PRESIDENCIA DE LA MESA DIRECTIVA, DEL CONGRESO DE LA CIUDAD DE MÉXICO, II LEGISLATURA.

PRESENTE

Los que suscriben **el Diputado Nazario Norberto Sánchez y el Diputado Christian Moctezuma González**, integrantes del Grupo Parlamentario de MORENA del Congreso de la Ciudad de México, II 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, todos del Reglamento del Congreso de la Ciudad de México, sometemos a consideración de este Pleno la **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,** al tenor de las consideraciones siguientes:

I. Planteamiento del problema que se pretende resolver:

La seguridad pública es un derecho fundamental, que implica que todas las personas tengan paz, una convivencia pacífica y solidaria, es decir, a vivir libre de amenazas generadas por el ejercicio de cualquier tipo de violencia y la comisión de delitos; en nuestro país, es una función a cargo del Estado, cuya finalidad es 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, lo anterior se puede observar en nuestra Constitución Política Federal.

Es importante señalar que esta prerrogativa se encuentra reconocida como un derecho humano en la Declaración Universal de los Derechos Humanos, la Declaración Americana de los Derechos y Deberes del Hombre, en el artículo 7 de la Convención Americana sobre Derechos Humanos y en el artículo 9 del Pacto Internacional de Derechos Civiles y Políticos, y por lo que hace a nivel Nacional, este derecho se encuentra consagrado única e indirectamente en el artículo 21 de la Constitución Política de los Estados Unidos Mexicanos; preceptos que a la letra señalan:

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."*

Aunado a lo anterior, es preciso señalar que en la Capital con la entrada en vigor de la Constitución Política de la Ciudad de México, se centraron las bases sobre las cuales se asumió una responsabilidad innovadora, pasando de la Seguridad Pública a la Seguridad Ciudadana, un nuevo concepto progresivo donde su importancia radica en que una sociedad se sienta y esté segura tanto en su persona, sus bienes, sus derechos, como en su entorno social; es por ello que la seguridad ciudadana implica un compromiso conjunto entre la sociedad y el gobierno, como un valor fundamental para la cultura cívica.

Bajo esa premisa, en primera instancia el **Derecho a la Seguridad** se encuentra reconocido en la Constitución Local en el artículo 14, mismo que prevé:

> ***"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."*

Ante este andamiaje jurídico, sabemos que una de las mayores preocupaciones de la sociedad actual, sin lugar a dudas es la Seguridad, es decir la preservación de la paz social, la integridad física de las personas y desde luego la búsqueda continua de las garantías necesarias para el debido ejercicio de todos y cada uno de los derechos humanos en un ambiente de libertad y tranquila convivencia, en la que todos puedan alcanzar su autodeterminación, desarrollo y bienestar colectivo, sin embargo, es una realidad que nos encontramos en una época digital en la que la Seguridad Pública se ve en un importante foco de atención, pues las tecnologías de la información están al día, pues cada vez va en aumento el número de operaciones comerciales en el ámbito digital, lo cual expande las oportunidades de servicios a nivel global. Esto se traduce en un crecimiento constante en el flujo de información personal, económica, política y social.

Hay que decir, que la pandemia por el Covid-19 en los años 2019 a 2021, favoreció el uso de los dispositivos tecnológicos, plataformas digitales, redes, convirtiéndose estos en una parte fundamental para la operatividad de la vida diaria en hogares,

empleos, educación, instituciones y gobiernos, conectando a grandes comunidades en la sociedad de la información por medio de conexión a internet.

Sabemos que la tecnología es una herramienta que en algunos casos exige sus propios instrumentos y estrategias de protección en conectividad, esto con el fin de salvaguardar la integridad de las personas y de sus derechos fundamentales, por ejemplo, para proteger el trabajo y la información en manos de las instituciones públicas y por supuesto proteger también las infraestructuras críticas como son los Sistemas Tecnológicos para el control y automatización de redes de energía, de distribución de agua, de Medios de Transporte, entre otros; sin embargo, lo cierto es que en el caso particular de nuestro País, el término que ha surgido de ciberseguridad se convirtió en un tema particularmente complejo durante este tiempo, lo anterior en razón de contar con poco conocimiento del tema, y por no encontrarse preparado para una nueva política criminal en la que la delincuencia se encuentra inclusive más preparada física y profesionalmente que el Gobierno, que como hemos dicho es el Estado quien debe garantizar la Seguridad.

La Ciberseguridad es una materia que surgió a raíz de la preocupación por los ataques que han surgido tanto a nivel macro como micro, en cuestión de la ciberdelincuencia, y su regulación debe estar encaminada de acuerdo al contexto en el que se necesite, pues lo que se busca que prevenir, abatir y en su caso sancionar los cientos de delitos que se llevan a cabo a través de las tecnologías de información y comunicación, y que su uso se basa principalmente en conductas como robo, fraude, sabotajes, ataques y daños a los sistemas informáticos. Sin duda el principal objetivo de la ciberseguridad, es brindar seguridad de tecnología de la información o seguridad de la información electrónica.

Este nuevo término, en materia de derecho comparado, fue usando con más frecuencia y comenzó a estar en el radar de los países, cuando en mayo de 2021 Estados Unidos de América se declaró el estado de emergencia tras un ciberataque

a la mayor red de oleoductos del país. Un grupo de hackers desconectó por completo y robó más de 100 GB de información del Oleoducto Colonial, que transportaba más de 2,5 millones de barriles por día, el 45% del suministro de diésel, gasolina y combustible que consumen los aviones de la costa este.[1]

CIO México, es una publicación de International Data Group (IDG), la empresa editora más grande de información relacionada con la computación y líder a nivel mundial como proveedor de servicios de información en Tecnología de la información, al respecto, esta editora asevera en el artículo ***"El paradigma de una cultura global de ciberseguridad en el mundo empresarial"***[2] que aproximadamente se producen más de 150 mil ciberataques en el mundo, el promedio al día de ataques online es de 45 millones. Sin embargo, en el artículo ***"¿Cómo es la "anatomía de un ciberataque"?",*** de la misma redacción, señala que de acuerdo con el *Informe de Riesgos Globales 2022*, elaborado por el Foro Económico Mundial, las fallas en ciberseguridad y la desigualdad digital se encuentran entre las 10 amenazas más críticas que enfrentará la humanidad en los próximos dos años. De hecho, se estima que para el año 2030 habrá un intento de ataque malicioso cada dos minutos. Menciona que en los casos más recientes de ciberataques, el 63% han sido para exfiltrar datos; la extorsión promedio fue de 247 mil dólares y la extorsión máxima fue de 240 millones de dólares, ocho veces mayor a la presentada en 2020.

Las Instituciones que han estado analizando el desarrollo de la Ciberseguridad, ha sido la Organización de los Estados Unidos Americanos (OEA) y el Bando

---

[1] https://www.bbc.com/mundo/noticias-internacional-57033536#:~:text=El%20ciberataque%20afect%C3%B3%20a%20una,El%20gobierno%20de%20EE.&text=declar%C3%B3%20este%20domingo%20un%20estado,desde%20la%20noche%20del%20viernes.

[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/

Internacional de Desarrollo, en la que se estudia la madurez de esta materia en 32 países que integran la Región de América Latina y el Caribe, bajo cinco ejes:

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 tomen los países respecto de estas dimensiones, la medición establece un nivel de madurez de la capacidad de ciberseguridad que va de la etapa inicial, pasando por la formativa, la consolidada, la estratégica hasta llegar a la dinámica.

Cabe mencionar que, es la Unión Europea quien a liderado la regulación de los ecosistemas digitales, pues desde el año 2013 ha impulsado un modelo de creación para suscitar la estabilidad cibernética global, basado en derechos y valores como el derecho a la privacidad y protección de datos personales, además de promover el espacio abierto, libre y seguro, lo que además se considera como prioridad de la Agenda 2030 para el Desarrollo Sostenible y los esfuerzos para su puesta en marcha. La Unión Europea sugiere que una resiliencia cibernética fuerte, requiere necesariamente de abordajes colectivos amplios y estructuras eficaces que promuevan la ciberseguridad y se pueda responder a los ciberataques en los Estados Miembros de la Unión Europea.

Se debe contar con enfoques de políticas transversales con autonomía estratégica para avances en la tecnología, esto realizado con expertos cada vez más calificados; sin duda se debe acompañar de normas, reglas y principios de manera voluntaria de los Estados que han sido articulados por el Grupo de Expertos Gubernamentales de Naciones Unidas, es de mencionar que la preparación

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

De acuerdo a las experiencias en esta materia, se ha señalado qué para establecer el nivel de ciberseguridad de un país, se toman en cuenta 5 criterios:

1. La capacidad de prevención de ciberataques;
2. Legislación en materia de ciberseguridad;
3. Cooperación con otros países;
4. El nivel de preparación de las organizaciones no gubernamentales, y
5. La eficacia del ente regulador a nivel nacional.

Por lo que hace a América Latina, la realidad es que los países se encuentran poco preparados en contra de los ciberataques, y los gobiernos y las empresas privadas en general invierten pocos recursos en este rubro, salvo algunos países como Colombia, Argentina y México en algunas áreas.

Pese que los países de América Latina no son países desarrollados, éstos cuentan con una alta tasa de conectividad, en especial en zonas urbanas, de acuerdo al estudio por el IICA, el BID y Microsoft, el 71% de la población ya cuenta con acceso a internet, en tanto que en las zonas rurales existe un rezago del 37%

En general la conectividad alcanza un 68%, lo que nos coloca por encima de África quien cuenta con sólo un 18% de población conectada a internet.

Desde los años noventa, los gobiernos latinoamericanos han sido fundamentales en la masificación de la conectividad o la red por medio de 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 concentraron en ofrecer a los países de la región de América Latina y Caribe, un estado de ciberseguridad y la manera de fortalecer las capacidades nacionales en esa materia; lamentablemente, los

ciberataques se han incrementado, dejando clara la vulnerabilidad que se presenta en esta región del mundo, no obstante, esto trajo como consecuencia la implementación del nuevo Modelo de Madurez de la Capacidad de Ciberseguridad para las Naciones (CMM), con el fin de medir el crecimiento y desarrollo de los Estados Miembros y poder defenderse de las constantes amenazas al espacio cibernético y generar oportunidades para que los profesionales en la rama se actualicen. De igual manera resalta que derivado de los constantes ataques cibernéticos, se incrementó el interés en usuarios por la seguridad cibernética y la búsqueda de capacitación cada vez más sofisticada.

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 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, de acuerdo con el Índice de Ciberseguridad Global (ICG) de la Unión Internacional de Telecomunicaciones (UIT), México ocupa el lugar 63 de 175 países en materia de preparación de seguridad cibernética; eso quiere decir que,

[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

nos encontramos en un importante rezago en cuanto a regulación sobre ciberseguridad; no solo respecto al resto de los países, sino a los desafíos en la materia.

Es importante señalar, que México representa un mercado enorme con gran potencial de ganancias económicas para cibercriminales, ejemplo de ellos son:

- Algunos de los ataques más recientes a instituciones mexicanas, que fueron llevados a cabo contra la Condusef, el SAT y Banxico en julio de 2020
- Los ataques a la Secretaría de la Función Pública en julio de 2020; que expuso la información sobre declaraciones patrimoniales de 830 mil funcionarios públicos
- Uno contra el ISSSTE, que expuso en internet durante un lapso indeterminado de tiempo la información de 551 asegurados del ISSSTE sin protección.
- El ataque de ransomware a la Lotería Nacional en junio de 2021, donde se encriptó información crítica, financiera, interna y de empleados, y como rescate se pidió casi un millón de pesos a cambio de las claves para descifrar esta información y que no se publicara.

A efecto de combatir casos como los anteriores, el Gobierno Federal cuenta con una Estrategia Nacional de Ciberseguridad, una guía rectora con cuatro ejes: sociedad, seguridad nacional, economía y gobierno, pero que según la Organización de los Estados Americanos (OEA) y el Banco Interamericano de Desarrollo (BID) no ha salido impreso y tampoco se ha convertido en una política de Estado. Cabe destacar, que las empresas mexicanas con una vulnerabilidad mayor son quienes sufren más de ciberataques; sin embargo, la gran mayoría de estas son pymes.

Ante este panorama, el pasado 14 de agosto de 2023, el Diputado Christian Moctezuma González, en su calidad de presidente de la Comisión de Ciencia,

Tecnología e Innovación, y el suscrito en mi calidad de presidente de la Comisión de Seguridad Ciudadana, llevamos a cabo un foro denominado ***"Ciberseguridad para una Ciudad Innovadora y de Derechos"*** en la que contamos con diversos expertos en la materia de inteligencia artificial y ciberseguridad, de allí que se obtuvo del especialista Erick Valdepeñas, 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 ***<u>es la tercera parte que está regulando de europa</u>***

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…"*

Retomando lo que dijo el especialista citado anteriormente, en la presente propuesta de iniciativa se coincide en que la regulación en esta materia ha sido escasa, lo único que sabemos es que en 2020 el Congreso del Estado Libre y Soberano de San Luis Potosí puso a discusión una iniciativa en materia Ciberseguridad, y pocas semanas después otro compañero de una Bancada presentó la misma ante este Órgano Legislativo de la Ciudad de México, la Ley Modelo de Ciberseguridad tiene como bases sólidas las investigaciones de *López Torres,* ya que la fue construyendo mientras realizaba la investigación de *Ciberespacio & Ciberseguridad*.

Esta Iniciativa contempla la creación de oficinas estatales de ciberseguridad, en coordinación con fiscalías especializadas, además de obligaciones y responsabilidades de los servidores públicos que deben ejecutarla y hacer valer su cumplimiento, sin embargo, cabe mencionar que de esta Iniciativa presentada tanto en San Luis Potosí y que fue replicada para el Congreso de la Ciudad de México, su impacto presupuestal asciende a un monto anual de $667,368,412.0 (seiscientos sesenta y siete millones, trescientos sesenta y ocho mil, cuatrocientos doce pesos 00/100 M.N.) dicho gasto es un presupuesto cercano al presupuesto aprobado para la Secretaría de Trabajo y Fomento al Empleo o la Secretaría de Desarrollo Económico para 2022, y en el que se hace la comparación, por ejemplo, con la Secretaría de Pueblos y Barrios Originarios y Comunidades Indígenas Residentes esta tuvo un presupuesto anual aprobado para 2022 de $164,164,249.0, un monto

equiparable al requerimiento trimestral de la Iniciativa Local, si es que en este Congreso la aprobáramos, (sin tener las bases, ni los estudios necesarios, además de las políticas necesarias de coordinación para 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**

II. Propuesta de Solución:

Bajo ese contexto, sabemos que aún falta mucho por avanzar con relación a la regulación de los ecosistemas digitales, la inteligencia artificial, la ciberseguridad y los ciberdelitos, sin embargo, es importante considerar que se necesita voluntad política, ya que el tema de regular el ciber espacio, pese a que ya lleva bastantes años su propuesta o intensión de regular, no se ha llevado a cabo, asimismo, es importante señalar que la presente Iniciativa al momento de que sea analizada y en su caso aprobada, debe ser enriquecida con mayores elementos y más enfoques de especialistas para que el ciberespacio pueda ser debidamente regulado.

En consecuencia, en la presente Propuesta de Iniciativa se tiene el propósito de que la Ciberseguridad y el ciberespacio sea reglamentado desde la perspectiva de la

[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.

Federación, y sea el Congreso de la Unión quien siente las bases para que podamos defendernos y defender a la Ciudadanía de los ciberataques y ciberdelitos en las entidades federativas, y desde luego en los Municipios y Alcaldías que, pues como hemos dicho al inicio de esta Iniciativa, cada día se encuentran en aumento.

En ese orden de ideas, se propone adicionar la fracción veintitrés Ter, al artículo 73 de la Constitución Política de los Estados Unidos Mexicanos, a efecto de que el Congreso de la Unión tenga la facultad para expedir la Ley General en materia de Ciberespacio y Ciberseguridad, en la que consideramos que sean establecidas al menos: a) Las reglas y la autoridad facultada para regular los ecosistemas digitales en materia de educación, ciberseguridad y ciberdelitos, protección de datos personales y 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.

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** **Artículo 73.** El Congreso tiene facultad: I… XXII Bis…	**Sección III** **De las Facultades del Congreso** **Artículo 73.** El Congreso tiene facultad: I… XXII Bis… **XXII Ter. Para expedir la Ley General en materia de Ciberespacio y Ciberseguridad, que establezca:**

XXIV… a XXXI…	**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 **XXXI**…

Con base en los razonamientos antes precisados, el suscrito Diputado propone al Pleno de este Congreso de la Ciudad de México, II 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,** 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 XXXI…

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 general de seguridad privada 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 Congreso de la Ciudad de México, a los cinco días del mes de septiembre de 2023.

ATENTAMENTE

Nazario Norberto Sánchez	Christian Moctezuma
DIP. NAZARIO NORBERTO SÁNCHEZ	**DIP. CHRISTIAN MOCTEZUMA GONZÁLEZ**