Decreto que modifica los artículos 20 Quáter párrafo primero, 20 Quáter párrafo tercero, 20 Sexies parrafo primero y 20 Sexies párrafo cuarto de la Ley General d Acceso de las Mujeres a una Vida Libre de Violencia y el artículo 199 Nonies del Código Penal Federal, a cargo de la diputada Melissa Estefanía Vargas Camacho, del Grupo Parlamentario del PRI.

La que suscribe, diputada Melissa Estefanía Vargas Camacho, integrante del Grupo Parlamentario del Partido Revolucionario Institucional en la LXIV Legislatura del honorable Congreso de la Unión, y con fundamento en lo dispuesto en los artículos 71, fracción II, y 78, fracción III, de la Constitución Política de los Estados Unidos Mexicanos; 116 y 122 de la Ley Orgánica del Congreso General de los Estados Unidos Mexicanos; 6, numeral 1, fracción I, 77 y 78 del Reglamento de la Cámara de Diputados, somete a consideración de la Comisión Permanente la iniciativa con proyecto de decreto por el que se modifica los artículos 20 Quáter párrafo primero, 20 Quáter párrafo tercero, 20 Sexies parrafo primero y 20 Sexies párrafo cuarto de la Ley General d Acceso de las Mujeres a una Vida Libre de Violencia y el artículo 199 Nonies del Código Penal Federal, con sustento en la siguiente:

Exposición de Motivos

La industria de la inteligencia artificial (IA) está creciendo a una velocidad imparable. Los países compiten para ganar la "carrera de la IA". El presidente ruso, Vladimir Putin, cree que la nación que salga victoriosa "gobernará el mundo". Las empresas están invirtiendo miles de millones de dólares para asegurarse la mayor cuota de mercado. Las simulaciones muestran que para 2030 cerca del 70% de las empresas habrán adoptado algún tipo de tecnología de IA. La razón es sencilla.

Ya sea para modelar el cambio climático, seleccionar candidatos para un puesto de trabajo o predecir si alguien va a cometer un delito, la IA puede sustituir a los humanos y tomar decisiones de forma más rápida y barata.

Sin embargo, los sistemas de IA suponen una amenaza para nuestros derechos fundamentales. Por ejemplo, los que moderan los contenidos en las plataformas de las redes sociales pueden restringir la libertad de expresión de manera injusta e influir en el debate público. Las tecnologías de vigilancia masiva biométrica violan nuestro derecho a la privacidad y desalientan la participación democrática. Los algoritmos se basan en conjuntos masivos de datos personales, cuya recopilación, procesamiento y almacenamiento a menudo viola nuestros derechos de protección de datos. El sesgo algorítmico puede perpetuar las estructuras de desigualdad existentes en nuestras sociedades y suponer una mayor discriminación y alienación de las minorías. Un ejemplo de ello son los algoritmos de contratación (que se utilizan para seleccionar candidatos) que suelen preferir a los hombres sobre las

mujeres y a las personas blancas sobre las negras, porque los datos de los que se alimentan dicen que los "candidatos exitosos" suelen ser hombres blancos.

Estos problemas se ven agravados por la complejidad de la IA. Aún no sabemos bien cuáles son los posibles riesgos que los sistemas de IA pueden implicar para nuestras sociedades. Jenna Burrell, investigadora de la Universidad de California, ha identificado tres tipos de opacidad de estos sistemas. Los que se mantienen intencionadamente opacos, porque las empresas o los Estados quieren mantener secretos. Los que son consecuencia del analfabetismo técnico, porque son demasiado complicados para que la sociedad en general los entienda. Y los que surgen de las complejas características de los algoritmos de aprendizaje automático. Es decir, aquellos que ni siquiera los programadores acaban de entender o captar.

Para prevenir o protegernos de estas amenazas, se debe regular la IA. A día de hoy, aún no se ha diseñado en ningún lugar un sistema de leyes que regulen específicamente el uso de la IA, permitiendo así que muchas empresas desarrollen sistemas que pueden generar daños a las personas con el fin de lucrarse. Algunos de estos sistemas ya existen y se utilizan. Debido a la falta de transparencia de las autoridades, a menudo no lo sabemos. Las fuerzas policiales de toda la UE utilizan tecnologías de reconocimiento facial y sistemas de policía predictiva. Como explicamos en otro artículo, estos sistemas contienen obligatoriamente un sesgo y, por ende, perpetúan la discriminación y la desigualdad.

En este artículo analizamos por qué es preciso regular el uso de la IA, qué tipo de regulación existe ya, qué debería contener una regulación y de qué depende el futuro de la misma.

Debemos regular la IA por dos razones fundamentales. En primer lugar, porque gobiernos y empresas la utilizan para tomar decisiones que pueden generar un impacto significativo en nuestras vidas. Por ejemplo, los algoritmos que calculan el rendimiento escolar pueden tener un efecto devastador. En Reino Unido, el secretario de Estado de Educación utilizó un algoritmo para determinar la nota del examen final de los estudiantes de todo el país. El resultado: casi el 40 por ciento de los estudiantes recibieron notas más bajas que las emitidas previamente por sus profesores. Pero el algoritmo no solo era inexacto, sino que además favorecía a los alumnos de los colegios privados frente a los de los públicos. La IA también ha mostrado sus limitaciones en el sector privado. En otro caso, una tarjeta de crédito introducida por el gigante tecnológico Apple ofrecía límites de crédito más bajos para mujeres que para hombres. Los sistemas de IA que calculan la probabilidad de reincidencia y determinan la duración de las penas de prisión de las personas acusadas pueden alterar significativamente la vida de una persona. Sin

una regulación adecuada, los sistemas tienen más probabilidad de ser inexactos y sesgados, ya que las empresas tienen menos incentivos para invertir en medidas de seguridad y garantizar la calidad y la imparcialidad de sus datos.

En segundo lugar, porque siempre que alguien toma una decisión que nos afecta, tiene una responsabilidad sobre la misma, debe rendir cuentas ante nosotros. La legislación de derechos humanos establece unas normas mínimas que todo el mundo reconoce y puede esperar y otorga a todas las personas el derecho a recurrir cuando se incumplen y se sufre un daño. Teóricamente, los gobiernos deben garantizar el respeto de estas normas y de que toda persona que las infrinja tiene que rendir cuentas, normalmente a través del derecho administrativo, civil o penal.

Esto significa que todo el mundo, incluidas las empresas y los gobiernos, tienen que seguir ciertas normas a la hora de tomar decisiones. Cuando alguna persona se salta las normas acordadas y perjudica a otra, debe responder por ello. Sin embargo, ya existen indicios de que las empresas que están detrás de la IA pueden eludir la responsabilidad de los problemas que causan. Por ejemplo, cuando en 2018 un coche autónomo de Uber mató a una peatona, al principio no estaba claro quién sería el responsable. ¿El fabricante del coche, Uber o la persona que iba en el coche? A pesar de que los investigadores descubrieron que el coche tenía problemas de seguridad (no tenía en cuenta a los peatones que cruzaban la calle por lugares que no fueran pasos de cebra), Uber fue declarado "sin responsabilidad penal". Fue la persona al volante quien fue acusada de homicidio por negligencia, ya que estaba viendo un episodio de un programa de televisión.

Como ya hemos mencionado, actualmente no existe una legislación específicamente diseñada para regular el uso de la IA. Más bien, los sistemas de IA se regulan por otras normativas existentes. Entre ellas, las leyes de protección de datos, de protección de los consumidores y de competencia en el mercado. Sí se han aprobado proyectos de ley para regular ciertos sistemas específicos de IA. En Nueva York, es posible que próximamente las empresas tengan que revelar cuándo utilizan algoritmos para elegir a sus empleados y varias ciudades de Estados Unidos ya han prohibido el uso de tecnologías de reconocimiento facial. En la UE, la Ley de Servicios Digitales tendrá un impacto significativo en el uso por parte de las plataformas en línea de algoritmos que clasifican y moderan el contenido, predicen nuestras preferencias personales y, en última instancia, deciden lo que leemos y vemos, los también llamados algoritmos de moderación de contenido.

Los gobiernos nacionales y municipales han comenzado a adoptar estrategias y a trabajar en nuevas leyes desde hace varios años, pero aún no se ha aprobado ninguna legislación. China, por ejemplo, desarrolló en 2017 una estrategia para convertirse en líder mundial en IA en 2030. En Estados Unidos, la Casa Blanca

publicó diez principios para la regulación de la IA. Entre ellos figuran la promoción de "aplicaciones de IA seguras, sólidas y fiables", la participación pública y la integridad científica. Los organismos internacionales que asesoran a gobiernos, como la OCDE o el Foro Económico Mundial, han elaborado directrices éticas. El Consejo de Europa creó un Comité para desarrollar un marco jurídico para la IA.

Sin embargo, la propuesta más ambiciosa hasta ahora procede de la UE. El 21 de abril de 2021, la Comisión Europea presentó una propuesta de nueva ley sobre IA.

El proyecto sugiere que se ilegalice el uso de la IA para fines considerados "inaceptables". Entre ellos, tecnologías de reconocimiento facial, los sistemas que se utilizan para clasificar a las personas en función de su "fiabilidad", y los sistemas que manipulan a las personas o explotan las vulnerabilidades de grupos específicos; por ejemplo, un juguete que utiliza la asistencia por voz para manipular a los niños para que hagan algo peligroso. El enfoque de la propuesta se basa en el riesgo: cuanto mayor sea el riesgo de una determinada utilización de la IA para nuestras libertades, más obligaciones de transparencia tendrá la autoridad o la empresa sobre el funcionamiento del algoritmo y de informar a los reguladores sobre cómo se ha utilizado.

Aunque parezca que la Comisión Europea se toma en serio la regulación de los sistemas de IA perjudiciales, en realidad la propuesta antepone lo empresarial a los derechos fundamentales. Aunque la Comisión se jacte de afirmar que ha prohibido la tecnología de reconocimiento facial, la propuesta ofrece lagunas que permiten que las empresas y las autoridades la utilicen. Además, las obligaciones de transparencia para los sistemas de alto riesgo tienen un fallo importante: la tarea de comprobar si la IA implica riesgos se deja en manos de las propias empresas que crean estos sistemas. Son empresas con ánimo de lucro que tienen interés en ver sus productos en el mercado, por lo que es probable que resten importancia a los riesgos.

Una regulación eficaz de la IA que proteja los derechos debe contener, como mínimo, las siguientes salvaguardas. En primer lugar, debe prohibir las tecnologías que violan nuestros derechos fundamentales, como la vigilancia masiva biométrica o los sistemas de policía predictiva. La prohibición no debe incluir excepciones que permitan que las empresas o a las autoridades públicas las empleen "bajo ciertas condiciones".

En segundo lugar, debe haber normas claras que establezcan exactamente la información que las empresas tienen que hacer pública acerca de sus productos, deben proporcionar una descripción detallada del propio sistema de IA. Desde información sobre los datos que utiliza, el proceso de desarrollo, la finalidad del

sistema y dónde y quién lo utiliza. También es esencial que las personas expuestas a la IA tengan información sobre la misma, por ejemplo, en el caso de los algoritmos de contratación. Los sistemas que pueden tener un impacto significativo en la vida de las personas deberían someterse a un escrutinio adicional y figurar en una base de datos de acceso público. Esto facilitaría que investigadores y periodistas puedan comprobar si las empresas y los gobiernos protegen adecuadamente nuestras libertades.

En tercer lugar, los individuos y organizaciones que protegen a los consumidores deben poder pedir responsabilidades a los gobiernos y a las empresas en caso de que provoquen problemas. Las normas existentes sobre responsabilidad deben adaptarse para reconocer que las decisiones son tomadas por un algoritmo y no por el usuario. Esto podría significar que la empresa que desarrolla el algoritmo tenga la obligación de comprobar los datos con los que se entrenan los algoritmos y las decisiones que toman para poder corregir los problemas.

En cuarto lugar, la nueva normativa debe garantizar la existencia de un organismo regulador que compruebe que las empresas y las autoridades cumplen las normas correctamente. Este organismo de control debe ser independiente y contar con los recursos y poderes necesarios para hacer su trabajo.

Por último, una regulación de la IA debe incluir asimismo las salvaguardas para proteger a los más vulnerables, establecer un sistema que permita que las personas que se han visto perjudicadas por sistemas de IA presenten una denuncia y obtengan una compensación. Y los trabajadores deberían tener derecho a actuar contra los sistemas de IA invasivos utilizados por su empresa sin temor a represalias.

Cuando la UE cree normas sobre IA, probablemente acabará marcando la pauta para el resto del mundo debido a todas las empresas que trabajan y tienen su sede en la UE. Por ello, tiene la gran responsabilidad de hacerlo bien, porque estas normas afectarán la forma en que se utilizan los sistemas de IA en partes del mundo menos democráticas. Por ejemplo, los algoritmos que pretenden predecir la orientación sexual de una persona pueden llevar a la muerte a personas en países en los que ser gay sigue estando castigado con la muerte.

Ahora son los responsables políticos y los dirigentes de la UE quienes deben elaborar normas que mejoren nuestra calidad de vida y fomenten la igualdad. Los negociadores de la UE pueden sentir la tentación de adoptar sistemas de IA porque creen que puede suponer un ahorro o porque estimulará la economía. Pero los atajos en los servicios públicos o utilizar la IA cuando no conlleva ningún beneficio social acabarán perjudicando nuestro modo de vida y las libertades que valoramos.

La pregunta que debe hacerse la UE es cómo pueden nuestras sociedades utilizar la IA para llevar a cabo nuestros derechos y libertades.

En las últimas décadas, la revolución tecnológica y la penetración de las Tecnologías de la Información y la Comunicación (TIC) han transformado la manera en que entendemos y nos relacionamos con el mundo, modificando radicalmente nuestros hábitos de consumo, los modos de ganarnos la vida, los flujos de información que recibimos y la forma en que interactuamos con otras personas.

De manera particular, la masificación del uso del Internet, la telefonía móvil y las redes sociales han tenido un impacto de carácter revolucionario en nuestra vida cotidiana. Hoy en día, el acceso a estas tecnologías es considerada por muchos países -incluido el nuestro- como un derecho humano, es decir, como uno de los elementos vitales que los Estados deben asegurar para garantizar el desarrollo pleno de las personas.

En el último eslabón evolutivo de este tipo de tecnologías disruptivas se encuentra la Inteligencia Artificial (IA), que consiste básicamente en la imitación de las actividades que realizamos las personas, por parte de computadoras con cierto grado de automaticidad y autonomía. En palabras simples, la IA se trata de darle una indicación a una computadora para que lleve a cabo una tarea, que puede ser desde una búsqueda de información en la web hasta una intervención quirúrgica.

Si bien los orígenes de esta tecnología se pueden rastrear a mediados del siglo XX, con los estudios de Alan Turing que sentaron las bases teóricas para la IA y la computación moderna en general, ha sido durante los primeros lustros de este milenio en los que la IA se ha presentado como una auténtica revolución tecnológica, tanto por el desarrollo cada vez más sofisticado y autónomo de los diferentes sistemas creados hasta el momento, como por su disponibilidad y accesibilidad, lo que ha hecho posible que en un lapso muy corto de tiempo, millones de personas en todo el mundo utilicen consiente e inconscientemente los sistemas de IA .

En este tenor ha surgido un debate fascinante sobre el impacto de la IA en la vida de las personas. En las redes sociales se ha originado una explosión de publicaciones que explican las bondades y maravillas de la creciente y variada oferta de páginas de IA, muchas de ellas de acceso libre. Del otro lado de la moneda, algunos científicos y desarrolladores de tecnología han advertido los riesgos que representa la IA, incluso afirmando que representa la amenaza más grande para la humanidad. Otros especialistas más cautelosos, como Nick Bostrom de la Universidad de Oxford, sostienen que todavía no podemos imaginar la infinita

gama de posibilidades y aplicaciones de la IA y que las iremos conociendo con el paso de los años, conforme a la propia evolución humana (Zuckerman, 2023).

De lo que no hay duda alguna es que la IA ha ganado e irá ganando un mayor protagonismo en nuestras vidas. Al igual que ocurrió con la telefonía celular y las redes sociales, la tendencia apunta hacia el uso generalizado, especializado y diversificado de la IA. De ahí la necesidad de estudiar las aplicaciones de la IA, a fin de que podamos sacar el máximo provecho de esta herramienta y al mismo tiempo tomar previsiones para mitigar los riesgos que guarda.

En México, el desarrollo y aprovechamiento de la IA encuentra su base constitucional en el artículo 3º, fracción V, que reconoce el derecho de las personas a gozar de los beneficios del desarrollo de la ciencia y la innovación tecnológica, en los siguientes términos:

- Toda persona tiene derecho a gozar de los beneficios del desarrollo de la ciencia y la innovación tecnológica. El Estado apoyará la investigación e innovación científica, humanística y tecnológica, y garantizará el acceso abierto a la información que derive de ella, para lo cual deberá proveer recursos y estímulos suficientes, conforme a las bases de coordinación, vinculación y participación que establezcan las leyes en la materia; además alentará el fortalecimiento y difusión de nuestra cultura (Art. 3 de la CPEUM).

A nivel reglamentario, no existe una legislación que trate de modo específico a la IA. La regulación vigente se relaciona de manera tangente con la IA en casos como la protección de datos personales y los derechos de los consumidores de proveedores de servicios de tecnología.

Es inminente que el Congreso Mexicano entre a este tema pues ya se han presentado algunas iniciativas y propuestas para regular el desarrollo y aprovechamiento seguro de la IA.

En el Senado de la República se han presentado cuatro puntos de acuerdo de distintas senadoras y senadores en el sentido de diseñar e implementar políticas públicas para el desarrollo de la IA.

En la Cámara de Diputados, el 30 de marzo de 2023, el Dip. Ignacio Loyola Vera presentó la iniciativa de Ley para la Regulación Ética de la Inteligencia Artificial y la Robótica, que propone, entre otras cosas, establecer lineamientos de políticas públicas para la regulación ética del uso de la inteligencia artificial y la robótica, expedir normas oficiales basadas en principios éticos para el uso de la inteligencia artificial y la robótica en beneficio de la sociedad mexicana, así como crear al

Consejo Mexicano de Ética para la Inteligencia Artificial y la Robótica y la Red Nacional de Estadística de uso y monitoreo de la Inteligencia Artificial y la Robótica.

Como se puede ver, el tema de la IA apenas está comenzando a atraer la atención del Poder Legislativo, pero dada la velocidad e intensidad de los cambios que trae consigo, es de esperarse que con el paso de los años ocupe una mayor centralidad en la agenda legislativa.

Estos límites evidentes de la IA reivindican a los seres humanos como los únicos sujetos políticos y su responsabilidad en las decisiones de interés colectivo, entre ellas, la elaboración de las normas jurídicas que nos rigen a todas y todos.

Por otro lado, también debemos ser conscientes y tomar medidas frente a los riesgos que entraña la IA, en donde se encuentran cuestiones como el uso de información imprecisa y desactualizada, la importación de soluciones no adecuadas para las realidades del país, problemas de plagio, la dependencia tecnológica, el mal uso de los datos personales e institucionales y los peligros cibernéticos que podrían vulnerar los sistemas que son usados por las instituciones para el cumplimiento de sus funciones.

Estos y otros problemas podrían ser abordados mediante una legislación que regule el desarrollo, aprovechamiento y mitigación de los riesgos de la IA. Esta legislación tiene que ser transversal considerando que la IA está penetrando velozmente en todas las actividades, lo que tendrá un impacto en el mercado laboral, la división social del trabajo, las necesidades educativas y la productividad del país.

El artículo 12 de la Declaración Universal de Derechos Humanos, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y varios otros instrumentos internacionales y regionales de derechos humanos reconocen el derecho a la intimidad como un derecho humano fundamental.

El derecho a la privacidad desempeña un papel fundamental en el equilibrio de poder entre el Estado y el individuo y es un derecho fundamental para una sociedad democrática. Su importancia para el disfrute y ejercicio de otros derechos humanos en línea y fuera de línea en un mundo cada vez más centrado en los datos está creciendo.

El derecho a la intimidad es una expresión de la dignidad humana y está vinculado a la protección de la autonomía humana y la identidad personal. Los aspectos de la privacidad que son de particular importancia en el contexto del uso de la IA incluyen la privacidad de la información, que abarca la información que existe o puede derivarse sobre una persona y su vida y las decisiones basadas en esa información, y la libertad de tomar decisiones sobre la propia identidad.

Cualquier injerencia en el derecho a la intimidad no debe ser arbitraria ni ilegal. El término "ilícito" significa que los Estados pueden interferir con el derecho a la privacidad sólo sobre la base de la ley y de conformidad con esa ley. La propia ley debe ajustarse a las disposiciones, propósitos y objetivos del Pacto Internacional de Derechos Civiles y Políticos y debe especificar en detalle las circunstancias precisas en que esa injerencia es permisible. La introducción del concepto de arbitrariedad tiene por objeto garantizar que incluso la injerencia prevista por la ley se ajuste a las disposiciones, fines y objetivos del Pacto y, en cualquier caso, sea razonable en las circunstancias particulares. Por consiguiente, toda injerencia en el derecho a la intimidad debe servir a una finalidad legítima, ser necesaria para alcanzar dicha finalidad legítima y ser proporcionada. Cualquier restricción también debe ser la opción menos intrusiva disponible y no debe menoscabar la esencia del derecho a la privacidad.

El derecho a la privacidad se aplica a todos. Las diferencias en su protección por motivos de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición son incompatibles con el principio de no discriminación establecido en el párrafo 1 del artículo 2 y en el artículo 3 del Pacto Internacional de Derechos Civiles y Políticos. La discriminación por estos motivos también viola el derecho a la igualdad ante la ley consagrado en el artículo 26 del Pacto.

El párrafo 1 del artículo 2 del Pacto Internacional de Derechos Civiles y Políticos exige a los Estados que respeten y garanticen los derechos reconocidos en el Pacto a todas las personas que se encuentren en su territorio y estén sujetas a su jurisdicción, sin discriminación. En otras palabras, los Estados no sólo deben abstenerse de violar los derechos reconocidos en el Pacto, sino que también tienen la obligación de adoptar medidas positivas para proteger el disfrute de esos derechos. Esto implica el deber de adoptar medidas legislativas y de otra índole adecuadas para proteger a las personas contra la injerencia en su vida privada, ya sea que emane de las autoridades estatales o de personas físicas o jurídicas. Este deber también se refleja en el pilar I de los Principios Rectores sobre las Empresas y los Derechos Humanos, que describe el deber de los Estados de proteger contra los impactos adversos sobre los derechos humanos que involucran a las empresas.

El funcionamiento de los sistemas de IA puede facilitar y profundizar la intromisión en la privacidad y otras interferencias con los derechos de diversas maneras. Estos incluyen aplicaciones completamente nuevas, así como características de los sistemas de IA que amplían, intensifican o incentivan la interferencia con el derecho a la privacidad, especialmente a través de una mayor recopilación y uso de datos personales.

Al los sistemas suelen basarse en grandes conjuntos de datos, que a menudo incluyen datos personales. Esto incentiva la recopilación, el almacenamiento y el procesamiento generalizados de datos. Muchas empresas optimizan los servicios para recopilar la mayor cantidad de datos posible. Por ejemplo, las empresas en línea como las compañías de redes sociales dependen de la recopilación y monetización de cantidades masivas de datos sobre los usuarios de Internet. La llamada Internet de las cosas es una fuente de datos en rápido crecimiento explotada tanto por las empresas como por los Estados. La recolección de datos ocurre en espacios íntimos, privados y públicos. Los intermediarios de datos adquieren, fusionan, analizan y comparten datos personales con innumerables destinatarios. Estas transacciones de datos están en gran medida protegidas del escrutinio público y solo marginalmente inhibidas por los marcos legales existentes.[21] Los conjuntos de datos resultantes son grandes y la información recopilada es de proporciones sin precedentes.

Además de exponer la vida privada de las personas a las empresas y los Estados, estos conjuntos de datos hacen que las personas sean vulnerables de otras maneras. Las violaciones de datos han expuesto repetidamente información confidencial de millones de personas. Los grandes conjuntos de datos permiten innumerables formas de análisis e intercambio de datos con terceros, lo que a menudo equivale a nuevas intrusiones en la privacidad e incurre en otros impactos adversos sobre los derechos humanos. Los acuerdos que permiten a los organismos gubernamentales tener acceso directo a esos conjuntos de datos en poder de las empresas, por ejemplo, aumentan la probabilidad de interferencia arbitraria o ilegal en el derecho a la privacidad de las personas afectadas. Una preocupación particular es la posibilidad de desanonimización que se facilita mediante la fusión de datos de diversas fuentes. Al mismo tiempo, el diseño de conjuntos de datos puede tener implicaciones para la identidad de los individuos. Por ejemplo, un conjunto de datos que registra el género como binario confunde a aquellos que no se identifican como hombres o mujeres. El almacenamiento a largo plazo de datos personales también conlleva riesgos particulares, ya que los datos están abiertos a futuras formas de explotación no previstas en el momento de la recopilación de datos. Con el tiempo, los datos pueden volverse inexactos, irrelevantes o arrastrar una identificación errónea histórica, lo que puede causar resultados sesgados o erróneos del procesamiento futuro de datos.

Muchas inferencias y predicciones afectan profundamente el disfrute del derecho a la privacidad, incluida la autonomía de las personas y su derecho a establecer detalles de su identidad. También plantean muchas cuestiones relativas a otros derechos, como los derechos a la libertad de pensamiento y de opinión, el derecho a la libertad de expresión y el derecho a un juicio justo y derechos conexos.

La necesidad de adoptar un enfoque basado en los derechos humanos en lo que respecta a las nuevas tecnologías en general, y a la inteligencia artificial en particular, ha sido reconocida por un número creciente de expertos y partes interesadas, así como por la comunidad internacional71. Dicho enfoque proporciona herramientas para ayudar a las sociedades a identificar formas de prevenir y limitar los daños obteniendo los máximos beneficios posibles de los avances tecnológicos.

Las restricciones del derecho a la privacidad deben estar previstas en la ley y ser necesarias y proporcionadas para alcanzar un objetivo legítimo. En la práctica, eso significa que los Estados tienen que valorar detenidamente si una medida podrá alcanzar un objetivo establecido, hasta qué punto es importante ese objetivo y qué efectos tendrá esa medida.

La protección efectiva del derecho a la privacidad y los derechos conexos depende de los marcos jurídicos, reglamentarios e institucionales establecidos por los Estados.

Con la aparición de los sistemas de IA basados en datos, las medidas de protección jurídica efectivas en el marco de las leyes sobre privacidad de los datos han ganado importancia. Estas protecciones deben cumplir las normas mínimas sobre el derecho a la vida privada.

Los marcos relativos a la privacidad de los datos deben tener en cuenta las nuevas amenazas relacionadas con el uso de la IA. Por ejemplo, las leyes podrían imponer limitaciones al tipo de datos que pueden inferirse y/o utilizarse y compartirse posteriormente de manera legal. Los legisladores también deberían valorar la posibilidad de reforzar los derechos de las personas, en particular reconociéndoles el derecho a una explicación significativa y a oponerse a las decisiones totalmente automatizadas que afectan a sus derechos80. A medida que evolucionen las tecnologías de IA, habrá que continuar reforzando las garantías previstas en los marcos de protección de la privacidad de los datos.

Los organismos independientes de supervisión de la privacidad de los datos constituyen un elemento clave para contrarrestar la complejidad y opacidad crecientes del entorno mundial de datos, incluidas sus enormes asimetrías de información. Estos organismos deben disponer de facultades efectivas de aplicación de la ley y contar con los recursos adecuados. Las organizaciones de la sociedad civil deberían estar capacitadas para prestar apoyo a la aplicación de las leyes sobre privacidad de los datos, en particular mediante el establecimiento de mecanismos sólidos de denuncia.

Más allá de la legislación sobre la privacidad de los datos, es necesario revisar y, si es posible, adoptar una gama más amplia de leyes para abordar los desafíos que plantea la IA de modo que el respeto de los derechos quede garantizado.

La diversidad de los riesgos derivados de los sistemas de IA hace que sea necesaria una supervisión adecuada, independiente e imparcial, de su desarrollo, implantación y uso. Esta puede estar a cargo de diversos órganos de supervisión administrativa, judicial, y/o parlamentaria. Por ejemplo, además de las autoridades responsables de la privacidad de los datos, el sistema de supervisión también podría abarcar agencias de protección del consumidor, organismos de regulación sectorial, organismos de lucha contra la discriminación e instituciones nacionales de derechos humanos. Además, los organismos de regulación intersectorial encargados de supervisar el uso de la IA pueden ayudar a definir normas fundamentales y garantizar la coherencia de las políticas y de su aplicación.

Toda innovación tecnológica produce beneficios, riesgos y daños. Entre otras ventajas, Internet es vital para asegurar el derecho de libertad de expresión, pero, por ejemplo, también se usa para traficar armas, órganos, y muchos otros delitos que se desarrollan en el mundo digital. Teniendo en cuenta este aspecto, en los dos puntos anteriores hemos abordado el lado luminoso de la inteligencia artificial. Ahora, trazaremos algunas breves líneas en torno a los riesgos, desafíos y retos que nos depara esta nueva tecnología. El "lado oscuro de la IA".

La realidad es que el derecho no puede ir en contra del progreso. Sin embargo, debemos tener en cuenta que es muy grande la afectación a nuestra libertad cuando se viola nuestra intimidad. Y no se puede concebir una sociedad moderna, una sociedad inteligente -artificial o no-, sin el resguardo de derechos fundamentales como la intimidad o como la libertad; de allí que el derecho deberá acompañar esos avances tecnológicos en resguardo de garantías fundamentales y regular a través de leyes modernas, la protección de los datos que se obtienen de los usuarios.

Algunos riesgos de no regular o legislar las prácticas de la IA generativa. Puede ser adherida a ciertos valores e intereses humanos; además de la generación de contenido escrito, imagen y video falso o malicioso que podría utilizarse en fraudes o suplantación de personas e identidades. También ser una influencia en la democracia hacia la polarización, incidir en la protección a la imagen e intimidad; se convertiría en un riesgo en la interacción con menores de edad.

Un principio fundamental de la inteligencia artificial debe ser el respeto a la dignidad humana, comprendiendo que es todo ser humano, que desde inicio de su existencia hasta su muerte natural es titular de derecho, denominados naturales o humanos sobre los cuales nadie puede suprimir10; este principio debe estar dentro de la

esfera ética donde el respeto impere hacia al humano evitando sea violentado por las tecnologías "autónomas". Con ello también, gozar del reconocimiento de la protección de datos personales, estableciendo límites por medio de mecanismos como el principio de minimización, el derecho al consentimiento de los interesados sobre el tratamiento de su información personal, y demás derechos que otorguen permiso en cuanto a la toma de decisión automatizada.

La violencia contra la mujer que se vive hoy en día por las tecnologías de la información y comunicación es real e impacta a las víctimas y personas de forma psicológica, emocional y profesional. Miles de mujeres han sufrido este tipo de violencia y en muchas ocasiones son revictimizadas por las propias autoridades.

La tipificación de las conductas cometidas a través de los medios digitales es una necesidad imperante ante casos de mujeres que han sido afectadas en su vida privada, al ser dadas a conocer por dichas vías imágenes, audios o videos de su intimidad sexual al compartirlas, divulgarlas o publicarlas sin su consentimiento.

Reconocer un problema tan profundo y delicado y plasmar en nuestro orden jurídico el delito de violencia de la intimidad sexual, a través de la Inteligencia Artificial, es un esfuerzo que nos permite enfrentarlo, dar a la autoridad las herramientas necesarias para ello y a la sociedad la tranquilidad de que se sigue avanzando en este tema.

Se entiende como violencia digital aquellas acciones en las que se expongan, difundan o reproduzcan imágenes, audios o videos de contenido sexual íntimo de una persona sin su consentimiento, a través de medios tecnológicos y que por su naturaleza atentan contra la integridad, la dignidad y la vida privada de las mujeres causando daño psicológico, económico o sexual tanto en el ámbito privado como en el público, además de daño moral, tanto a ellas como a sus familias

Con esta iniciativa, se asegura y protege el espacio digital para sancionar a todas aquellas personas que violenten, divulguen, compartan o comercien imágenes, audios o videos íntimos de una persona sin su consentimiento, utilizando la Inteligencia Artificial.

Se incorpora en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia, toda acción dolosa realizada mediante el uso de tecnologías de la información, e inteligencia artificial y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmite, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.

Las reformas al Código Penal Federal, por su parte, tipifican el delito de Violación a la Intimidad Sexual, señalando que lo comete aquella persona que divulgue, comparta, distribuya o publique imágenes, videos o audios de contenido íntimo sexual de una persona que tenga la mayoría de edad, sin su consentimiento, su aprobación o su autorización, a través de la inteligencia artificial.

Por lo expuesto, y con el objeto de mostrar de manera más clara las modificaciones que se pretende llevar a cabo en la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia y en el Código Penal Federal, se presentan los siguientes cuadros:

LEY GENERAL DE ACCESO DE LAS MUJERES A UNA VIDA LIBRE DE VIOLENCIA	
ARTÍCULO 20 Quáter.- Violencia digital es toda acción dolosa realizada mediante el uso de tecnologías de la información y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia. Así como aquellos actos dolosos que causen daño a la intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación. Para efectos del presente Capítulo se entenderá por Tecnologías de la Información y la Comunicación aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos. La violencia digital será sancionada en la forma y términos que establezca el Código Penal Federal.	**ARTÍCULO 20 Quáter.-** Violencia digital es toda acción dolosa realizada mediante el uso de tecnologías de la información, **la inteligencia artificial** y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia. Así como aquellos actos dolosos que causen daño a la intimidad, privacidad y/o dignidad de las mujeres, que se cometan por medio de las tecnologías de la información y la comunicación. Para efectos del presente Capítulo se entenderá por Tecnologías de la Información y la Comunicación aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos **o aquellas que se utilicen con inteligencia artificia**l. La violencia digital será sancionada en la forma y términos que establezca el Código Penal Federal.
ARTÍCULO 20 Sexies.- Tratándose de violencia digital o mediática para garantizar la integridad de la víctima, la o el Ministerio Público, la jueza o el juez, ordenarán de manera	**ARTÍCULO 20 Sexies.-** Tratándose de violencia digital o mediática para garantizar la integridad de la víctima, la o el Ministerio Público, la jueza o el juez, ordenarán de manera

inmediata, las medidas de protección necesarias, ordenando vía electrónica o mediante escrito a las empresas de plataformas digitales, de medios de comunicación, redes sociales o páginas electrónicas, personas físicas o morales, la interrupción, bloqueo, destrucción, o eliminación de imágenes, audios o videos relacionados con la investigación previa satisfacción de los requisitos de Ley. En este caso se deberá identificar plenamente al proveedor de servicios en línea a cargo de la administración del sistema informático, sitio o plataforma de Internet en donde se encuentre alojado el contenido y la localización precisa del contenido en Internet, señalando el Localizador Uniforme de Recursos. La autoridad que ordene las medidas de protección contempladas en este artículo deberá solicitar el resguardo y conservación lícita e idónea del contenido que se denunció de acuerdo a las características del mismo. Las plataformas digitales, medios de comunicación, redes sociales o páginas electrónicas darán aviso de forma inmediata al usuario que compartió el contenido, donde se establezca de forma clara y precisa que el contenido será inhabilitado por cumplimiento de una orden judicial. Dentro de los cinco días siguientes a la imposición de las medidas de protección previstas en este artículo deberá celebrarse la audiencia en la que la o el juez de control podrá cancelarlas, ratificarlas o modificarlas considerando la información disponible, así como la irreparabilidad del daño.	inmediata, las medidas de protección necesarias, ordenando vía electrónica o mediante escrito a las empresas de plataformas digitales, de medios de comunicación, redes sociales o páginas electrónicas **o aplicación de inteligencia artificial,** personas físicas o morales, la interrupción, bloqueo, destrucción, o eliminación de imágenes, audios o videos relacionados con la investigación previa satisfacción de los requisitos de Ley. En este caso se deberá identificar plenamente al proveedor de servicios en línea a cargo de la administración del sistema informático, sitio o plataforma de Internet en donde se encuentre alojado el contenido y la localización precisa del contenido en Internet, señalando el Localizador Uniforme de Recursos. La autoridad que ordene las medidas de protección contempladas en este artículo deberá solicitar el resguardo y conservación lícita e idónea del contenido que se denunció de acuerdo a las características del mismo. Las plataformas digitales, medios de comunicación, redes sociales, páginas electrónicas **o aplicación de inteligencia artificial**, darán aviso de forma inmediata al usuario que compartió el contenido, donde se establezca de forma clara y precisa que el contenido será inhabilitado por cumplimiento de una orden judicial. Dentro de los cinco días siguientes a la imposición de las medidas de protección previstas en este artículo deberá celebrarse la audiencia en la que la o el juez de control podrá cancelarlas, ratificarlas o modificarlas considerando la información disponible, así como la irreparabilidad del daño.

CÓDIGO PENAL FEDERAL	
Artículo 199 Nonies.- Se impondrán las mismas sanciones previstas en el artículo anterior cuando las imágenes, videos o audios de contenido íntimo sexual que se divulguen, compartan, distribuyan o publiquen no	**Artículo 199 Nonies.-** Se impondrán las mismas sanciones previstas en el artículo anterior cuando las imágenes, videos o audios de contenido íntimo sexual que se divulguen, compartan, distribuyan o publiquen no

correspondan con la persona que es señalada o identificada en los mismos.	correspondan con la persona que es señalada o identificada en los mismos **o cuyas imágenes hayan sido manipuladas a través de la inteligencia artificial.**

Por lo anteriormente expuesto y fundado, someto a consideración de esta soberanía la siguiente iniciativa con proyecto de

Artículo Primero. Se reforman los artículos los artículos 20 Quáter párrafo primero, 20 Quáter párrafo tercero, 20 Sexies parrafo primero y 20 Sexies párrafo cuarto de la Ley General d Acceso de las Mujeres a una Vida Libre de Violencia, para quedar como sigue:

ARTÍCULO 20 Quáter.- Violencia digital es toda acción dolosa realizada mediante el uso de tecnologías de la información, **la inteligencia artificial** y la comunicación, por la que se exponga, distribuya, difunda, exhiba, transmita, comercialice, oferte, intercambie o comparta imágenes, audios o videos reales o simulados de contenido íntimo sexual de una persona sin su consentimiento, sin su aprobación o sin su autorización y que le cause daño psicológico, emocional, en cualquier ámbito de su vida privada o en su imagen propia.

Para efectos del presente Capítulo se entenderá por Tecnologías de la Información y la Comunicación aquellos recursos, herramientas y programas que se utilizan para procesar, administrar y compartir la información mediante diversos soportes tecnológicos **o aquellas que se utilicen con inteligencia artificia**l

---

ARTÍCULO 20 Sexies.- Tratándose de violencia digital o mediática para garantizar la integridad de la víctima, la o el Ministerio Público, la jueza o el juez, ordenarán de manera inmediata, las medidas de protección necesarias, ordenando vía electrónica o mediante escrito a las empresas de plataformas digitales, de medios de comunicación, redes sociales o páginas electrónicas **o aplicación de inteligencia artificial,** personas físicas o morales, la interrupción, bloqueo, destrucción, o eliminación de imágenes, audios o videos relacionados con la investigación previa satisfacción de los requisitos de Ley.

Las plataformas digitales, medios de comunicación, redes sociales, páginas electrónicas **o aplicación de inteligencia artificial**, darán aviso de forma inmediata al usuario que compartió el contenido, donde se establezca de forma clara y precisa que el contenido será inhabilitado por cumplimiento de una orden judicial.

Articulo Segundo. Se reforma el articulo199 Nonies del Código Penal Federal, para quedar como sigue:

Artículo 199 Nonies.- Se impondrán las mismas sanciones previstas en el artículo anterior cuando las imágenes, videos o audios de contenido íntimo sexual que se divulguen, compartan, distribuyan o publiquen no correspondan con la persona que es señalada o identificada en los mismos **o cuyas imágenes hayan sido manipuladas a través de la inteligencia artificial.**

Transitorio

Único. El presente decreto entrará en vigor el día siguiente al de su publicación en el Diario Oficial de la Federación.

Notas

https://www.oracle.com/mx/artificial-intelligence/what-is-ai/#:~:text=La%20inteligencia%20artificial%20(IA)%20se,clientes%20o%20jugar%20al%20ajedrez
http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://documents-dds-ny.un.org/doc/UNDOC/GEN/G21/249/24/PDF/G2124924.pdf?OpenElement
Usan Inteligencia Artificial para crear contenido íntimo
radioformula.com.mx
bufetejuridicogratuito.org.mx
https://www.bufetejuridicogratuito.org.mx › News
https://www.itmastersmag.com/noticias-analisis/delitos-informaticos-en-mexico-que-dice-la-ley/#:~:text=El%20C%C3%B3digo%20Penal%20Federal%20mexicano,para%20est

Dado en el salón de sesiones de la Comisión Permanente, a 25 de julio de 2023.

DIPUTADA MELISSA ESTEFANÍA VARGAS CAMACHO