CIUDAD DE MÉXICO A 15 DE OCTUBRE DE 2024

DIP. MARTHA ÁVILA VENTURA, PRESIDENTA DE LA MESA DIRECTIVA, DEL CONGRESO DE LA CIUDAD DE MÉXICO, III LEGISLATURA.

PRESENTE

Honorable Congreso de la Ciudad de México:

La que suscribe **Diputada Ana Luisa Buendía García,** integrante del Grupo Parlamentario de MORENA del Congreso de la Ciudad de México, III Legislatura, con fundamento en los artículos 122 apartado A, fracciones I y II párrafo 5 de la Constitución Política de los Estados Unidos Mexicanos; 29 Apartado D, inciso a) y 30 numeral 1, inciso b) de la Constitución Política de la Ciudad de México; 12 fracción II, y 13 párrafo primero de la Ley Orgánica del Congreso de la Ciudad de México; 5 fracciones I y II, 82, 95 fracción II, 96, 325 y 326 (Cámara de Diputados), todos del Reglamento del Congreso de la Ciudad de México, someto a consideración de este Pleno la presente **PROPUESTA DE INICIATIVA ANTE EL CONGRESO DE LA UNIÓN, CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UNA FRACCIÓN XXII TER AL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, EN MATERIA DE CIBERSEGURIDAD Y CIBERESPACIO,** lo anterior al tenor de las siguientes consideraciones:

EXPOSICIÓN DE MOTIVOS

La seguridad pública es un derecho esencial que garantiza a todas las personas la paz y una convivencia pacífica y solidaria, permitiéndoles vivir sin amenazas de violencia o delitos. En nuestro país, esta responsabilidad recae en el Estado, cuyo objetivo es proteger la vida, las libertades, la integridad y el patrimonio de las personas, además de contribuir al mantenimiento del orden público y la paz social, como lo establece nuestra Constitución Política Federal.

Este derecho está reconocido como un derecho humano en la Declaración Universal de los Derechos Humanos, la Declaración Americana de los Derechos y Deberes del Hombre, el artículo 7 de la Convención Americana sobre Derechos Humanos y el artículo 9 del Pacto Internacional de Derechos Civiles y Políticos. A nivel nacional, este derecho está consagrado de manera única e indirecta en el artículo 21 de la Constitución Política de los Estados Unidos Mexicanos, cuyos preceptos indican:

Declaración Universal de los Derechos Humanos

> **"***Artículo 3*
>
> *Todo individuo tiene derecho a la vida, a la libertad y a la seguridad de su persona."*

Declaración Americana de los Derechos y Deberes del Hombre

> *"Artículo I. Todo ser humano tiene derecho a la vida, a la libertad y a la seguridad de su persona."*

Convención Americana sobre Derechos Humanos

"ARTÍCULO 7. Derecho a la Libertad Personal

1. Toda persona tiene derecho a la libertad y a la seguridad personales.

2. Nadie puede ser privado de su libertad física, salvo por las causas y en las condiciones fijadas de antemano por las Constituciones Políticas de los Estados Partes o por las leyes dictadas conforme a ellas.

3. Nadie puede ser sometido a detención o encarcelamiento arbitrarios.

4. Toda persona detenida o retenida debe ser informada de las razones de su detención y notificada, sin demora, del cargo o cargos formulados contra ella.

5. Toda persona detenida o retenida debe ser llevada, sin demora, ante un juez u otro funcionario autorizado por la ley para ejercer funciones judiciales y tendrá derecho a ser juzgada dentro de un plazo razonable o a ser puesta en libertad, sin perjuicio de que continúe el proceso. Su libertad podrá estar condicionada a garantías que aseguren su comparecencia en el juicio.

6. Toda persona privada de libertad tiene derecho a recurrir ante un juez o tribunal competente, a fin de que éste decida, sin demora, sobre la legalidad de su arresto o detención y ordene su libertad si el arresto o la detención fueran ilegales. En los Estados Partes cuyas leyes prevén que toda persona que se viera amenazada de ser privada de su libertad tiene derecho a recurrir a un juez o tribunal competente a fin de que éste decida sobre la legalidad de tal amenaza, dicho recurso no puede ser restringido ni abolido. Los recursos podrán interponerse por sí o por otra persona. 7. Nadie será detenido por deudas. Este principio no limita los mandatos de autoridad judicial competente dictados por incumplimientos de deberes alimentarios."

Pacto Internacional de Derechos Civiles y Políticos

"Artículo 9

1. Todo individuo tiene derecho a la libertad y a la seguridad personales. Nadie podrá ser sometido a detención o prisión arbitrarias. Nadie podrá ser privado de su libertad, salvo por las causas fijadas por ley y con arreglo al procedimiento establecido en ésta.

2. Toda persona detenida será informada, en el momento de su detención, de las razones de la misma, y notificada, sin demora, de la acusación formulada contra ella.

3. Toda persona detenida o presa a causa de una infracción penal será llevada sin demora ante un juez u otro funcionario autorizado por la ley para ejercer funciones judiciales, y tendrá derecho a ser juzgada dentro de un plazo razonable o a ser puesta en libertad. La prisión preventiva de las personas que hayan de ser juzgadas no debe ser la regla general, pero su libertad podrá estar subordinada a garantías que aseguren la comparecencia del acusado en el acto del juicio, o en cualquier momento de las diligencias procesales y, en su caso, para la ejecución del fallo.

4. Toda persona que sea privada de libertad en virtud de detención o prisión tendrá derecho a recurrir ante un tribunal, a fin de que éste decida a la brevedad posible sobre la legalidad de su prisión y ordene su libertad si la prisión fuera ilegal.

5. Toda persona que haya sido ilegalmente detenida o presa, tendrá el derecho efectivo a obtener reparación."

Constitución Política de los Estados Unidos Mexicanos.

***"Artículo 21.** La investigación de los delitos corresponde al Ministerio Público y a las policías, las cuales actuarán bajo la conducción y mando de aquél en el ejercicio de esta función.*

El ejercicio de la acción penal ante los tribunales corresponde al Ministerio Público. La ley determinará los casos en que los particulares podrán ejercer la acción penal ante la autoridad judicial.

La imposición de las penas, su modificación y duración son propias y exclusivas de la autoridad judicial.

Compete a la autoridad administrativa la aplicación de sanciones por las infracciones de los reglamentos gubernativos y de policía, las que únicamente consistirán en multa, arresto hasta por treinta y seis horas o en trabajo a favor de la comunidad; pero si el infractor no pagare la multa que se le hubiese impuesto, se permutará esta por el arresto correspondiente, que no excederá en ningún caso de treinta y seis horas.

Si el infractor de los reglamentos gubernativos y de policía fuese jornalero, obrero o trabajador, no podrá ser sancionado con multa mayor del importe de su jornal o salario de un día.

Tratándose de trabajadores no asalariados, la multa que se imponga por infracción de los reglamentos gubernativos y de policía, no excederá del equivalente a un día de su ingreso.

El Ministerio Público podrá considerar criterios de oportunidad para el ejercicio de la acción penal, en los supuestos y condiciones que fije la ley.

El Ejecutivo Federal podrá, con la aprobación del Senado en cada caso, reconocer la jurisdicción de la Corte Penal Internacional.

La seguridad pública es una función del Estado a cargo de la Federación, las entidades federativas y los Municipios, cuyos fines son salvaguardar la vida, las libertades, la integridad y el patrimonio de las personas, así como contribuir a la generación y preservación del orden público y la paz social, de conformidad con lo previsto en esta Constitución y las leyes en la materia. La seguridad pública comprende la prevención, investigación y persecución de los delitos, así como la sanción de las infracciones administrativas, en los términos de la ley, en las respectivas competencias que esta Constitución señala. La actuación de las instituciones de seguridad pública se regirá por los principios de legalidad, objetividad, eficiencia, profesionalismo, honradez y respeto a los derechos humanos reconocidos en esta Constitución.

Las instituciones de seguridad pública, incluyendo la Guardia Nacional, serán de carácter civil, disciplinado y profesional. El Ministerio Público y las instituciones policiales de los tres órdenes de gobierno deberán coordinarse entre sí para cumplir los fines de la seguridad pública y conformarán el Sistema Nacional de Seguridad Pública, que estará sujeto a las siguientes bases mínimas:

a) *La regulación de la selección, ingreso, formación, permanencia, evaluación, reconocimiento y certificación de los integrantes de las instituciones de seguridad pública. La operación y desarrollo de estas acciones será competencia de la Federación, las entidades federativas y los Municipios en el ámbito de sus respectivas atribuciones.*

b) *El establecimiento de un sistema nacional de información en seguridad pública a cargo de la Federación al que ésta, las entidades federativas y los Municipios, a través de las dependencias responsables de la seguridad pública, proporcionarán la información de que dispongan en la materia, conforme a la ley. El sistema contendrá también las bases de datos criminalísticos y de personal para las instituciones de seguridad pública. Ninguna persona podrá ingresar a las instituciones de seguridad pública si no ha sido debidamente certificada y registrada en el sistema.*

c) *La formulación de políticas públicas tendientes a prevenir la comisión de delitos.*

d) *Se determinará la participación de la comunidad que coadyuvará, entre otros, en los procesos de evaluación de las políticas de prevención del delito así como de las instituciones de seguridad pública.*

e) *Los fondos de ayuda federal para la seguridad pública, a nivel nacional serán aportados a las entidades federativas y municipios para ser destinados exclusivamente a estos fines.*

La Federación contará con una institución policial de carácter civil denominada Guardia Nacional, cuyos fines son los señalados en el

párrafo noveno de este artículo, la coordinación y colaboración con las entidades federativas y Municipios, así como la salvaguarda de los bienes y recursos de la Nación.

La ley determinará la estructura orgánica y de dirección de la Guardia Nacional, que estará adscrita a la secretaría del ramo de seguridad pública, que formulará la Estrategia Nacional de Seguridad Pública, los respectivos programas, políticas y acciones.

La formación y el desempeño de los integrantes de la Guardia Nacional y de las demás instituciones policiales se regirán por una doctrina policial fundada en el servicio a la sociedad, la disciplina, el respeto a los derechos humanos, al imperio de la ley, al mando superior, y en lo conducente a la perspectiva de género."

Además de lo mencionado, es importante señalar que, con la entrada en vigor de la Constitución Política de la Ciudad de México, se establecieron las bases para una responsabilidad innovadora, evolucionando de la Seguridad Pública a la Seguridad Ciudadana. Este nuevo concepto progresivo se centra en la importancia de que la sociedad se sienta y esté segura en su persona, bienes, derechos y entorno social. Por ello, la seguridad ciudadana requiere un compromiso conjunto entre la sociedad y el gobierno, siendo un valor fundamental para la cultura cívica.

En este contexto, el Derecho a la Seguridad está reconocido en el artículo 14 de la Constitución Local, el cual establece:

"Artículo 14

Ciudad segura

A. Derecho a la seguridad urbana y a la protección civil

Toda persona tiene derecho a vivir en un entorno seguro, a la protección civil, a la atención en caso de que ocurran fenómenos de carácter natural o antropogénico, así como en caso de accidentes por fallas en la infraestructura de la ciudad. Las autoridades adoptarán las medidas necesarias para proteger a las personas y comunidades frente a riesgos y amenazas derivados de esos fenómenos.

B. Derecho a la seguridad ciudadana y a la prevención de la violencia y del delito

Toda persona tiene derecho a *la convivencia pacífica y solidaria, a* ***la seguridad ciudadana*** *y a vivir libre de amenazas generadas por el ejercicio de las violencias y los delitos. Las autoridades elaborarán políticas públicas de prevención y no violencia, así como de una cultura de paz, para brindar protección y seguridad a las personas frente a riesgos y amenazas."*

En el marco de este sistema jurídico, es evidente que una de las mayores preocupaciones de la sociedad actual es la Seguridad. Esto implica mantener la paz social, proteger la integridad física de las personas y asegurar continuamente las garantías necesarias para el ejercicio pleno de los derechos humanos en un entorno de libertad y convivencia pacífica, donde todos puedan alcanzar su autodeterminación, desarrollo y bienestar colectivo. Sin embargo, en la era digital, la Seguridad Pública ha cobrado una relevancia especial debido al avance de las tecnologías de la información y al incremento de las transacciones comerciales en el ámbito digital, lo que amplía las oportunidades de servicios a nivel global y genera un constante flujo de información personal, económica, política y social.

La pandemia de Covid-19 entre 2019 y 2021 impulsó el uso de dispositivos tecnológicos, plataformas digitales y redes, convirtiéndolos

en elementos esenciales para la vida diaria en hogares, trabajos, educación, instituciones y gobiernos, conectando a grandes comunidades a través de internet.

Sabemos que la tecnología requiere, en algunos casos, sus propias herramientas y estrategias de protección en conectividad para salvaguardar la integridad de las personas y sus derechos fundamentales. Esto incluye proteger el trabajo y la información en manos de instituciones públicas y también las infraestructuras críticas, como los sistemas tecnológicos para el control y automatización de redes de energía, distribución de agua y medios de transporte. No obstante, en nuestro país, el concepto de ciberseguridad se ha vuelto particularmente complejo debido al escaso conocimiento del tema y a la falta de preparación para una nueva política criminal, en la que la delincuencia está más preparada física y profesionalmente que el Gobierno, que es el responsable de garantizar la Seguridad.

La ciberseguridad surgió como respuesta a la preocupación por los ataques de ciberdelincuencia a nivel macro y micro. Su regulación debe adaptarse al contexto necesario para prevenir, combatir y sancionar los numerosos delitos que se cometen a través de las tecnologías de información y comunicación, como el robo, fraude, sabotaje, ataques y daños a los sistemas informáticos. El objetivo principal de la ciberseguridad es proporcionar seguridad en la tecnología de la información o seguridad de la información electrónica.

Este nuevo término en el ámbito del derecho comparado comenzó a ganar relevancia y a ser más utilizado por los países cuando, en mayo de 2021, Estados Unidos declaró el estado de emergencia tras un ciberataque a la mayor red de oleoductos del país. Un grupo de hackers desconectó

completamente y robó más de 100 GB de información del Oleoducto Colonial, que transportaba más de 2.5 millones de barriles diarios, lo que representaba el 45% del suministro de diésel, gasolina y combustible para aviones en la costa este[1].

CIO México, una publicación de International Data Group (IDG), la mayor empresa editora de información relacionada con la computación y líder mundial en servicios de información en tecnología, afirma en su artículo "*El paradigma de una cultura global de ciberseguridad en el mundo empresarial*"[2] que se producen más de 150 mil ciberataques en el mundo, con un promedio diario de 45 millones de ataques online. Sin embargo, en el artículo "*¿Cómo es la 'anatomía de un ciberataque'*?", de la misma redacción, se menciona que, según el Informe de Riesgos Globales 2022 del Foro Económico Mundial, las fallas en ciberseguridad y la desigualdad digital están entre las 10 amenazas más críticas que enfrentará la humanidad en los próximos dos años. De hecho, se estima que para 2030 habrá un intento de ataque malicioso cada dos minutos. En los casos más recientes de ciberataques, el 63% han sido para exfiltrar datos; la extorsión promedio fue de 247 mil dólares y la máxima alcanzó los 240 millones de dólares, ocho veces más que en 2020.

Las instituciones que han estado evaluando el desarrollo de la ciberseguridad son la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo. Estas entidades han estudiado la

[1] BBC News Mundo. (2021, mayo 9). Ciberataque afecta a la mayor red de oleoducto de EE.UU. y provoca estado de emergencia. BBC News Mundo. https://www.bbc.com/mundo/noticias-internacional-57033536
[2] José Luis Becerra Pozas "El paradigma de una cultura global de ciberseguridad en el mundo empresarial". Sitio web: https://cio.com.mx/el-paradigma-de-una-cultura-global-de-ciberseguridad-en-el-mundo-empresarial/

madurez de la ciberseguridad en 32 países de América Latina y el Caribe, basándose en cinco ejes principales:

1. Política y Estrategia de Ciberseguridad;
2. Cultura Cibernética y Sociedad;
3. Educación, Capacitación y Habilidades en Ciberseguridad;
4. Marcos Legales y Regulatorios;
5. Estándares, Organizaciones y Tecnologías.

Dependiendo de las acciones que los países tomen en estas áreas, se mide el nivel de madurez de su capacidad de ciberseguridad, que puede ir desde la etapa inicial, pasando por la formativa, la consolidada, la estratégica, hasta llegar a la dinámica.

Es importante mencionar que la Unión Europea ha liderado la regulación de los ecosistemas digitales desde 2013, promoviendo un modelo para la estabilidad cibernética global basado en derechos y valores como la privacidad y la protección de datos personales. Además, fomenta un espacio digital abierto, libre y seguro, lo cual es una prioridad en la Agenda 2030 para el Desarrollo Sostenible y sus esfuerzos de implementación. La Unión Europea sostiene que una fuerte resiliencia cibernética requiere enfoques colectivos amplios y estructuras eficaces que promuevan la ciberseguridad y permitan responder a los ciberataques en los Estados Miembros.

Es necesario contar con políticas transversales y autonomía estratégica para avanzar en tecnología, apoyadas por expertos cada vez más calificados. Esto debe ir acompañado de normas, reglas y principios voluntarios articulados por el Grupo de Expertos Gubernamentales de

Naciones Unidas. La preparación cibernética es fundamental tanto para el Mercado Único Digital como para la Seguridad y Defensa de la Unión.

Según las experiencias en este campo, se ha identificado que para evaluar el nivel de ciberseguridad de un país se consideran cinco criterios:

1. La capacidad para prevenir ciberataques;
2. La legislación en materia de ciberseguridad;
3. La cooperación con otros países;
4. El nivel de preparación de las organizaciones no gubernamentales;
5. La eficacia del ente regulador a nivel nacional.

En cuanto a América Latina, la realidad es que los países están poco preparados para enfrentar ciberataques. Tanto los gobiernos como las empresas privadas generalmente invierten pocos recursos en este ámbito, con algunas excepciones en áreas específicas de países como Colombia, Argentina y México.

Aunque los países de América Latina no son considerados desarrollados, tienen una alta tasa de conectividad, especialmente en zonas urbanas. Según un estudio del IICA, el BID y Microsoft, el 71% de la población tiene acceso a internet, aunque en las zonas rurales esta cifra es del 37%. En general, la conectividad alcanza el 68%, lo que coloca a la región por encima de África, donde solo el 18% de la población está conectada a internet.

Desde los años noventa, los gobiernos latinoamericanos han sido clave en la expansión de la conectividad mediante el diseño e implementación de

políticas que ampliaron las infraestructuras y facilitaron el acceso a dispositivos.

En marzo de 2016, el Banco Interamericano de Desarrollo (BID) y la Organización de los Estados Americanos (OEA) se enfocaron en ofrecer a los países de América Latina y el Caribe un estado de ciberseguridad y en fortalecer las capacidades nacionales en esta materia. Lamentablemente, los ciberataques han aumentado, evidenciando la vulnerabilidad de la región. Esto llevó a la implementación del nuevo Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), con el objetivo de medir el crecimiento y desarrollo de los Estados Miembros, defenderse de las constantes amenazas cibernéticas y generar oportunidades para que los profesionales del sector se actualicen. Además, los constantes ataques cibernéticos han incrementado el interés de los usuarios en la seguridad cibernética y en la búsqueda de capacitación cada vez más avanzada.

De acuerdo con datos del año 2020, Uruguay ha sido el país calificado en la región con la más alta madurez en estrategias de ciberseguridad[3], Colombia fue el de mayor desarrollo de dicha seguridad en dimensiones de "Política y estrategia" y "Cultura y Sociedad", para el caso de Centro América y México presentaron un nivel superior en las dimensiones de "Cultura y Sociedad" y en "Educación, capacitación y habilidades" mientras que el puntaje ha sido inferior en las dimensiones de "Política y Estrategia" y "Estándares, organizaciones y tecnologías", México en

[3] Centro Nacional de Respuesta a Incidentes de Seguridad Informática. Ciberseguridad: Uruguay lidera en América Latina y el Caribe. 28 de julio de 2020. Sitio web: https://www.gub.uy/centro-nacional-respuesta-incidentes-seguridad-informatica/comunicacion/noticias/ciberseguridad-uruguay-lidera-america-latina-caribe#:~:text=As%C3%AD%20lo%20indica%20el%20reporte,modelo%20de%20madurez%20en%20ciberseguridad

particular presento la mejor posición de la región con madurez en todas las dimensiones, pero el reporte sugiere que debería centrarse en mejorar el despliegue de estándares de seguridad cibernética y controles técnicos, así como fomentar el desarrollo de un mercado de ciberseguridad.

En nuestro país, según el Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones (UIT), México ocupa el puesto 63 de 175 países en términos de preparación en seguridad cibernética. Esto indica un significativo rezago en la regulación de ciberseguridad, no solo en comparación con otros países, sino también frente a los desafíos actuales en esta materia.

Es importante destacar que México representa un mercado enorme con gran potencial de ganancias para los cibercriminales. Algunos ejemplos recientes de ataques a instituciones mexicanas incluyen:

- Los ataques a la Condusef, el SAT y Banxico en julio de 2020.
- El ataque a la Secretaría de la Función Pública en julio de 2020, que expuso las declaraciones patrimoniales de 830 mil funcionarios públicos.
- Un ataque al ISSSTE, que dejó expuesta la información de 551 asegurados en internet durante un tiempo indeterminado.
- El ataque de ransomware a la Lotería Nacional en junio de 2021, donde se encriptó información crítica y se pidió casi un millón de pesos como rescate para no publicar los datos y proporcionar las claves de descifrado.

Para combatir estos casos, el Gobierno Federal cuenta con una Estrategia Nacional de Ciberseguridad, una guía con cuatro ejes: sociedad,

seguridad nacional, economía y gobierno. Sin embargo, según la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID), esta estrategia no ha sido impresa ni se ha convertido en una política de Estado. Cabe mencionar que las empresas mexicanas más vulnerables a los ciberataques son principalmente las pymes.

Durante la segunda legislatura del Congreso de la Ciudad de México se intentó legislar en la materia, por ello, el 14 de agosto de 2023, se llevó a cabo un foro titulado "Ciberseguridad para una Ciudad Innovadora y de Derechos". En este evento, se contó con la participación de diversos expertos en inteligencia artificial y ciberseguridad, entre ellos el especialista Erick Valdepeñas, quien aportó el siguiente enfoque:

> *"…¿Qué necesitamos como mexicanos? una actualización de software legal, ¿Por qué?, Porque estamos todavía muy atrasados que hoy día será un tema de discusión y es un tema un poquito más para el tema de ciberseguridad que es en la siguiente mesa y es donde se estará practicando más de fondo.*
>
> *En el tema legal aquí tenemos este asunto tenemos que empezar con lo básico primero* ***si queremos regular el tema de la de inteligencia artificial tenemos que regular también el ecosistema digital,*** *de entrada, para llegar a la inteligencia artificial primero hay que pasar por el ecosistema digital y ¿cuál es lo principal? diputado, diputadas las personas que nos están viendo, pues yo creo que lo primero es darle facultades al congreso de la unión, primero es darle facultades para que se pueda legislar este tema.*
>
> ***Vamos a empezar por lo básico el artículo 73 de la constitución, pues bueno, son las facultades que tienen los congresos y a partir de eso creo que si nosotros podemos darle una facultad para regular el ecosistema digital estaremos por buen camino.***
>
> *Ahora bien, cuál es el derecho comparado, en derecho internacional, bueno ya que aquí que hago un paréntesis muy breve, nosotros estamos o no estamos con retraso en el tema de la legislación de la inteligencia artificial la respuesta es no, no estamos retrasados porque*

qué creen, a partir del día de mañana 15 de agosto en china por primera vez se aplicará esta esta ley de inteligencia artificial para regularlo, entonces no llevamos nada de retraso y 14 de agosto estamos teniendo este foro no tenemos ningún retraso; ahora bien ¿qué es lo que están regulando los países o qué están regulando también el parlamento europeo o la unión europea? muy sencillo en china a qué se están basando, ellos están basando como lo comentaba nuestros panelistas, al tema de la ética, los valores socialistas fundamentales es algo principal que en china se está solicitando, la moral social y la ética profesional en la aplicación de la inteligencia artificial, y bueno, la única prohibición que se ve así a los cuatro vientos, es prohibido generar contenido que atenten contra la seguridad nacional, y bueno yo creo que esa debería de ser una base para todo, o sea una base para todos los países.

Ahora bien, y hay otro tema muy importante en china referente a la transparencia y la fiabilidad, y este en el caso de Doujin, ¿qué es doujin? es el tik tok, el realmente el origen del tiktok la aplicación de tik tok, pero en china no se llama tiktok, y ellos se enfocaron mucho en este asunto recuerden que ya las redes sociales allá están muy controladas y se tiene otro asunto, entonces ellos tienen su propia red se llama Doujin y este tema que metieron la regulación, pues bueno, fue específicamente para ellos para la transparencia de todo lo que hace esta aplicación.

Ahora bien, ¿qué pasa en el parlamento europeo?, nos vamos de Asia nos vamos a Europa, el parlamento europeo ellos decidieron dividir este tema de la inteligencia artificial en tres aspectos, uno con los de riesgo inaceptable, la inteligencia artificial ellos lo dividen como riesgo inaceptable, son los que considerar una amenaza para las personas y están prohibidas, esto qué quiere decir, que no podemos tener una manipulación cognitiva ninguna inteligencia artificial puede manejarnos por la mente o nosotros la debemos de preparar para que manejen a terceros con la mente; otro ejemplo, el de alto riesgo que son los sistemas de inteligencia artificial que afectan negativamente a la seguridad de los derechos fundamentales, esto qué quiere decir o sea por ejemplo un juguete, los juguetes la aviación los automóviles los dispositivos médicos, todo lo que plantee el parlamento europeo es que todas estas áreas tengan una previa investigación y un previo análisis para ver si se pueden presentar ante el público, O sea,

imagínense un juguete de Inteligencia artificial debe estar bien reglamentado, y eso es lo que la comunidad europea está presentando.

Ahora bien, el otro pues bueno el invitado los sistemas de Inteligencia artificial limitados, eso me voy a ir un poquito más al tema de redes sociales a lo mejor muchos de aquí conocerán lo que es una deepfake o muchos no conocerán, sin embargo, una deepfake se refiere a estos videos donde ponen tu imagen, no sé bailando, haciendo otra cosa, pero no eres tú, realmente solamente pusieron tu cara es como un photoshop pero de video, ese es un deepfake y la gente piensa que es real, y entonces ahí este tema ***es la tercera parte que está regulando de europa***

Ahora bien, con estos tres puntos, con esto que también China ha hecho este derecho comparado, pues podemos asemejarlo mucho con lo que nuestros panelistas nos han manejado, que hablamos de la ética, que hablamos de la moral, hablamos un poco de este los temas de ciberseguridad, todo esto engloba a esta situación.

[…]

Mitos o realidades de la inteligencia artificial en México.

El sesgo social es real, sí la inteligencia artificial sí puede tener un sesgo social, que era lo que se comentaba al inicio de esta ponencia, fue lo primero que se comentó, el Maestro Adrián fue lo primero que comentó, si nos comentó sobre el sesgo.

Referente al trabajo, es real que se va a eliminar muchos trabajos, eso es muy real, pero ojo, eso no quiere decir que se va a quedar que vamos a tener desempleo, ¿por qué?, porque la inteligencia artificial necesita nuevos empleos y los nuevos empleos se refieren al call center, como ya lo comentaron, que van a ser los robots los que comenten, o a lo mejor los cajeros de un estacionamiento también es un primer empleo.

Esos son los que los que van a eliminarse, pero se van a crear nuevos, como las personas que puedan crear un prompt, para pedirle algo a la inteligencia artificial, o sea, es una por otra en el tema laboral.

*Ahora bien, en **la protección de datos**, sí tenemos muchos problemas porque no sabemos hacia dónde va nuestros datos no sabemos hacia dónde va a ir nuestra iris, no sabemos hacia dónde van a ir nuestras huellas, no sabemos hacia dónde va a ir todo lo que hemos producido, porque recordemos que la inteligencia artificial no crea cosas nuevas, la inteligencia artificial es un collage que ya existe de todo lo que tenemos de toda la información, la inteligencia artificial se junta y entonces no crea cosas nuevas, solamente las mezcla y nos las presenta como si fuera nueva y nosotros asumimos que son nuevas, pero no lo son.*

*Ahora bien, las **crisis políticas** pues bueno obviamente vamos a tener políticas con la inteligencia artificial, ya vemos el tema de los deepfakes, las imágenes falsas, todo este asunto, pues bueno pueden crear una perspectiva en el tema de comunicación política a nivel global.*

*Ahora bien en el **tema de la educación** este es un tema que se tiene que también estudiar a fondo, ¿Por qué?, porque hoy somos súper humanos porque somos súper humanos porque estamos mandando un mensaje, porque estamos tomando una foto a través de un celular, y ahí hablamos de los súper humanos pero qué pasa con los superhumanos que nacen en esta época con la inteligencia artificial, ellos van a tener acceso a la inteligencia artificial, pero hay algo bien interesante, y eso digo yo tengo un hijo y un bebé que nace con la inteligencia artificial y me pregunto qué va a pasar si en 15 años yo le quito la inteligencia artificial, ¿se volverá un analfabeta? es la gran duda, y ese es un tema de educación que tenemos que estudiarlo muy a fondo.*

*Y pues bueno, **el tema de propiedad intelectual** el más claro ejemplo, veamos el tema de la chamarra Balenciaga del papa, pues bueno los abogados de balenciaga van a decirle a los abogados del papa, "oye pues esa es mi chamarra, ¿por qué la tiene una imagen, y está pública por todos lados?" entonces el tema de propiedad intelectual, para los abogados será un tema fundamental, y es algo que también se tiene que tomar en este tema de la regulación…"*

Refiriéndonos a lo mencionado por el especialista previamente citado, en esta propuesta de iniciativa se reconoce que la regulación en esta área ha sido insuficiente. Sabemos que en 2020 el Congreso del Estado Libre y Soberano de San Luis Potosí discutió una iniciativa sobre ciberseguridad, y pocas semanas después, un miembro de otra bancada presentó una propuesta similar ante este Órgano Legislativo de la Ciudad de México igualmente en la segunda legislatura.

Esta iniciativa propuso la creación de oficinas estatales de ciberseguridad en coordinación con fiscalías especializadas, además de establecer las obligaciones y responsabilidades de los servidores públicos encargados de su implementación y cumplimiento. Sin embargo, es importante señalar que esta iniciativa, presentada tanto en San Luis Potosí como replicada para el Congreso de la Ciudad de México en su segunda legislatura, tiene un impacto presupuestal anual de $667,368,412.00 (seiscientos sesenta y siete millones, trescientos sesenta y ocho mil, cuatrocientos doce pesos 00/100 M.N.). Este gasto es comparable al presupuesto aprobado para la Secretaría de Trabajo y Fomento al Empleo o la Secretaría de Desarrollo Económico para 2022. Por ejemplo, la Secretaría de Pueblos y Barrios Originarios y Comunidades Indígenas Residentes tuvo un presupuesto anual aprobado para 2022 de $164,164,249.00, una cantidad similar al requerimiento trimestral de esta iniciativa local, en caso de ser aprobada por este Congreso, sin contar con las bases, estudios necesarios y políticas de coordinación entre los tres órdenes de gobierno

Requerimientos trimestrales para operar una Ley de Ciberseguridad en

la Capital[4]:

Trimestre	Monto (pesos)
I	166,842,103.0
II	166,842,103.0
III	166,842,103.0
IV	166,842,103.0
Total	**667,368,412.0**

En los últimos años, México ha experimentado un alarmante incremento en la ciberdelincuencia, reflejado en diversos reportes y estudios. Desde el aumento significativo de los delitos cibernéticos durante la pandemia de Covid-19 hasta la preocupante posición de México entre los países más afectados por ciberataques a nivel mundial, la evidencia subraya la urgencia de fortalecer nuestras estrategias de ciberseguridad. Este panorama no solo destaca la vulnerabilidad de nuestras instituciones y ciudadanos, sino también la necesidad imperiosa de implementar medidas efectivas para proteger la información y los recursos digitales en un entorno cada vez más interconectado. A continuación, se presenta una de las noticias y estudios más relevantes que ilustran esta creciente amenaza:

> *"**México, uno de los países más expuestos a la inseguridad digital en 2024***
>
> *La formación en ciberseguridad es clave para enseñar prácticas seguras, como crear contraseñas robustas, identificar estafas de phishing y comprender la importancia de la seguridad digital.*

[4] Unidad de Estudios y Finanzas Públicas del Congreso de la Ciudad de México. 8 de marzo de 2022. Impacto presupuestal de la Iniciativa con proyecto de Decreto por la que se expide la Ley de Ciberseguridad para la Ciudad de México.

Aníbal Rojas

jue 14 marzo 2024 06:03 AM

En la primera mitad de 2023, América Latina ha sido sacudida por más de 63,000 millones de ciberataques, con México y Colombia entre los más afectados. Esta alarmante estadística, respaldada por informes de FortiGuard Labs y Accenture , pone de manifiesto una vulnerabilidad crítica en la seguridad digital de la región.

En estos reportes regionales se indica que más del 50% de las organizaciones están incrementando sus inversiones en ciberseguridad como parte esencial de su transformación digital. Sin embargo, a pesar de este aumento, que asciende a un 82%, un alarmante 55% de las empresas aún se encuentra vulnerable a ataques cibernéticos efectivos.

De toda la región, México, Colombia, Argentina, Chile y Brasil son los países más afectados, lo que resalta la urgente necesidad de estrategias de seguridad más robustas y adaptadas a la realidad regional.

En este sentido, se destaca cómo la creciente dependencia de la tecnología digital ha hecho que la ciberseguridad sea un componente esencial de la infraestructura empresarial y gubernamental. Los informes sugieren que no basta con asignar presupuestos sustanciales a la ciberseguridad, es imperativo adoptar un enfoque holístico y proactivo. Esto incluye la implementación de controles de seguridad avanzados, la formación continua del personal y la creación de una cultura organizacional centrada en la seguridad digital.

En respuesta a esta situación, existen algunas estrategias clave para fortalecer la ciberseguridad en México y otros países afectados. Entre ellas, la plataforma de educación en línea Platzi, en donde se ofrecen diversidad capacitaciones sobre ciberseguridad, recomienda realizar una evaluación de riesgos de ciberseguridad para identificar y abordar vulnerabilidades que podrían ser explotadas por atacantes, proceso en el que se incluyen la identificación de activos, análisis de amenazas, evaluación de riesgos y recomendaciones para su mitigación.

Realizar estas evaluaciones al menos una vez al año es esencial, especialmente para organizaciones que manejan datos sensibles o que operan en industrias reguladas.

También, la capacitación en ciberseguridad para el personal, ya que el 95% de las violaciones de ciberseguridad se debe a errores humanos, según el Foro Económico Mundial. La formación en ciberseguridad es clave para enseñar prácticas seguras, como crear contraseñas robustas, identificar estafas de phishing y comprender la importancia de la seguridad digital. Además, crear políticas de seguridad claras y concisas para proteger los sistemas, datos y empleados de tu empresa.

Estas políticas deben también ser fácilmente comprensibles, incluyendo aspectos como la creación de contraseñas seguras, la encriptación de datos y los procedimientos en caso de un ataque cibernético.

Por otro lado, implementar controles de seguridad, los cuales son esenciales para prevenir, detectar y responder a incidentes cibernéticos. Estos controles incluyen firewalls, antivirus, sistemas de detección y prevención de intrusiones, y prácticas como la filosofía de zero trust y el principio de mínimo privilegio. Estos controles ayudan a proteger tu red y tus sistemas de posibles amenazas.

Asimismo, también impulsar la encriptación de datos para proteger la información confidencial. Este proceso implica convertir datos sensibles en un código ilegible, accesible solo a través de una clave de descifrado, tanto en el almacenamiento como en la transmisión de datos, incluyendo dispositivos móviles y redes internas.

Por último, también es relevante diseñar un plan de respuesta a incidentes, que debe incluir la definición de incidentes, la selección de un equipo de respuesta, procedimientos de respuesta detallados y estrategias de comunicación. Este plan debe ser claro y detallado para permitir una respuesta rápida y efectiva ante cualquier violación de seguridad.

El panorama de la ciberseguridad en América Latina exige una atención urgente y coordinada. Las organizaciones deben no solo fortalecer sus defensas internas, sino también participar en la cooperación internacional y el intercambio de inteligencia sobre amenazas. Solo a través de un enfoque integral y colaborativo

podremos abordar eficazmente los desafíos de la ciberseguridad en nuestra era digital."[5]

Aunado a lo anterior, el medio de comunicación EL PAIS, destaca que México es el único país latinoamericano incluido en un ranking mundial de cibercriminalidad, **ocupando el noveno** puesto según un estudio de la firma de seguridad informática Surfshark. Se menciona que 1,100 usuarios mexicanos reportaron ser víctimas de fraude en línea, aunque la cifra real podría ser mayor debido a la falta de reportes. Además, la página incluye información sobre la suscripción digital de EL PAÍS, indicando que para compartir una cuenta se debe optar por la modalidad Premium, y ofrece recomendaciones para cambiar la contraseña si se sospecha de un uso no autorizado[6].

En ese orden de ideas, podemos afirmar que la Ciudad de México ha experimentado un aumento significativo en los ciberdelitos, especialmente contra mujeres, con un incremento del 315% entre enero y febrero de este año en comparación con el mismo periodo de 2021[7].

Los ciberdelitos incluyen robo de identidad, ciberacoso, ciberbullying y malware, afectando principalmente a mujeres y personas mayores.

[5] Rojas, A. (2024, marzo 14). México, uno de los países más expuestos a la inseguridad digital en 2024. Expansión. Recuperado de https://expansion.mx/opinion/2024/03/14/mexico-uno-de-los-paises-mas-expuestos-a-la-inseguridad-digital-en-2024

[6] El País. (2023, mayo 12). México está entre los 10 países con más cibercrímenes en el mundo. El País. Recuperado de https://elpais.com/mexico/2023-05-12/mexico-esta-entre-los-10-paises-con-mas-cibercrimenes-en-el-mundo.html

[7] R. Pansza, Arturo. (2024). Ciudad de México es la entidad más vulnerable a la ciberdelincuencia. La Prensa. Recuperado de https://www.la-prensa.com.mx/metropoli/cdmx-es-la-entidad-mas-vulnerable-a-la-ciberdelincuencia-9151478.html

WhatsApp es una de las plataformas más vulneradas, con fraudes y hackeos frecuentes.

Actualmente las autoridades como la Secretaría de Seguridad Ciudadana a nivel local o el consejo para la seguridad y justicia de la Ciudad de México, recomiendan respaldar evidencia digital y contactar a instituciones financieras si la información bancaria está comprometida. Para asistencia jurídica gratuita, se puede acudir al Consejo Ciudadano para la Seguridad y Justicia de la Ciudad de México. También se pueden reportar delitos cibernéticos a la Policía Cibernética y la Guardia Nacional. Lo anterior, por el momento, es crucial mantener las aplicaciones actualizadas y configurar la verificación en dos pasos para proteger la información personal.

I. Propuesta de Solución:

Es evidente que aún queda mucho por avanzar en la regulación de los ecosistemas digitales, la inteligencia artificial, la ciberseguridad y los ciberdelitos. Sin embargo, es crucial contar con voluntad política para regular el ciberespacio, una propuesta que lleva años sin concretarse y que los nuevos modus operandi usando la tecnología nos demandan a las y los legisladores urgir expedir la ley que lo regule.

La presente Iniciativa, al ser analizada y eventualmente aprobada, debe enriquecerse con aportaciones de especialistas para una regulación adecuada del ciberespacio. El objetivo es que la ciberseguridad y el ciberespacio sean reglamentados a nivel federal, con el Congreso de la

Unión estableciendo las bases para proteger a la ciudadanía de ciberataques y ciberdelitos en las entidades federativas, municipios y alcaldías, donde estos incidentes están en aumento.

En consecuencia, se propone adicionar la fracción XXIII Ter al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, otorgando al Congreso de la Unión la facultad para expedir la Ley General en materia de Ciberespacio y Ciberseguridad. Esta ley debería establecer al menos:

a) **Regulación de ecosistemas digitales**: Normas y autoridades competentes en educación, ciberseguridad, ciberdelitos, protección de datos personales y propiedad intelectual;

b) **Coordinación intergubernamental**: Reglas para la coordinación entre autoridades federales, estatales y municipales para una organización y funcionamiento adecuados en ciberseguridad, y

c) **Supervisión de políticas públicas**: Aspectos relacionados con la coordinación, aplicación y supervisión de políticas públicas en ecosistemas digitales y ciberseguridad.

De tal manera que la propuesta quedaría de la siguiente manera:

CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS

TEXTO VIGENTE	TEXTO PROPUESTO
Sección III **De las Facultades del Congreso**	**Sección III** **De las Facultades del Congreso**

Artículo 73. El Congreso tiene facultad: I… XXII Bis… XXIV… a XXXII…	**Artículo 73.** El Congreso tiene facultad: I… XXII Bis… **XXII Ter. Para expedir la Ley General en materia de Ciberespacio y Ciberseguridad, que establezca:** **a) Las reglas y la autoridad facultada para regular los ecosistemas digitales en materia de educación, ciberseguridad y ciberdelitos, protección de datos personales y de propiedad intelectual;** **b) Las reglas de coordinación entre las autoridades correspondientes de la Federación, las entidades federativas y los municipios, para la adecuada organización y funcionamiento en materia de ciberseguridad, y** **c) Los aspectos vinculados a la coordinación, aplicación y supervisión de las políticas públicas en materia de ecosistemas digitales y ciberseguridad.** **XXIV**… a **XXXII**…

Con base en los razonamientos antes precisados, la suscrita Diputada, propone al Pleno de este Congreso de la Ciudad de México III Legislatura, la presente **PROPUESTA DE INICIATIVA ANTE EL CONGRESO DE LA UNIÓN, CON PROYECTO DE DECRETO POR EL QUE SE ADICIONA UNA FRACCIÓN XXII TER AL ARTÍCULO 73 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, EN MATERIA DE CIBERSEGURIDAD Y CIBERESPACIO,** para quedar de la siguiente manera:

DECRETO

ÚNICO. Se adiciona la fracción XXII Ter al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, para quedar como sigue:

Artículo 73. El Congreso tiene facultad:

I… XXII Bis…

XXII Ter. Para expedir la Ley General en materia de Ciberespacio y Ciberseguridad, que establezca:

a) Las reglas y la autoridad facultada para regular los ecosistemas digitales en materia de educación, ciberseguridad y ciberdelitos, protección de datos personales y de propiedad intelectual;

b) Las reglas de coordinación entre las autoridades correspondientes de la Federación, las Entidades Federativas y los Municipios, para la adecuada organización y funcionamiento en materia de ciberseguridad, y

c) Los aspectos vinculados a la coordinación, aplicación y supervisión de las políticas públicas en materia de ecosistemas digitales y ciberseguridad.

XXIV… a XXXII…

TRANSITORIOS

PRIMERO. Remítase a la Cámara de Diputados del H. Congreso de la Unión para el trámite legislativo respectivo.

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

TERCERO. Remítase al titular del Poder Ejecutivo Federal para su publicación en el Diario Oficial de la Federación.

CUARTO. Dentro del plazo de un año siguiente a la entrada en vigor del presente Decreto, el Congreso de la Unión deberá expedir la ley General en materia de Ciberespacio y Ciberseguridad a que hace referencia el artículo 73, fracción XXIII Ter de esta Constitución.

QUINTO. Dentro del plazo de 180 días naturales siguientes a la entrada en vigor de la Ley a que se refiere el artículo 73, fracción XXIII Ter de esta Constitución, las legislaturas de las Entidades

Federativas deberán expedir la legislación necesaria para adecuar el marco normativo con este Decreto y la ley citada.

Dado en el Recinto del Congreso de la Ciudad de México, III Legislatura, a los quince días del mes de octubre del año dos mil veinticuatro.

ATENTAMENTE

DIP. ANA BUENDÍA GARCÍA

DISTRITO IV