye proporcionar información sobre cómo se utilizan los datos personales, el tipo de algoritmos que utiliza y la trazabilidad de los datos.

Privacidad desde el diseño y defecto: Los sujetos obligados que implementen o utilicen modelos de inteligencia artificial deben garantizar la máxima privacidad, de manera que el usuario no necesite tomar medidas adicionales para proteger sus datos personales. Esta protección debe estar asegurada desde antes de la puesta en producción, con un enfoque orientado a la gestión del riesgo y la responsabilidad proactiva.

Artículo 8. Además de los principios rectores mencionados, se deberán considerar para la imposición de sanciones los siguientes principios adicionales:

Auditabilidad: Los responsables del despliegue de la inteligencia artificial deben programar la implementación de auditorías algorítmicas como parte del procedimiento para la gestión de riesgos de privacidad y la revisión de los modelos de inteligencia artificial, para corroborar el origen lícito de los datos de entrenamiento, el tipo de inteligencia artificial que se utiliza o desarrolla y las decisiones que toma, con el fin de garantizar que no impacta de forma adversa a la privacidad de las personas.

Evaluación de impactos adversos a la privacidad: Informe que se genera como resultado de la implementación de sistemas de gestión de riesgos de privacidad y de un plan de inteligencia artificial, que periódicamente se somete a auditorías algorítmicas, para valorar los impactos adversos al tratamiento de datos personales.

Interoperabilidad: Los sistemas de IA deben diseñarse para ser interoperables con otros sistemas y bases de datos, facilitando el intercambio seguro y eficiente de datos personales entre diferentes plataformas ya sea que se utilicen mediante códigos de fuentes abiertas o códigos de fuentes cerradas. Los sujetos obligados en la Ciudad de México deben generar estándares y técnicas de colaboración e intercambio de datos con la finalidad de agilizar procesos, ahorrar recursos y aprovechar la información para trámites, servicios y análisis de datos de conformidad con la Ley de Operación e Innovación Digital para la Ciudad de México.

Supervisión humana: Debe existir una supervisión humana efectiva en el ciclo de vida de los modelos de inteligencia artificial, especialmente cuando el grado de autonomía permita tomar decisiones sin intervención del ser humano o cuando esté creado para sustituir al ser humano en la toma de decisiones. Esta supervisión garantiza que el responsable del despliegue de la inteligencia artificial y, en su caso, el sujeto obligado pueda gestionar riesgos, corregir errores y prevenir sesgos. La aplicación de esos principios debe traducirse, cuando sea posible, en el diseño y el uso

de modelos y sistemas de IA. En cualquier caso, deben servir de base para la elaboración de códigos de conducta en los sujetos obligados.

Transparencia algorítmica: Los sistemas de IA se desarrollan y utilizan de un modo que permita una trazabilidad y explicabilidad adecuadas a la persona o grupos de personas que se sientan afectados en sus derechos humanos, dignidad, democracia, estado de Derecho o medio ambiente, y que, al mismo tiempo, haga que las personas sean conscientes de que se comunican o interactúan con un sistema de IA e informe debidamente a los responsables del despliegue sobre las capacidades y limitaciones de dicho sistema de IA y a las personas afectadas acerca de sus derechos.

TÍTULO TERCERO
MODELOS, TIPOS Y USOS DE LA IA

Capítulo I
Modelos de Inteligencia Artificial

Artículo 9. Son modelos de inteligencia artificial:

a) Supervisada

Modelos de IA entrenados con datos etiquetados, donde el sistema aprende a partir de ejemplos específicos para realizar predicciones o clasificaciones.

b) No supervisada

Modelos de IA que analizan datos no etiquetados para identificar patrones y relaciones subyacentes sin supervisión humana directa.

c) Semi-supervisada

Combinación de enfoques supervisados y no supervisados, donde los modelos se entrenan con una mezcla de datos etiquetados y no etiquetados.

d) Aprendizaje por refuerzo

Un tipo de IA donde los sistemas aprenden a tomar decisiones mediante la interacción con un entorno dinámico, recibiendo recompensas o castigos en función de sus acciones y resultados.

Capítulo II
Tipos de Inteligencia Artificial

Artículo 10. Son tipos de inteligencia artificial:

a) Estrecha o débil: Modelos diseñados y entrenados para realizar tareas específicas. Estos sistemas no tienen capacidades de razonamiento general y sólo pueden ejecutar las tareas para las que fueron programados. Ejemplos incluyen asistentes virtuales, sistemas de recomendación y programas de reconocimiento de voz y texto.

b) General o fuerte: Modelos con capacidades de razonamiento general similares a las de un ser humano. Estos sistemas pueden realizar cualquier tarea intelectual que un humano pueda, aunque actualmente no existe una IA general completamente funcional.

c) Generativa: Sistemas diseñados para crear contenido, como texto, imágenes, videos, código o audio, a partir de datos que son ingresados por los usuarios.

Capítulo III
Usos de la Inteligencia Artificial

Artículo 11. Usos de la inteligencia artificial

Para la gestión de riesgos de privacidad, los sujetos obligados deberán tomar en cuenta el tipo de uso de sistemas o modelos de inteligencia artificial, el sector al que va dirigido, así como su impacto al principio de privacidad.

Las personas físicas o morales que participen en alguna contratación pública que tenga como finalidad el desarrollo o uso de algún modelo de inteligencia artificial por los sujetos obligados, deberán de demostrar durante el proceso de contratación , que cubren con los principios para el tratamiento de datos personales. Para al fin y como requisito que se incluirá en la convocatoria y cuerpo de los contratos, deberán entregar una Declaración de cumplimiento. Es responsabilidad de los sujetos obligados verificar este requisito, previo a la contratación del servicio en los siguientes supuestos:

a) Buena administración pública: Uso de sistemas de inteligencia artificial para lograr una buena administración pública, siempre y cuando garanticen la protección de los datos personales, así como la mejora de políticas públicas o la implementación de programas en los que los sujetos obligados justifiquen su desarrollo o utilización, mediante una manifestación de no impacto adverso al derecho a la privacidad. La expedición de esta manifestación, se hará a través de la Agencia Digital de Innovación Pública en auditorías algorítmicas y a petición del proveedor, distribuidor o del propio sujeto obligado.

b) Ciudad educadora y del conocimiento: Uso de sistemas de inteligencia artificial para actividades educativas, de investigación académica, capacitación o innovación tecnológica. Este tipo de aplicaciones sólo podrán contratarse o desarrollarse si el proveedor, distribuidor o el propio sujeto obligado hacen una manifestación de no impacto a la privacidad comprobada mediante una auditoría algorítmica. Tratándose de actividades en donde participen niñas o niños y adolescentes, deberá tenerse en cuenta el interés superior de la niñez como eje para la contratación, desarrollo o uso de modelos de inteligencia artificial.

c) Seguridad pública, procuración y administración de justicia: Uso de sistemas de inteligencia artificial para actividades de seguridad pública, procuración y administración de justicia. En estos casos, los sujetos obligados, deberán emitir una regulación específica y entregar anualmente al Instituto un informe sobre casos en donde se vulneró el derecho a la privacidad con motivo de acciones o investigaciones derivadas de sus atribuciones.

TÍTULO CUARTO
TRANSPARENCIA ALGORÍTMICA

Capítulo I
Transparencia de los datos de entrenamiento

Artículo 12. Cuando los sujetos obligados utilicen datos personales para el entrenamiento de sus modelos de IA y con el fin de generar confianza y transparencia a las personas, cuando así lo requiera el Instituto, deberán proporcionar información sobre:

a) Tamaño del conjunto de datos: La cantidad total de datos utilizados para entrenar el modelo.
b) Fuente de los datos: El origen de los datos recopilados, especificando si son datos abiertos, compartidos o privados.
c) Creadores de los datos: Información sobre las personas que crearon los datos y cómo fueron creados.
d) Propósito de la creación: Explicación del objetivo detrás de la creación y el uso de los datos.

e) **Filtros aplicados:** Descripción de los filtros de contenido nocivo, discriminatorio u ofensivo en el conjunto de datos.
f) **Datos con derechos de autor:** Declaración sobre la inclusión de datos con derechos de autor y las licencias correspondientes.
g) **Información personal:** Identificación de cualquier información personal contenida en los datos y medidas para su protección.

Artículo 13. Los sujetos obligados que utilicen datos personales para el entrenamiento de sus modelos de IA deben contar con un registro que concentre los conjuntos de datos utilizados para entrenamiento, revisión y validación de los modelos de IA. Está información deberá estar a disposición del Instituto en cualquier momento que este lo requiera. El archivo debe contener:

a) **Descripción del conjunto de datos:** Resumen comprensible del contenido y características del conjunto de datos.
b) **Métodos de recolección:** Descripción de los métodos utilizados para recolectar y procesar los datos.
c) **Licencias y permisos:** Información sobre las licencias y permisos asociados con los datos utilizados.
d) **Medidas de protección de datos**: Explicación de las medidas implementadas para proteger la privacidad y ciberseguridad de los datos personales.

Capitulo II

Intercambio de datos y herramientas de valor

Artículo 14. Para maximizar el valor social y económico del intercambio de datos, los sujetos obligados, con las medidas de seguridad apropiadas a fin de no vulnerar la privacidad de las personas, deben:

a) Facilitar el intercambio de datos y la interconexión para abordar desafíos sociales, económicos y ambientales.
b) Promover el uso de datos abiertos para fomentar la innovación y el desarrollo de la Ciudad de México.
c) Utilizar las herramientas que la Agencia Digital de Innovación Pública de la Ciudad de México proponga.

Artículo 15. Los sujetos obligados, en la medida de sus posibilidades técnicas y presupuestarias, implementarán herramientas y marcos que permitan:

a) Evaluar cómo el intercambio de datos puede generar valor para una buena administración pública y para la sociedad.

b) Identificar y cuantificar los beneficios económicos y sociales del intercambio de datos.
c) Desarrollar estrategias de gobierno y políticas públicas para maximizar el valor derivado del intercambio de datos.

Artículo 16. Para fomentar el uso de un ecosistema de datos el Instituto, en coordinación con la Agencia Digital de Innovación Pública y los sujetos obligados, deberán:

a) Garantizar el acceso a datos públicos para entrenar modelos de IA, asegurando que estos datos sean de alta calidad y estén bien documentados.
b) Facilitar el acceso a datos privados mediante acuerdos de intercambio de datos que respeten los derechos de propiedad intelectual y la privacidad de las personas.
c) Desarrollar y mantener una infraestructura de datos que permita el acceso equitativo y responsable a datos críticos para el desarrollo de IA.

Capítulo III
Carpetas de evidencias

Artículo 17. Los sujetos obligados que desarrollen, implementen o utilicen sistemas de inteligencia artificial deben asegurar que la recolección y uso de datos personales se realice de manera lícita y transparente. La carga de la prueba corresponde siempre al proveedor, distribuidor, comercializador o sujeto obligado, quienes deberán integrar una carpeta de evidencias con los siguientes documentos:

a) Carpeta de evidencias que permita demostrar que los datos personales fueron obtenidos con el consentimiento explícito, libre e informado de las y los titulares de los datos personales antes de recolectarlos y utilizarlos en sistemas de IA.
b) Carpeta de evidencias que permita demostrar que la recopilación y utilización de los datos personales se hizo para fines específicos, explícitos y legítimos, evitando cualquier uso incompatible con sus funciones o facultades.
c) Carpeta de evidencias en la que se demuestre que la recolección de datos personales se hizo siguiendo el plan de IA del sujeto obligado y los estándares de protección a la privacidad que el Comité de IA haya aprobado.

Capítulo IV
Evaluaciones de transparencia algorítmica

Artículo 18. Verificación del cumplimiento de la ley

El Instituto podrá realizar evaluaciones de transparencia algorítmica para verificar el cumplimiento de esta Ley y publicará informes anuales con sus hallazgos de tal forma que los sujetos obligados pueden conocer sobre el uso de buenas prácticas.

TÍTULO QUINTO
GOBERNANZA DE LA INTELIGENCIA ARTIFICIAL

Capítulo I
Del ciclo de vida de los datos

Artículo 19. Los sujetos obligados deberán adoptar principios de gobernanza de datos a lo largo del ciclo de vida de la IA, que incluyan:

a) Responsabilidad y transparencia: Asegurar la responsabilidad y transparencia en la recolección, uso y gestión de datos.
b) Privacidad y seguridad: Implementar medidas robustas de privacidad y seguridad para proteger los datos personales utilizados en el desarrollo y operación de sistemas de IA.
c) Ética y justicia: Garantizar que los sistemas de IA se desarrollen y operen de manera ética y justa, evitando sesgos y discriminación.

Artículo 20. Los datos sintéticos deben ser generados y utilizados, en la medida de lo posible, para asegurar que cumplen con las normativas de protección de datos, además de explicar su papel en la minimización de riesgos de privacidad y en el entrenamiento de modelos de IA sin utilizar datos personales.

La generación de datos sintéticos debe seguir estándares que aseguren su calidad y representatividad, evitando sesgos que puedan trasladarse al comportamiento de los sistemas de IA. El uso de datos sintéticos debe estar sujeto a auditorías regulares para verificar la adhesión a las normativas de privacidad y ética. Los resultados de estas auditorías deben ser accesibles para las autoridades competentes y, en un formato adecuado, al público general.

Capítulo II
Ciclo de vida de la gobernanza

Artículo 21. La gobernanza de datos debe aplicarse en todas las etapas del ciclo de vida de los datos, incluyendo:

a) **Recolección de datos**: Adoptar prácticas responsables y éticas en la recolección de datos.

b) **Almacenamiento y gestión:** Asegurar que los datos se almacenen y gestionen de manera segura y eficiente.
c) **Uso y compartición:** Regular mediante un manual de políticas y procedimientos el uso y la compartición de datos para garantizar la conformidad con las leyes y regulaciones vigentes.
d) **Eliminación y retención:** Establecer políticas claras para la eliminación y retención de datos, asegurando que los datos no se conserven más allá de lo necesario y de acuerdo a las finalidades señaladas en el aviso de privacidad.

Capítulo III
Gobernanza y fomento a la innovación

Artículo 22. El Instituto, en coordinación con los sujetos obligados, promoverá un entorno para la innovación basado en los siguientes ejes de política pública:

a) Establecer lineamientos claros y confiables para la publicación y el acceso a datos abiertos que faciliten su intercambio y la reutilización para investigación y el desarrollo de IA, sin que se afecte el derecho a la privacidad de las personas.

b) Implementar políticas de uso de la IA sin un perfilamiento social que genere manipulación, inequidad o discriminación.

TÍTULO SEXTO
RESPONSABILIDAD ALGORÍTMICA

Capítulo I
Elementos y atenuantes de responsabilidad algorítmica

Artículo 23. La responsabilidad algorítmica se produce cuando se agrupan las siguientes causales:

a) Una persona tiene a su disposición un sistema de IA para la toma decisiones;
b) Las decisiones del sistema se toman a través de sus propios modelos algorítmicos, sin la participación de la persona que la tiene a su disposición;
c) El sistema de IA modifica las circunstancias de la persona que la tiene a su disposición o de su entorno, la sociedad o el medioambiente;
d) La modificación de las circunstancias impacta de forma adversa a sus derechos humanos;
e) Derivado del uso indebido de datos personales en alguna etapa del ciclo de vida del sistema de IA.

La responsabilidad algorítmica por el desarrollo, implementación y uso de sistemas de IA puede ser compartida entre las partes interesadas, incluyendo desarrolladores, proveedores de servicios, distribuidores, empleados de los anteriores; usuarios finales, sujetos obligados, el responsable del

despliegue de la IA o cualquier persona que haya hecho uso de la IA sin tomar las medidas necesarias de prevención.

Artículo 24. Para atenuar o deslindarse de la responsabilidad algorítmica, las personas responsables, deberán demostrar que se realizaron todas las acciones necesarias para cumplir con los siguientes principios:

a) Explicabilidad: Capacidad de explicar en términos del lenguaje sencillo y ciudadano, cómo y por qué se tomó una decisión específica por un modelo de IA. Incluye la capacidad de desglosar y describir los procesos internos de la IA, ofreciendo una transparencia completa de las decisiones.

b) Gobernanza: Conjunto de políticas, procesos y procedimientos implementados para supervisar el desarrollo y utilización de sistemas de inteligencia artificial dentro de una organización o en la sociedad. El objeto de la gobernanza en el ámbito de la privacidad se centra en asegurar que la recolección, almacenamiento, uso y transmisión de información personal se realice de manera segura, ética y conforme a la ley.

c) Interpretabilidad: Se refiere a la facilidad con la que las personas pueden entender el proceso de toma de decisiones de un modelo de IA. Un modelo es interpretable cuando él o la observadora externa puede comprender cómo el modelo procesa sus entradas para llegar a sus salidas. Un modelo interpretable ofrece una visión general del razonamiento detrás de sus decisiones, pero no necesariamente explica cada detalle de su proceso interno.

d) Rendición de cuentas: Los sujetos obligados que desarrollen o utilicen modelos de inteligencia artificial deben ser capaces de rendir cuentas sobre las decisiones y resultados generados por estos sistemas. Esto incluye la obligación de proporcionar explicaciones claras y comprensibles sobre el funcionamiento de los algoritmos y de sus decisiones. Para ello deberán implementar un sistema de gestión de riesgos de privacidad y un plan de IA que periódicamente sea auditado con alguna metodología reconocida y cuyos resultados se plasmen en un informe hecho por un externo certificador.

e) Supervisión humana: Las decisiones automatizadas que puedan tener un impacto significativo en la privacidad de las personas deben ser revisables en todo momento por un ser humano. Los modelos de inteligencia artificial deben contar con supervisión humana en todas las etapas críticas de su operación.

Capítulo II
Responsabilidad algorítmica de proveedores y distribuidores

Artículo 25. Los modelos de inteligencia artificial deben ser diseñados y desarrollados de acuerdo con el principio de privacidad por diseño y defecto, cuidando que no se genere una responsabilidad algorítmica. Para tal fin, se deberá tomar en cuenta que todo sistema de IA que se comercialice con un sujeto obligado deberá:

a) **Evaluar el impacto algorítmico:** Antes de poner en producción cualquier modelo de inteligencia artificial por un sujeto obligado, los desarrolladores y el responsable del despliegue deberán realizar una evaluación de impacto algorítmico para identificar y mitigar posibles riesgos a la privacidad.

b) **Documentar y registrar:** Mantener documentación detallada y registros de todas las etapas del desarrollo del modelo de inteligencia artificial, incluyendo los datos de entrenamiento utilizados, los tipos de algoritmos implementados, las pruebas realizadas para validar su funcionamiento, así como la metodología para la generación de auditorías algorítmicas.

c) **Implementar auditorías algorítmicas:** Los sujetos obligados deben someter los modelos de inteligencia artificial a auditorías algorítmicas periódicas, las cuales estarán a cargo de la Agencia Digital de Innovación Pública, para garantizar la imparcialidad y objetividad en el cumplimiento de los principios contenidos en esta ley.

d) **Implementar herramientas de ciberseguridad:** Implementar medidas de ciberseguridad para proteger los datos personales utilizados por los modelos de inteligencia artificial, incluyendo el uso de herramientas de ciberseguridad.

Capítulo III
Política de Inteligencia Artificial en sujetos obligados

Artículo 26. Los sujetos obligados que utilicen IA deberán contar con una política transversal cuyos lineamientos contemplen acciones previas y posteriores al desarrollo o uso de sistemas de IA y con la cual el responsable del despliegue de la IA tenga la posibilidad de gestionar los riesgos de privacidad mediante un sistema automatizado acorde a las necesidades de cada unidad administrativa y con el cual se generen alertas y reportes para proteger la privacidad de las personas. Para que la política de IA de los sujetos obligados sea transversal deberán contar con:

a) Comité de IA;
b) Código de conducta para el uso responsable de la IA;
c) Programa de capacitación;
d) Metodología básica para la gestión de riesgos de privacidad;
e) Sistema de gestión de riesgos de privacidad; y,
f) Procedimiento para protección de la privacidad desde el diseño y defecto y respuesta a incidentes.

Artículo 27. Antes de implementar sistemas de IA que impliquen el tratamiento de datos personales, los sujetos obligados deberán realizar evaluaciones de impacto a la privacidad. Estas evaluaciones deben permitir:

a) Identificar y evaluar los riesgos potenciales a la privacidad y los derechos de las y los titulares de los datos.
b) Proponer medidas para mitigar los riesgos identificados, asegurando que los sistemas de IA cumplan con los principios de privacidad por diseño y por defecto.

c) Registrar los resultados de los datos de prueba y las medidas de corrección para mitigar los riesgos y permitir su entrada en ambiente de producción.

TÍTULO SÉPTIMO
GESTIÓN DE RIESGOS DE PRIVACIDAD

Capítulo I
Identificación de riesgos

Artículo 28. Los sujetos obligados deberán desarrollar una metodología para la gestión de riesgos de privacidad que, por lo menos permita identificar, evaluar y mitigar el impacto adverso de los sistemas de IA.

El Instituto, fungirá como un órgano consultivo para determinar si el tipo de inteligencia artificial que se utiliza por los sujetos obligados debe ser sometida a una gestión de riesgos para evitar impactos adversos al derecho a la privacidad de las personas.

Artículo 29. Como medida preventiva, los sujetos obligados deberán evaluar la calidad, integridad y representatividad de los datos utilizados para entrenar y operar los sistemas de IA, identificando posibles sesgos y errores que puedan influir en los resultados. En caso de que esto corresponda a los proveedores, el sujeto obligado deberá pedir una constancia o manifestación de no impacto adverso a la privacidad y el compromiso de que la gestión de riesgos se realiza periódicamente.

Artículo 30. Deberán identificar, permanentemente, los posibles impactos adversos a la privacidad de las personas durante todo el ciclo de vida de un sistema de IA, incluyendo posibles ataques cibernéticos, envenenamiento de datos, accesos no autorizados o pérdida de datos.

Capítulo II

Evaluación de sistemas de IA

Artículo 31. Los sujetos obligados deberán analizar cómo el sistema de IA afectará la privacidad de las personas, incluyendo la recopilación, almacenamiento, procesamiento y uso de datos personales.

Articulo 32. Evaluarán los modelos de IA que utilizan los sistemas, en colaboración con sus proveedores o desarrolladores, considerando su diseño, funcionamiento y las posibles implicaciones éticas o legales, en particular, aquellas que suplan decisiones humanas.

Artículo 33. Los sujetos obligados deberán evaluar las vulnerabilidades de seguridad del sistema de IA, incluyendo posibles ataques cibernéticos, envenenamiento de datos, accesos no autorizados o pérdida de datos.

Capítulo III

Mitigación de riesgos

Artículo 34. Los sujetos obligados deberán mitigar los riesgos relacionados con el uso de datos personales que deriven del desarrollo o utilización de sistemas de IA, incluyendo posibles ataques cibernéticos, envenenamiento de datos, accesos no autorizados o pérdida de datos, por lo que el responsable del despliegue o el proveedor del sistema de IA realizarán acciones relacionadas con la implementación de:

Medidas técnicas: Adoptar tecnologías y prácticas que minimicen los riesgos identificados, como técnicas de anonimización, cifrado de datos y controles de acceso.

Medidas organizativas: Establecer una política de IA y los lineamientos internos que promuevan el uso responsable y ético de los sistemas de IA, incluyendo la formación y capacitación del personal.

Medidas regulatorias: Cumplir con todas las normativas y estándares de gestión de riesgos aplicables para cumplir la política de IA, y colaborar con el Instituto para asegurar el cumplimiento de las leyes en materia de privacidad y uso de datos personales.

Medidas de supervisión y control: Implementar mecanismos de supervisión y control para monitorear el desempeño y los impactos de los sistemas de IA en tiempo real, así como ajustar la política de IA y los procedimientos internos.

TÍTULO OCTAVO
AUDITORÍAS ALGORÍTMICAS

Capítulo I

Objeto y alcances

Artículo 35. Las auditorías algorítmicas tienen como objetivo garantizar que los sistemas o modelos de IA operen de manera transparente, justa, segura y conforme a los principios establecidos en esta ley. Estas auditorías buscan identificar y corregir posibles exrrores, sesgos y vulnerabilidades en los sistemas de IA que impacten de forma adversa a la privacidad de las personas y el uso de sus datos.

Los sujetos obligados deberán realizar auditorías algorítmicas periódicas para evaluar su política de IA, procesos o procedimientos internos. Estas se llevarán a cabo por la Agencia Digital de Innovación Pública de la Ciudad de México. Los resultados de las auditorías deben ser documentados y publicados de manera transparente, permitiendo el acceso a la información a todas las personas.

Artículo 36. Las auditorías algorítmicas, con el fin de proteger el derecho humano a la privacidad, tendrán como mínimo el siguiente alcance técnico:

a) Datos de entrenamiento: Evaluar la calidad, integridad y representatividad de los datos utilizados para entrenar los modelos de IA, asegurando que no contengan sesgos ni errores que puedan afectar los resultados.

b) Algoritmos y modelos: Revisar los algoritmos y modelos utilizados, incluyendo su diseño, implementación y funcionamiento, para asegurar que operen de manera justa y equitativa.

c) Resultados y decisiones: Analizar las decisiones generadas por los sistemas de IA y su impacto en las personas, identificando posibles impactos en su privacidad y datos personales.

d) Medidas de seguridad: Evaluar las medidas de seguridad implementadas para proteger los datos personales y garantizar la integridad y confidencialidad del sistema de IA.

Capítulo II

Transparencia y publicación de resultados

Artículo 37. Para fomentar la confianza y la transparencia, los resultados de las auditorías algorítmicas deben ser publicados y accesibles a las personas, en este sentido, los sujetos obligados deberán publicarlos en la Plataforma Nacional de Transparencia y en su portal de Internet.

Capítulo III.

Revisión, mejora y responsabilidad de cumplimiento

Artículo 38. Los sujetos obligados utilizarán los hallazgos de las auditorías algorítmicas para corregir y mejorar continuamente los sistemas de IA y sus procesos de gestión de riesgos.

Artículo 39. Los responsables de los sistemas de IA deben asegurarse de cumplir con las recomendaciones de las auditorías algorítmicas levantando el testigo correspondiente a fin de documentar su progreso. Esto incluye:

a) Plan de Acción: Desarrollar e implementar un plan de acción basado en los hallazgos de la auditoría, con plazos y responsables claros.

b) Monitoreo Continuo: Establecer mecanismos de monitoreo continuo para verificar el cumplimiento de las recomendaciones y la efectividad de las medidas correctivas.

c) Reporte a Autoridades: Informar sobre el cumplimiento de las recomendaciones de la auditoría y cualquier incidente relevante que pueda afectar el funcionamiento del sistema de IA.

TÍTULO NOVENO
PROCEDIMIENTOS PARA LA PROTECCIÓN DE DATOS PERSONALES

Capítulo I

De los Derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad

Artículo 40. Toda persona por sí o a través de su representante, podrá ejercer los derechos de Acceso, Rectificación, Cancelación, Oposición y Portabilidad al tratamiento de sus datos personales en posesión de los sujetos obligados para el desarrollo y utilización de la Inteligencia Artificial, ello, de conformidad con los requisitos y plazos previstos en la Ley de Datos y demás disposiciones aplicables.

Capítulo II

Recurso de Revisión

Artículo 41. Las personas, podrán promover el recurso de revisión en contra de la respuesta a la solicitud de acceso, rectificación, cancelación, oposición y portabilidad a datos personales que el sujeto obligado haya emitido, ello, de conformidad con los requisitos y plazos previstos en la Ley de Datos y demás disposiciones aplicables.

Capítulo III

Verificación del tratamiento lícito de los datos personales en la IA

Artículo 42. El Instituto tendrá la atribución de vigilar y verificar el cumplimiento de los principios y las disposiciones contenidas en la presente Ley y demás ordenamientos que se deriven de ésta. En el ejercicio de las funciones de vigilancia y verificación, el personal del Instituto estará obligado a guardar confidencialidad sobre la información a la que tengan acceso en virtud de la verificación correspondiente.

Artículo 43. La verificación podrá iniciarse:

I. De oficio cuando el Instituto cuente con indicios que hagan presumir fundada y motivada la existencia de violaciones a las leyes correspondientes;

II. Por denuncia de la persona titular cuando considere que han sido vulnerados sus datos personales por actos del responsable que puedan ser contrarios a lo dispuesto por la presente Ley y demás normativa aplicable. La denuncia se resolverá de conformidad con el Procedimiento que para tal efecto emita el Instituto.

III. Por cualquier persona cuando tenga conocimiento de presuntos incumplimientos a las obligaciones previstas en la presente Ley y demás disposiciones que resulten aplicables en la materia;

Artículo 44. El procedimiento de verificación a que se refiere este capítulo, se llevará a cabo conforme al procedimiento establecido en el Título Octavo y Noveno de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Artículo 45. El Instituto, podrá dar fe pública sólo respecto de los actos en materia de protección de datos personales por el desarrollo o uso de inteligencia artificial, a fin de tomar las medidas necesarias para evitar que se alteren, destruyan o extravíen las huellas o vestigios que acrediten la existencia de los hechos denunciados.

Artículo 46. La resolución que emita el Instituto deberá contener:

I. Sentido de la resolución.
II. Sanción decretada, en su caso.
III. Plazo para el cumplimiento, en su caso.
IV. Vista a la autoridad competente, cuando se advierta la presunta comisión de una infracción diversa a la investigada derivada o vinculado con el uso de sistemas de IA, o cuando el Instituto no sea competente para sancionar al infractor.

Artículo 47. Para el caso de las medidas cautelares que refiere el artículo 114 de la Ley de Datos y 192 de los Lineamientos de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, deberá de cumplir con los siguientes requisitos:

I. Presentarse ante el Instituto por escrito libre, o a través de los formatos, medios electrónicos o cualquier otro medio que al efecto se establezca y estar relacionada con una queja o denuncia.

II. Precisar el acto o hecho que constituya la infracción denunciada y de la cual se pretenda hacer cesar;

III. Identificar el daño cuya irreparabilidad se pretenda evitar;

Artículo 48. La solicitud de adoptar medidas cautelares será notoriamente improcedente, cuando:

I. La solicitud no se formule conforme a lo señalado en el artículo que precede.

II. De la investigación preliminar realizada no se deriven elementos de los que pueda inferirse siquiera indiciariamente, la probable comisión de los hechos e infracciones denunciadas que hagan necesaria la adopción de una medida cautelar.

III. Del análisis de los hechos o de la investigación preliminar, se observe que se trata de actos consumados, irreparables o futuros de realización incierta, y

IV. Cuando ya exista pronunciamiento del Instituto respecto de los hechos materia de la solicitud.

Artículo 49. Si la solicitud de adoptar medidas cautelares no actualiza una causal de notoria improcedencia, el Instituto resolverá sobre su adopción o no en un plazo de tres días.

Artículo 50. El Acuerdo que ordene la adopción de medidas cautelares deberá contener las consideraciones fundadas y motivadas acerca de:

I. El cese de cualquier acto o hecho, que pueda entrañar una violación o afectación a los datos personales y privacidad de las personas y en su caso la inmovilización del sistema de inteligencia artificial, y

II. El apercibimiento al sujeto obligado de la imposición de medidas de apremio en caso de incumplimiento al acuerdo de adopción de medidas cautelares.

Artículo 51. El acuerdo en que se determine la adopción de medidas cautelares establecerá la suspensión inmediata de los hechos materia de la misma, otorgando en su caso un plazo no mayor a dos días atendiendo la naturaleza del acto para que los sujetos obligados la atiendan.

TÍTULO DÉCIMO
MEDIDAS DE APREMIO

Artículo 52. El Instituto podrá imponer las siguientes medidas de apremio para asegurar el cumplimiento de sus determinaciones:

I. La amonestación pública; o
II. La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.

Artículo 53. Para calificar las medidas de apremio establecidas en el presente Capítulo, el Instituto deberá considerar:

I. La gravedad de la falta del responsable, determinada por elementos tales como el daño causado, los indicios de intencionalidad, la duración del incumplimiento de las determinaciones del Instituto y la afectación al ejercicio de sus atribuciones;
II. La condición económica del infractor; y
III. La reincidencia. Se considerará reincidente al que habiendo incurrido en una infracción que haya sido sancionada, cometa otra del mismo tipo o naturaleza. Por lo que el Instituto podrá imponer una multa equivalente hasta el doble de la que se hubiera determinado.

El Instituto podrá requerir al infractor la información necesaria para determinar su condición económica, apercibido de que en caso de no proporcionar la misma, las multas se cuantificarán con base a los elementos que se tengan a disposición, entendidos como los que se encuentren en los registros públicos, los que contengan medios de información o sus propias páginas de Internet y, en general, cualquiera que evidencie su condición, quedando facultado el Instituto para requerir aquella documentación que se considere indispensable para tal efecto a las autoridades competentes.

Artículo 54. Las medidas de apremio a que se refiere el presente Capítulo deberán ser aplicadas por el Instituto, por sí mismo o con el apoyo de la autoridad competente, de conformidad con los procedimientos que establezcan las leyes respectivas.

Artículo 55. Las medidas de apremio deberán aplicarse e implementarse en un plazo máximo de quince días, contados a partir de la notificación correspondiente al infractor.

Artículo 56. Los medios de apremio deberán ser aplicados, previo apercibimiento, con el propósito de hacer cumplir las determinaciones del Instituto.

Artículo 57. Para la imposición del medio de apremio debe estar acreditado el incumplimiento de los sujetos obligados a alguna de las determinaciones del Instituto, y es necesario que se notifique el acuerdo en el que se establezca el apercibimiento, precisando que en el supuesto que no se desahogue en tiempo y forma lo requerido, se le aplicará una de las medidas de apremio previstas en el presente Título.

Artículo 58. La amonestación pública será impuesta por el Instituto y será ejecutada por el superior jerárquico inmediato del infractor con el que se relacione.

Artículo 59. Las multas que fije el Instituto se harán efectivas por la Secretaría de Finanzas de la Ciudad de México, a través de los procedimientos que las leyes establezcan.

Artículo 60. Si a pesar de la ejecución de las medidas de apremio previstas en el artículo anterior no se cumpliere con la resolución, se requerirá el cumplimiento al superior jerárquico para que en el plazo de cinco días lo obligue a cumplir sin demora.

Transcurrido el plazo, sin que se haya dado cumplimiento, se dará vista la autoridad competente en materia de responsabilidades.

Artículo 61. En caso de que el incumplimiento de las determinaciones del Instituto implique la presunta comisión de un delito o una de las conductas señaladas en la presente Ley, deberán denunciar los hechos ante la autoridad competente. Las medidas de apremio de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 62. La facultad del Instituto para fincar responsabilidades por vulnerar datos personales en el desarrollo y utilización de la inteligencia artificial prescribe en tres años.

I. El término de la prescripción se empezará a contar a partir de la fecha en que hayan ocurrido los presuntos hechos que vulneraron los datos personales y privacidad de las personas por el uso de la inteligencia artificial por parte de los sujetos obligados, a partir de que se tenga conocimiento de los mismos, o bien, tratándose de actos continuados a partir de cuándo cese su comisión.

II. La presentación de una denuncia o el inicio oficioso de un procedimiento de verificación por parte del Instituto, interrumpe el cómputo de la prescripción.

Artículo 63. En contra de la imposición de medidas de apremio, procede el recurso correspondiente ante el Poder Judicial de la Ciudad de México.

TÍTULO UNDÉCIMO
SANCIONES

Artículo 64. Son sujetos de responsabilidad por infracciones cometidas a las disposiciones previstas en esta ley:

a) Los Sujetos Obligados;

b) Responsable del despliegue de la inteligencia artificial;

c) Proveedores y distribuidores

Artículo 65. Además de las señaladas en la Ley de Datos, serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

I. Actuar con negligencia, dolo o mala fe durante el desarrollo, mantenimiento y utilización de la inteligencia artificial, así como en el tratamiento de los datos personales durante todo su ciclo de vida;

II. Incumplir los plazos y obligaciones previstos en la presente Ley;

III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión;

IV. Dar tratamiento, de manera intencional, a los datos personales en contravención a los principios y deberes establecidos en la presente Ley;

V. No recabar el consentimiento de la persona titular, lo que constituye que el tratamiento sea ilícito, o no contar con el aviso de privacidad, o bien tratar de manera dolosa o con engaños datos personales y las demás disposiciones que resulten aplicables en la materia;

VI. Incumplir el deber de confidencialidad establecido en la presente Ley;

VII. No establecer las medidas de seguridad en los términos que establece la presente Ley;

VIII. Presentar vulneraciones a los datos personales por la falta de implementación de medidas de seguridad en el desarrollo y uso de la inteligencia artificial;

IX. Llevar a cabo la transferencia de datos personales, en contravención a lo previsto en la presente Ley y la Ley de Datos;

X. Obstruir los actos de verificación del Instituto;

XII. No acatar las resoluciones emitidas por el Instituto; y

Las causas de responsabilidad previstas en las fracciones I, II, IV, IX y XI, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa.

En caso de que la presunta infracción hubiere sido cometida por algún integrante de un partido político, la investigación y, en su caso, sanción, corresponderán a la autoridad electoral competente. Por lo que, para estos casos, únicamente se remitira a la autoridad electoral la denuncia con el expediente que sustenta las omisiones u acciones aquí señaladas.

Las sanciones de carácter económico no podrán ser cubiertas con recursos públicos.

Artículo 66. Para las conductas a que se refiere el artículo anterior se dará vista a la autoridad competente para que ejecute la sanción.

Artículo 67. Para imponer la sanción el Instituto calificará la falta determinando lo siguiente:

a) Tipo de infracción (acción u omisión).

b) Circunstancias de tiempo, modo y lugar en que se concretaron.

c) Comisión intencional o culposa de la falta.

d) La trascendencia de las normas transgredidas.

e) Los valores o bienes jurídicos tutelados que fueron vulnerados o la lesión, daño perjuicios que pudieron generarse con la comisión de la falta.

f) La singularidad o pluralidad de la falta acreditada.

g) La condición de que el ente infractor haya incurrido con antelación en la comisión de una infracción similar (Reincidencia).

Artículo 68. Para la imposición de la sanción, se considerará además que la misma no afecte sustancialmente el desarrollo de las actividades del sujeto obligado de tal manera que comprometa el cumplimiento de sus propósitos fundamentales o subsistencia.

Artículo 69. Para establecer la sanción que más se adecúe a la infracción cometida, se tomarán en consideración la capacidad económica del infractor, así como las agravantes y atenuantes a fin de que se imponga una sanción proporcional a la falta cometida.

Artículo 70. El Instituto podrá imponer las siguientes sanciones para asegurar el cumplimiento de sus determinaciones:

I. La amonestación pública; o
II. La multa, equivalente a la cantidad de ciento cincuenta hasta mil quinientas veces el valor diario de la Unidad de Medida y Actualización.
IV. La suspensión temporal de las operaciones del sistema de IA hasta que se corrijan los problemas identificados y se garantice el cumplimiento de la ley.
V. Revocación de permisos y licencias para operar el sistema de IA.

Artículo 71. Las responsabilidades que resulten derivados de la violación a lo dispuesto por esta ley son independientes de las del orden civil, penal o de cualquier otro tipo que se puedan derivar de los mismos hechos. Dichas responsabilidades se determinarán, en forma autónoma, a través de los procedimientos previstos en las leyes aplicables y las sanciones que, en su caso, se impongan por las autoridades competentes, también se ejecutarán de manera independiente.

Para tales efectos, el Instituto podrá denunciar ante las autoridades competentes cualquier acto u omisión violatoria de esta Ley y aportar las pruebas que consideren pertinentes, en los términos de las leyes aplicables.

Artículo 72. En el caso de usuarios y sujetos obligados, vinculados a una investigación por responsabilidad algorítmica, el Instituto coadyuvará con ellos para solicitar a los fabricantes, creadores o distribuidores de sistemas de IA o modelos de IA, la información necesaria para verificar el grado de responsabilidad de las y los involucrados.

Transitorios

Primero. El presente decreto entrará en vigor el día siguiente a su publicación en la Gaceta Oficial de la Ciudad de México.

Segundo. El Poder Ejecutivo de la Ciudad de México, a través de la Agencia Digital de Innovación Pública de la Ciudad de México y el Instituto se coordinarán para la emisión de las disposiciones secundarias que se requieran para la correcta implementación de esta Ley.

Tercero. Para el caso de las auditorías algorítmicas, la Agencia Digital de Innovación Pública de la Ciudad de México tendrá un plazo de un año para comenzar a implementarlas.

Tercero. Los sujetos obligados que ya utilizan modelos de inteligencia artificial deberán adaptar sus desarrollos o sus usos con las disposiciones de esta ley dentro de un plazo que no exceda los dieciocho meses a partir de su entrada en vigor.

Cuarto. El Instituto proporcionará un programa de capacitación para todos los sujetos obligados, enfocado en el cumplimiento de las nuevas disposiciones legales. Este programa de capacitación será anual y permanente.

Congreso de la Ciudad de México, a los ___ días del mes de _____de dos mil veinticuatro.