



**DIP. JESUS SESMA SUAREZ
PRESIDENTE DE LA MESA DIRECTIVA DEL
CONGRESO DE LA CIUDAD DE MÉXICO
III LEGISLATURA
P R E S E N T E**

Quien suscribe, **OLIVIA GARZA DE LOS SANTOS**, Diputada Local integrante del Grupo Parlamentario del Partido Acción Nacional en el Congreso de la Ciudad de México, III Legislatura, con fundamento en lo dispuesto por los artículos 122, numeral A, fracción II de la Constitución Política de los Estados Unidos Mexicanos; 29, Apartado D, inciso a), b); y 30, numeral 1, inciso b), de la Constitución Política de la Ciudad de México; 12, fracción II, 13 fracción LXIV, LXXIV de la Ley Orgánica del Congreso de la Ciudad de México; y 5, fracción I; 95, fracción II; 96; y 118 del Reglamento de Congreso de la Ciudad de México, todos ordenamientos de la Ciudad de México, someto a la consideración de este órgano legislativo la presente **INICIATIVA CON PROYECTO DE DECRETO POR EL QUE SE REFORMA Y ADICIONA LO SIGUIENTE: EL ARTÍCULO 213 BIS AL CÓDIGO PENAL PARA EL DISTRITO FEDERAL; UN PÁRRAFO LA FRACCIÓN III, Y LA MODIFICACIÓN DEL ANTEPENÚLTIMO PÁRRAFO DEL ARTÍCULO 127 DE LA LEY DE PROTECCIÓN DE DATOS PERSONALES EN POSESIÓN DE SUJETOS OBLIGADOS DE LA CIUDAD DE MÉXICO; SE ADICIONA EL ARTÍCULO 64 BIS A LA LEY DE RESPONSABILIDADES ADMINISTRATIVAS DE LA CIUDAD DE MÉXICO; SE MODIFICA LA FRACCIÓN XVIII DEL ARTÍCULO 3 DE LA LEY DE VÍCTIMAS PARA LA CIUDAD DE MÉXICO; SE MODIFICA LA FRACCIÓN X DEL ARTÍCULO 7 DE LA LEY DE ACCESO DE LAS MUJERES A UNA VIDA LIBRE DE VIOLENCIA DE LA CIUDAD DE MÉXICO, LO ANTERIOR CON EL OBJETO DE TIPIFICAR Y COMBATIR LA PRÁCTICA CONOCIDA COMO “DOXING”.** Conforme a lo siguiente:

I. TÍTULO DE LA PROPUESTA.

Iniciativa con proyecto de decreto por el que se adiciona el artículo 213 Bis al Código Penal para el Distrito Federal; un párrafo la fracción III, y la modificación del



antepenúltimo párrafo del artículo 127 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad De México; se adiciona el artículo 64 Bis a la Ley de Responsabilidades Administrativas de la Ciudad de México; se modifica la fracción XVIII del artículo 3 de la Ley de Víctimas para la Ciudad de México; se modifica la fracción X del artículo 7 de la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México, lo anterior con el objeto de tipificar y combatir la práctica conocida como “doxing”.

II. PLANTEAMIENTO DEL PROBLEMA

En un mundo cada vez más interconectado, la forma de interactuar ha cambiado, y la vida cotidiana se ve afectada profundamente por la esfera virtual. En nuestros días cada vez es más raro encontrar a personas que no tengan una huella digital, las redes sociales y las interacciones por internet, se han vuelto igual de importantes que las interacciones presenciales, pues a través de estas podemos ponernos en contacto tanto con personas queridas como con desconocidos.

La razón de las interacciones puede ser por simple ocio como con fines profesionales, pues es extremadamente común que las agencias gubernamentales, políticos y negocios de todo tipo busquen a través de las redes sociales una forma de atraer personas con algún fin específico. Estas interacciones son en su mayoría positivas o inofensivas, sin embargo, hay cada día un número creciente de personas que buscan de manera dolosa generar un efecto negativo en su desarrollo diario.

Una de estas formas es precisamente el doxing, la cual implica la filtración maliciosa de datos sin su consentimiento con la intención de causarle un daño, intimidarla, a través de una exposición que facilite agresiones, hostigamiento, extorsión o persecución en línea y fuera de ella.

El doxing no es un fenómeno aislado, sino una herramienta de poder que se utiliza en contextos variados, desde disputas personales en redes sociales hasta



estrategias de control en conflictos armados o políticos, y su escalada en los últimos años representa una amenaza creciente para la privacidad y la seguridad individual en sociedades como la nuestra en la Ciudad de México.

El doxing se define no solo por la divulgación de información, sino por la intención maliciosa detrás de ella, que puede incluir extorsión, silenciamiento o incluso el fomento de violencia física. Esta práctica sirve para controlar o castigar a personas percibidas como adversarias, mientras que en escenarios de tensión política, se emplea como arma para desestabilizar a oponentes. Esta dualidad subraya la necesidad de abordarla no solo como un delito cibernético, sino como una violación a los derechos humanos fundamentales, ya que erosiona la confianza en el espacio digital y perpetúa desigualdades, particularmente afectando a grupos vulnerables como mujeres, periodistas y activistas.

La relevancia normativa y social del fenómeno del doxing se acentúa cuando la práctica deja de ser un instrumento exclusivo de particulares y pasa a convertirse en una táctica empleada o facilitada por servidores públicos, pues estos muchas veces, manejan bases de datos con información personal de la ciudadanía, lo cual les da la posibilidad de que estos mecanismos se utilicen para intimidar, perseguir o estigmatizar a ciudadanos, periodistas, activistas o personas en situación de vulnerabilidad constituye una forma de violencia de Estado que erosiona derechos fundamentales como la privacidad, la libertad de expresión, la seguridad personal y la igualdad ante la ley.

El simple hecho de que sea un funcionario gubernamental quien cometa la acción de “doxear” genera un efecto intimidatorio y de indefensión, pues las personas que deberían de estar para servir a la población están siendo en la práctica quienes la dañan. Además, al ser cometida por un funcionario público y ser por tanto personas de relevancia para la vida pública, suelen contar con un foro mayor que el de los particulares, lo cual genera que cualquier acción de “doxing” tenga un efecto amplificador de daño, pues se pone al alcance de terceros hostiles para campañas



de hostigamiento, las cuales pueden desarrollarse tanto en el mundo digital como el material.

Ejemplos de “doxing” lo hemos visto de forma palpable como en las elecciones presidenciales pasadas donde tanto el número celular de Claudia Sheinbaum, como el Xóchitl Gálvez fueron filtrados y fueron utilizados con fines de hostigamiento e intimidación¹, lo mismo ha sucedido en casos como el de diputados y senadores de diversas corrientes políticas en las que malos actores buscan entorpecer un proyecto político con el que no están de acuerdo. Ahora bien, aunque resulta preocupante cuando lo hacen a altos perfiles, también lo es que estos suelen también tener un mayor acceso a herramientas y apoyo gubernamental que evita que tenga efectos demasiado perjudiciales para ellos.

La Ley General de Protección de Datos Personales en Posesión de Sujetos Obligados define a los datos personales y los datos personales sensibles de la siguiente forma:

Artículo 3. Para los efectos de la presente Ley se entenderá por:

(...)

IX. Datos personales: Cualquier información concerniente a una persona física identificada o identificable. Se considera que una persona es identificable cuando su identidad pueda determinarse directa o indirectamente a través de cualquier información;

X. Datos personales sensibles: Aquellos que se refieran a la esfera más íntima de su titular, o cuya utilización indebida pueda dar origen a

¹ Redacción El Economista. (26 febrero 2024). *Xóchitl Gálvez, Claudia Sheinbaum y morenistas que denunciaron filtración de sus números telefónicos*. El Economista. <https://www.eleconomista.com.mx/politica/Xochitl-Galvez-Claudia-Sheinbaum-y-morenistas-que-denunciaron-filtracion-de-sus-numeros-telefonicos--20240225-0033.html>



discriminación o conlleve un riesgo grave para éste. De manera enunciativa más no limitativa, se consideran sensibles los datos personales que puedan revelar aspectos como origen racial o étnico, estado de salud presente o futuro, información genética, creencias religiosas, filosóficas y morales, opiniones políticas y preferencia sexual;

Así, los datos personales corresponden a aquella información referente a la identidad de una persona, como pueden ser nombres reales, número telefónico, direcciones, empleos y fotografías, entre otros. Por otro lado, los datos personales sensibles son los concernientes a la esfera íntima de las personas cuya mala utilización provoque discriminación o algún tipo de riesgo grave para la persona.

El jueves 22 de febrero de 2024, en la conferencia de prensa matutina del entonces presidente Andrés Manuel López Obrador, éste mostró un documento enviado por la periodista Natalie Kitroeff consistente en una carta con preguntas para un reportaje sobre la investigación de Estados Unidos a sus campañas presidenciales de 2006 y 2018. En ese acto, el hoy ex presidente también reveló el número telefónico de la periodista, lo cual constituye una práctica conocida como doxing, definida como: “publicar información privada de alguien sin su permiso, y ante una audiencia que puede ser hostil, con la finalidad de perjudicar”.

El doxing por parte de cualquier autoridad constituye un abuso de funciones. En ese sentido, la Ley General de Responsabilidades Administrativas, el abuso de funciones ocurre cuando un “servidor público que ejerza atribuciones (...) para causar perjuicio a alguna persona o al servicio público (...)”.

Por su parte, la filtración de teléfonos de periodistas por parte de autoridades, en aquellos casos en que se trata de periodistas mujeres, también constituye un acto de violencia mediática. En ese sentido, la Ley General de Acceso de las Mujeres a una Vida Libre de Violencia define como violencia mediática 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”.

La encuesta global, encargada por la Unesco y realizada por el Centro Internacional de Periodistas (ICFJ, por sus siglas en inglés), en 2020, reunió datos de más de 1 mil 200 respuestas de todo el mundo. Los resultados iniciales de la encuesta mostraron que:

- El 73 por ciento de las mujeres periodistas que participaron en la encuesta dijeron haber experimentado violencia en línea en el curso de su trabajo, incluyendo amenazas de violencia física y sexual, junto con ataques a la seguridad digital.
- El 20 por ciento de las mujeres periodistas que respondieron a la encuesta dicen que han sido abusadas y atacadas fuera de línea en relación con la violencia en línea que las ataca.

Mientras en el ámbito nacional y de acuerdo con la organización Comunicación e Información de la Mujer (Cimac):

- Tan solo del 1 de abril al 30 de junio de 2022, Cimac registró 44 atentados en contra de mujeres periodistas por el ejercicio de su labor, de las cuales 25 por ciento se efectuaron en el espacio digital.
- El perfil de las periodistas correspondía en un 27.27 por ciento a reportera, 18.18 por ciento a columnista, directora y conductora respectivamente, y 9.09 por ciento a periodista de investigación y a profesora investigadora respectivamente.



- Respecto a la cobertura y tipo de investigación 45.45 por ciento corresponde a Política, 27.27 por ciento a Corrupción, 18.18 por ciento a Megaproyectos y 9.09 por ciento a Congreso.
- En cuanto a las personas agresoras el 27.27 por ciento fue de cuentas falsas, el 18.18 por ciento de usuarios de redes y el 9.09 por ciento a funcionarios estatales, funcionarios municipales, medios locales, militante/ simpatizante, particular, y sin identificar, respectivamente. Es importante destacar que la Cimac identifica como “cuentas falsas” los perfiles que son de reciente creación, su actividad favorece a políticos o partidos, o cuentan con pocos seguidores.
- En relación con los atentados contra la libertad de expresión el 45.45 por ciento se trató de descrédito a la labor, el 27.27 por ciento a amenaza de muerte, el 9.09 por ciento a control y manipulación de la información, robo de identidad y doxing respectivamente. Entendiendo al doxing como la difusión de información personal sin consenso como la dirección, datos de su familia o de su entorno más cercano, lo que expone a las periodistas a agresiones de otro tipo.

El Doxing es una forma de ciberbullying que utiliza información, declaraciones o registros confidenciales o secretos para el acoso, la exposición, el daño financiero u otra explotación de personas objetivo. Este significado de doxing implica tomar información específica sobre alguien y luego difundirla por Internet o a través de algún otro medio para difundirla al público. Esta práctica ha sido ferviente durante muchos años, simplemente porque los documentos contienen registros permanentes de hechos sobre las personas y las cosas que han hecho y dicho, que pueden ser armas poderosas contra ellas, sin embargo, el término “doxing” ganó popularidad por primera vez en la década de 1990 cuando los piratas informáticos comenzaron a dejar documentos en personas que se habían escondido detrás de



nombres falsos. De esta manera, los piratas informáticos podrían exponer a otros atacantes con quienes habían estado en competencia. Eliminar su anonimato los dejó expuestos a las autoridades y a otras personas que intentaban rastrearlos.

El Doxing ha desempeñado un papel prominente en las guerras culturales modernas, que involucran a personas dirigidas a aquellos que apoyan una causa o tienen una creencia que está en oposición a una que están tratando de impulsar.

De cuatro a siete años de prisión se le impondrá como sanción a quien investigue y sustraiga información privada o identificable sobre una persona de equipos de cómputo, redes sociales privadas, sistemas informáticos o teléfonos móviles sin su consentimiento.

Además de que amenace con exhibirla por cualquier medio, ya sea, impreso, grabado o digital, sin su consentimiento, con el fin de lograr que la víctima realice un acto u omisión, contrario a su voluntad, obtener un beneficio personal, o en favor de un tercero.

Así lo propuso, la legisladora del PRI en el Congreso de la Ciudad de México, María de Lourdes González Hernández, quien dijo que esto tiene como propósito combatir el llamado “doxing”, nueva forma de acoso y extorsión “que prácticamente no tiene límites”.

(...)

Asimismo, si esto sea realizado en contra de una mujer, de una persona menores de edad o adulta mayor o si hay relación jerárquica entre las partes involucradas, la sanción se agrava en una tercer parte.

“La violencia en contra de las mujeres, es importante, regular y extinguir aquellas conductas que a través del uso de las tecnologías de la información, se realizan en



contra de ellas, acosándolas, amenazándolas y evitando que puedan llevar una vida plena, libre de cualquier tipo de violencia”, añadió.

Expuso que de acuerdo con el informe “Violencia política a través de las tecnologías contras las mujeres en México”, realizado por el colectivo feminista Luchadoras, en el pasado proceso electoral se identificaron 84 ataques contra 62 candidatas distintas en 24 estados del país.

Es por ello, que se considera que esta práctica es especialmente grave cuando es cometida hacia particulares y aún más, cuando el perpetrador es una persona al servicio del gobierno. Las estadísticas demuestran que la exposición y el acoso a través de medios digitales son fenómenos que afectan a millones de personas en México, con patrones que colocan a mujeres, adolescentes, periodistas y activistas entre los más vulnerables.

Según el Módulo sobre Ciberacoso (MOCIBA) del Instituto Nacional de Estadística y Geografía (INEGI), alrededor del 20.9% de la población usuaria de Internet en 2023 declaró haber vivido alguna situación de acoso cibernético, lo que equivale a decenas de millones de personas, con señales claras sobre las formas predominantes de contacto (identidades falsas, difusión de mensajes ofensivos, amenazas) y sobre la exposición de datos personales como modo de incrementar el daño². Estos indicadores sitúan al ciberacoso, del que el doxing es una forma de ejercerlo, como un problema de seguridad y garantía de derechos humanos que exige respuestas integrales en el plano preventivo, sancionador y reparatorio.

Desde el punto de vista jurídico, México cuenta con un entramado normativo que aborda la protección de datos personales, la comunicación privada y las

² INEGI. (2024). *MÓDULO SOBRE CIBERACOSO (MOCIBA) 2023* [Review of *MÓDULO SOBRE CIBERACOSO (MOCIBA) 2023*]. Inegi.org.mx.
<https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/MOCIBA/MOCIBA2023.pdf>



responsabilidades de los servidores públicos, pero ese marco presenta vacíos, solapamientos y dificultades de implementación que complican la prevención y la sanción efectiva del doxing, sobre todo cuando éste proviene de o está facilitado por actores estatales.

Los incidentes de doxing, se vuelven cada vez más comunes impulsado por la facilidad de acceso a datos personales en la era de las big data y las redes sociales, por ejemplo, un estudio realizado por ONU Mujeres, reveló que entre el 16% y el 58% de las mujeres y niñas han sido blanco de violencia de género en línea, incluyendo el doxing como una de sus manifestaciones más comunes, lo que agrava las desigualdades de género y representa una amenaza significativa para sus derechos y seguridad tanto en el mundo virtual como en el real³.

En el contexto de la Ciudad de México, contamos con leyes que sancionan cuando un servidor público cuando descuida información a su cargo, sin embargo, no se castiga de forma diferenciada cuando la práctica es realizada de forma dolosa, De igual manera la normativa no castiga al servidor público que teniendo en su posesión información sensible, sobre la cual no tuviese un deber de cuidado a priori sobre dicha información, decide utilizarla como mecanismo para atacar o intimidar manera tangible a un particular.

De igual manera en nuestra ciudad capital, no se encuentra regulado las consecuencias para los particulares que difundan información sensible de otros particulares sin su consentimiento con el propósito de generarle un daño, ya sea en el ámbito digital o material, de ahí que sea vital legislar en la materia.

Desde una óptica de derechos humanos, el uso de información personal como recurso de intimidación por parte de servidores públicos vulnera el derecho a la

³ *Crear espacios digitales seguros sin troleo, doxing ni discursos de odio | ONU Mujeres.* (28 junio 2024). ONU Mujeres. <https://www.unwomen.org/es/articles/articulo-explicativo/crear-espacios-digitales-seguros-sin-troleo-doxing-ni-discursos-de-odio>



privacidad y la protección de datos personales reconocidos en la Constitución y en instrumentos internacionales, además de que actúa como un mecanismo de poder que condiciona la libertad de opinión, la participación cívica y el acceso a la justicia, generando un efecto escalofriante de autocensura que las organizaciones o personas críticas al poder gubernamental.

El doxing, por su propia naturaleza facilita la divulgación se combina con campañas de desinformación y con herramientas tecnológicas para amplificar el daño, mediante el uso de bots, grupos de mensajería, foros y plataformas que permiten la viralización inmediata y la persistencia del contenido convierten una filtración puntual en un archivo permanente que reproduce el daño una y otra vez, pues a diferencia de la ofensa verbal pasajera, la información personal publicada en la red es como una huella que puede ser republicada, relanzada y replicada en múltiples dominios lo que dificulta la eliminación total y la reparación del daño. Esta dimensión técnica hace que las respuestas puramente jurídicas resulten insuficientes sin la coordinación tecnológica entre plataformas, autoridades y las propias personas afectadas para remover contenido, rastrear la procedencia y cortar cadenas de republicación

El doxing puede funcionar desgraciadamente como eslabón entre la vida digital y la material, pues con la exposición de información personal como lo podría ser un lugar de residencia o sitio de empleo, facilita la realización de acciones que tengan por objeto el generar miedo o propiciar una agresiones reales que pueden fácilmente desembocar en amenazas directas, acoso en el espacio físico, seguimiento y, en los peores casos, violencia sexual o asesinatos.

La transición entre el plano digital y el daño físico es particularmente preocupante en contextos donde la protección física de las víctimas es insuficiente y donde los grupos criminales u otros actores violentos pueden aprovechar la información divulgada para localizar objetivos. Los datos publicados con intención de hostigar configuran, de esta manera, un facilitador de violencia que exige una respuesta



preventiva y reactiva coordinada entre la política pública de seguridad, la protección a víctimas y las políticas de derechos digitales.

III. PROBLEMÁTICA DESDE LA PERSPECTIVA DE GÉNERO

Haciendo uso de una perspectiva de género, el doxing tiene efectos diferenciados y acumulativos contra las mujeres, pues ellas se encuentran en condiciones de mayor vulnerabilidad pues sufren con más frecuencia la exposición de datos íntimos, amenazas que buscan silenciarlas, así como la circulación de contenido sexual no consentido, aunque en esta última ha habido avances significativos, particularmente desde la existencia de la Ley Olimpia.

Se debe por tanto evitar que la falta de una regulación adecuado abone a la revictimización que ocurre cuando las autoridades no responden con prontitud a la persona afectada. En este sentido, la respuesta estatal debe incluir rutas claras para la atención psicosocial, órdenes de protección digitales y físicas y la garantía de procedimientos que preserven la dignidad de la persona. Datos estadísticos nacionales muestran las dimensiones del fenómeno y la necesidad de políticas transversales que consideren la interseccionalidad de las afectaciones⁴.

La violencia digital adquiere matices particulares cuando se cruza con la violencia de género, la defensa de derechos humanos y el periodismo. Informes de organizaciones internacionales y nacionales muestran que las mujeres y las periodistas son desproporcionadamente atacadas en el espacio digital: estudios de organizaciones como UNESCO y Amnesty International documentaron que la tecnología digital ha servido para acelerar la velocidad y alcance de lenguaje abusivo, amenazas de violencia, dirigidas contra mujeres y personas de la comunidad LGBTTT. En su investigación dicha organización encontró que actores

⁴ INEGI. (2024). *MÓDULO SOBRE CIBERACOSO (MOCIBA) 2023* [Review of *MÓDULO SOBRE CIBERACOSO (MOCIBA) 2023*]. Inegi.org.mx.
<https://www.inegi.org.mx/contenidos/saladeprensa/boletines/2024/MOCIBA/MOCIBA2023.pdf>



maliciosos han utilizado el “doxing” contra numerosas mujeres como táctica de intimidación que busca generar un efecto, de autocensura y daños psicológicos como depresión, ansiedad, en una contraposición clara al derecho de vivir una vida libre de violencia⁵.

El auge de internet, las redes sociales y la conectividad móvil ha facilitado diversas formas de violencia en línea, incluyendo el acoso y el bullying cibernético, el ciberstalking, el discurso de odio en línea basado en el género, los insultos racistas, el abuso sexual mediante imágenes y el doxing.

Estos actos no solo profundizan la brecha digital de género, al disuadir a mujeres y niñas de participar en línea, sino que también extienden el alcance de la violencia de género del ámbito físico al digital. Este cambio representa una grave amenaza para la participación política y la libertad de expresión de las mujeres, especialmente para aquellas involucradas en la política, el periodismo y el activismo. Las jóvenes son particularmente vulnerables, ya que suelen ser víctimas de graves abusos en línea.

Un estudio de la Unión Europea revela que el 73 % de las mujeres ha sufrido acoso en línea (Agencia de los Derechos Fundamentales de la UE, 2014). En Alemania, una encuesta indicó que las mujeres tienen más probabilidades de sufrir acoso cibernético que los hombres. Las Naciones Unidas estiman que el 95 % de las agresiones, el acoso, el lenguaje abusivo y el contenido denigrante en línea se dirigen contra las mujeres⁶.

⁵ Amnesty International. (2024). *BRIEFING: GENDER AND HUMAN RIGHTS IN THE DIGITAL AGE*. Amnesty.org. <https://www.amnesty.org/ar/wp-content/uploads/2024/07/POL4081702024ENGLISH.pdf>

⁶ RECAVARREN, I. S., & ELEFANTE, M. (27 noviembre de 2023). *Protecting women and girls from cyber harassment: a global assessment*. World Bank Blogs. <https://blogs.worldbank.org/en/developmenttalk/protecting-women-and-girls-cyber-harassment-global-assessment>



El acoso cibernético afecta a tres de cada diez mujeres en México, según datos del Instituto Nacional de Estadística y Geografía (INEGI). El país se encuentra entre los diez más afectados del mundo, siendo las mujeres jóvenes de entre 12 y 29 años las más vulnerables debido a su alto uso de las redes sociales.

El aumento del acoso cibernético en México está vinculado al mayor uso de plataformas digitales. Según la Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2023, el ciberacoso y la difusión de contenido íntimo sin consentimiento figuran entre las formas más comunes de violencia digital⁷, entre las que se incluye el “doxing” como una de estas prácticas.

La dimensión de género del problema debe entenderse en términos cuantitativos y cualitativos: cuantitativo pues como ya se ha visto las encuestas nacionales muestran que las mujeres usuarias de Internet en México han experimentado ciberacoso en proporciones superiores a las de los hombres y cualitativamente, porque las formas de agresión tienden a ser diferentes pues se suelen basar en campañas de humillación sexualizada, amenazas de violencia física y la exposición de datos familiares que remiten a mecanismos clásicos de control y dominación que reproducen y amplifican la violencia de género en el entorno digital.

Ese mismo tipo de agresión tiene un efecto doblemente pernicioso cuando proviene de actores vinculados al poder o cuando se combina con prácticas de vigilancia y filtración de datos por parte de funcionarios, pues la amenaza no solo es individual sino estructural, porque busca desactivar la voz pública de las mujeres mediante la intimidación y la posibilidad real de daño físico.

La exposición de datos personales (domicilios, teléfonos, documentación de identidad) se ha mostrado en varios episodios recientes en México como un vector

⁷ INEGI. (2023). *Encuesta Nacional sobre Disponibilidad y Uso de Tecnologías de la Información en los Hogares (ENDUTIH) 2023*. Inegi.org.mx. <https://www.inegi.org.mx/programas/endutih/2023/>



que puede facilitar ataques offline, por lo que su tratamiento exige una mirada que articule derechos digitales y protección física diferenciada respecto de los hombres.

Es por ello que se considera que deben de ser modificadas tanto la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México y la Ley de Víctimas para la Ciudad de México, pues la violencia digital hacia las mujeres va más allá de la violencia sexual, pues el simple hecho de realizar una práctica como el “doxing” puede generar consecuencias graves y especialmente hacia las mujeres.

IV. ARGUMENTOS.

En el contexto de lo narrado anteriormente se considera por tanto que se deben de modificar 3 leyes a fin de atender a dicha problemática los cuales son:

1. Adicionar el artículo 213 Bis al Código Penal para el Distrito Federal;
2. Añadir un párrafo la fracción III, y se modifica el antepenúltimo párrafo del artículo 127 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad De México;
3. Adicionar el artículo 64 Bis a la Ley de Responsabilidades Administrativas de la Ciudad de México.
4. Se modifica la fracción XVIII del artículo 3 de la Ley de Víctimas para la Ciudad de México.
5. Se modifica la fracción X del artículo 7 de la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México

A continuación, se explicarán cada una de las modificaciones propuestas.



El Código Penal del Distrito Federal, contiene en su artículo 213 el delito de revelación de secretos, sin embargo, dicha normativa es insuficiente para el propósito de la presente reforma pues sólo considera delito cuando se revele información reservada, es decir, información sobre la cual tenía un deber de cuidado, y que en la práctica se utiliza en un contexto más empresarial, respecto de secretos o técnicas industriales.

Es por ello que con la actual propuesta se busca tipificar explícitamente el delito de revelación ilícita de datos personales cuando el objeto de esta sea el defraudar, intimidar, amenazar, o buscar el hostigamiento por parte de un tercero, distribuya electrónicamente, publique, envíe por correo electrónico, enlaces o ponga a disposición para su descarga información de identificación personal que genere o busque generar uno o más de los efectos mencionados anteriormente.

Igualmente, dicho artículo prevé mecanismos de control para evitar que sea utilizado como una herramienta de censura al periodismo, pues señala que no se considerará delito cuando la información revelada sea de un servidor público y esta pueda ser considerada de interés general y periodístico.

Conforme lo anterior el artículo quedaría redactado de la manera siguiente:

Artículo 213 Bis. Comete el delito de revelación ilícita de datos personales, toda persona que, con la intención de infundir en otra persona un temor razonable por su seguridad o la de su familia inmediata, mediante un dispositivo de comunicación electrónica, y sin el consentimiento de la otra persona, y con el propósito defraudar, intimidar, amenazar, o buscar el hostigamiento por parte de un tercero, distribuya electrónicamente, publique, envíe por correo electrónico, enlaces o ponga a disposición para su descarga información de identificación personal, que genere o busque generar uno o más de los efectos mencionados anteriormente, se le impondrán prisión de seis meses a dos años y de veinticinco a cien días multa.

Solo se considerará delito, cuando la información revelada no hubiese sido publicada de manera previa por la misma persona denunciante. Tampoco se considerará delito cuando la información revelada sea de un servidor público y esta pueda ser considerada de interés general y periodístico.



Cuando quien cometa la conducta sea un servidor público, la sanción se verá aumentada al doble.

Este delito se perseguirá de querella.

Por otro lado la adición de un párrafo la fracción III, y la modificación del antepenúltimo párrafo del artículo 127 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México, busca que los servidores públicos puedan ser sancionados no únicamente cuando difundan información a la cual tenían acceso por motivo de su cargo, sino cuando cualquier servidor público difunda datos personales de un particular.

Lo anterior se planeo así pues lo que busca es evitar la colusión entre servidores públicos en donde uno filtre información de manera secreta y otro la difunda, pues lo que debe de buscar nuestro ordenamiento jurídico es que los servidores públicos intimiden a los particulares mediante la revelación de información que no debería de ser pública.

Con esta modificación se busca además que los servidores públicos tengan un deber de cuidado de la información personal de los particulares sobre información que no está a su cargo, pero si a su alcance, limitando su responsabilidad a no difundirla por ningún medio.

En este sentido, la redacción del artículo quedaría de la manera siguiente:

127. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes:

(...)

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



También se considerará causa de sanción, cuando un servidor público difunda datos personales de un particular. Lo anterior a pesar de que no hayan provenido con motivo de su cargo, y estos tengan su origen en un tercero.

(...)

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

De igual manera se modifica el ante penúltimo párrafo para convertir la conducta de “doxing” como una que se considere grave.

La adición planteada de un artículo 64 Bis, busca que los servidores públicos puedan ser sancionados administrativa y sean inhabilitados, cuando incurran en practicas como el “doxing” pues es contrario a la más elemental lógica del servicio público el revelar o difundir dolosamente información sensible de los particulares.

En este sentido, la redacción del artículo quedaría de la manera siguiente:

Artículo 64 Bis. Incurran en revelación de datos personales, las personas Servidoras Públicas que difundan por cualquier medio electrónico total o parcialmente y sin el consentimiento expreso de quien pudiese otorgarla, datos personales de particulares con el objeto de infundir en otra persona un temor razonable por su seguridad o la de su familia inmediata. Se entenderán datos personales los establecidos en la fracción IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Como parte de la visión con equidad de género con la cual se redacta la actual propuesta es que se propone modificar la fracción X Artículo 7, de la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México, expandiendo la definición de violencia digital para incluir explícitamente el doxing como una manifestación de esta, sin alterar el enfoque de violencia sexual digital que actualmente contiene dicho artículo.



Esta modificación busca fortalecer las medidas de protección contra la violencia que sufren las mujeres, pues reconoce al “doxing” como una práctica que busca menoscabar su dignidad y causar daños psicológicos, económicos o físicos hacia quienes lo sufren.

En este sentido, la redacción del artículo quedaría de la manera siguiente:

Violencia digital: Es cualquier acto realizado mediante el uso de materiales impresos, correo electrónico, mensajes telefónicos, redes sociales, plataformas de internet, correo electrónico, o cualquier medio tecnológico, por el que se obtenga, exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos reales o simulados o por inteligencia artificial de contenido sexual íntimo de una persona, sin su consentimiento, **así como la difusión no consentida de datos personales identificables, tales como domicilios, números telefónicos, información familiar, laboral o de identificación personal, con la intención de infundir temor, intimidar, hostigar, perseguir o poner en riesgo la seguridad o integridad de la mujer o su familia;** que atente contra la integridad, la dignidad, la intimidad, la libertad, la vida privada de las mujeres o cause 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.

Finalmente se propone la modificación de la fracción XVIII del artículo 3 de la Ley de Víctimas para la Ciudad de México, para incluir la práctica del “doxing” como una conducta comprendida entre lo que debe de ser considerado como un “hecho victimizante”, pues con ello se permitiría que las víctimas de este pudiesen acceder a derechos como asistencia inmediata, reparación integral y asesoría jurídica, todos ellos previstos ya dentro de dicha ley.

En este sentido, la redacción del artículo quedaría de la manera siguiente:

Artículo 3.- Para los efectos de la presente Ley, se entiende por:

(...)



XVIII. Hecho victimizante: Actos u omisiones que dañan, menoscaban o ponen en peligro los bienes jurídicos o derechos de una persona convirtiéndola en víctima. Éstos pueden estar tipificados como delito o constituir una violación a los derechos humanos reconocidos por la Constitución y los Tratados Internacionales de los que México forme parte, y la Constitución Política de la Ciudad de México.

También se considerará un hecho victimizante la revelación o difusión no consentida de datos personales identificables, tales como domicilios, números telefónicos, información familiar o laboral, con la intención de intimidar, hostigar, amenazar o causar daño psicológico, físico o económico, configurando una violación a la privacidad y seguridad personal.

(...)

Una vez explicadas las modificaciones planteadas se procede a señalar la:

V. FUNDAMENTACIÓN LEGAL, DE CONSTITUCIONALIDAD Y CONVENCIONALIDAD

PRIMERO. Que el artículo 1 de la Constitución Política de los Estados Unidos Mexicanos establece que todas las personas gozarán de los derechos humanos reconocidos en la Constitución y en los tratados internacionales de los que el Estado mexicano sea parte, es decir, los derechos reconocidos en la constitución deben de ser aplicadas para todos los habitantes de México, independientemente de su situación migratoria.

SEGUNDO. Que el artículo 16, párrafo segundo, de la Constitución Política de los Estados Unidos Mexicanos, que reconoce el derecho a la protección de los datos personales como un derecho humano fundamental, obligando al Estado a garantizar su resguardo contra injerencias arbitrarias, lo cual justifica la tipificación del doxing como revelación ilícita de datos en el artículo 213 Bis propuesto para el Código Penal del Distrito Federal, ya que esta práctica implica una violación directa a la privacidad al divulgar información identificable sin consentimiento y con intención maliciosa, alineándose con la obligación constitucional de velar por la integridad de



los individuos en el ámbito digital, y respondiendo a la necesidad de adaptar el ordenamiento penal local a las realidades tecnológicas que facilitan tales conductas, sin que ello contravenga otros derechos, pues se limita a sancionar actos intencionales de intimidación o hostigamiento.

SEGUNDO. Que la Constitución Política de los Estados Unidos Mexicanos, en su artículo 21, establece que 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 preservar el orden y la paz públicos. Es deber del Estado garantizar condiciones que permitan el ejercicio pleno de los derechos y libertades de la ciudadanía. Preservar la seguridad pública necesariamente de abarcar la ciberseguridad.

TERCERO. Que la Constitución Política de los Estados Unidos Mexicanos, en su artículo 21, establece que 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 preservar el orden y la paz públicos. Es deber del Estado garantizar condiciones que permitan el ejercicio pleno de los derechos y libertades de la ciudadanía.

CUARTO. Que el artículo 122, inciso A , fracción II, de la Constitución Política de los Estados Unidos Mexicanos, establece que la Ciudad de México es una entidad federativa que goza de autonomía en todo lo concerniente a su régimen interior y a su organización política y administrativa y que por consiguiente el ejercicio del Poder Legislativo se deposita en la Legislatura de la Ciudad de México, la cual se integrará en los términos que establezca la Constitución Política de la entidad.

QUINTO. Que el artículo 7, apartado E, numerales 2, 3 y 4 de la Constitución Política de la Ciudad de México, establecen al derecho a la privacidad y a la protección de



datos personales, así como la prohibición de injerencias arbitrarias en la vida privada

SEXTO. Que la propuesta equilibra la protección de datos con la libertad de expresión y el interés público: el tipo penal requiere, para su consumación, la finalidad intimidatoria (intención de infundir temor razonable) y la ausencia de consentimiento, elementos que delimitan la conducta punible y excluyen de la tipificación la divulgación legítima de información de interés público o actos periodísticos realizados de buena fe.

SÉPTIMO. Que la incorporación de tipos administrativos y penales específicos atiende a la experiencia práctica de impunidad en casos de doxing

OCTAVO. Que es necesario establecer medidas legales que permitan a las autoridades actuar de manera efectiva en la prevención y persecución de delitos, sin menoscabo de los derechos humanos y libertades fundamentales.

VI. TEXTO NORMATIVO PROPUESTO

Por todo lo antes expuesto y fundado, someto a la consideración del Pleno de este órgano legislativo la presente Iniciativa con proyecto de decreto por el que se reforma y adiciona el artículo 213 Bis al Código Penal para el Distrito Federal; un párrafo la fracción III, y la modificación del antepenúltimo párrafo del artículo 127 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad De México; se adiciona el artículo 64 Bis a la Ley de Responsabilidades Administrativas de la Ciudad de México; se modifica la fracción XVIII del artículo 3 de la Ley de Víctimas para la Ciudad de México; se modifica la fracción X del artículo 7 de la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México, en los términos siguientes:



CÓDIGO PENAL PARA EL DISTRITO FEDERAL	
TEXTO VIGENTE	TEXTO DE LA INICIATIVA
Sin correlativo	Artículo 213 Bis. Comete el delito de revelación ilícita de datos personales, toda persona que, con la intención de infundir en otra persona un temor razonable por su seguridad o la de su familia inmediata, mediante un dispositivo de comunicación electrónica, y sin el consentimiento de la otra persona, y con el propósito defraudar, intimidar, amenazar, o buscar el hostigamiento por parte de un tercero, distribuya electrónicamente, publique, envíe por correo electrónico, enlaces o ponga a disposición para su descarga información de identificación personal, que genere o busque generar uno o más de los efectos mencionados anteriormente, se le impondrán prisión de seis meses a dos años y de veinticinco a cien días multa. Solo se considerará delito, cuando la información revelada no hubiese sido publicada de manera previa por la misma persona denunciante. Tampoco se considerará delito cuando la información revelada sea de un servidor público y esta pueda ser considerada de interés general y periodístico. Cuando quien cometa la conducta sea un servidor público, la sanción se verá aumentada al doble. Este delito se perseguirá de querella.



Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México	
TEXTO VIGENTE	TEXTO DE LA INICIATIVA
Artículo 127. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes: (...) III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión; (...) Las causas de responsabilidad previstas en las fracciones I, II, IV, IX, XI y XIII, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa. (...)	Artículo 127. Serán causas de sanción por incumplimiento de las obligaciones establecidas en la materia de la presente Ley, las siguientes: (...) III. Usar, sustraer, divulgar, ocultar, alterar, mutilar, destruir o inutilizar, total o parcialmente y de manera indebida datos personales, que se encuentren bajo su custodia o a los cuales tengan acceso o conocimiento con motivo de su empleo, cargo o comisión; También se considerará causa de sanción, cuando un servidor público difunda datos personales de un particular. Lo anterior a pesar de que no hayan provenido con motivo de su cargo, y estos tengan su origen en un tercero. (...) Las causas de responsabilidad previstas en las fracciones I, II, III, IV, IX, XI y XIII, así como la reincidencia en las conductas previstas en el resto de las fracciones de este artículo, serán consideradas como graves para efectos de su sanción administrativa. (...)



Ley de Responsabilidades Administrativas de la Ciudad de México	
TEXTO VIGENTE	TEXTO DE LA INICIATIVA
Sin correlativo.	Artículo 64 Bis. Incurran en revelación de datos personales, las personas Servidoras Públicas que difundan por cualquier medio electrónico total o parcialmente y sin el consentimiento expreso de quien pudiese otorgarla, datos personales de particulares con el objeto de infundir en otra persona un temor razonable por su seguridad o la de su familia inmediata. Se entenderán datos personales los establecidos en la fracción IX y X de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México.

Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México	
TEXTO VIGENTE	TEXTO DE LA INICIATIVA
Artículo 7. Las modalidades de violencia contra las mujeres son: (...) X. Violencia digital: Es cualquier acto realizado mediante el uso de materiales impresos, correo electrónico, mensajes telefónicos, redes sociales, plataformas de internet, correo electrónico, o cualquier medio tecnológico, por el que se obtenga, exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos reales o simulados o por inteligencia artificial de contenido sexual íntimo de una persona, sin su consentimiento; que atente contra la integridad, la dignidad, la intimidad, la libertad, la vida privada de las mujeres o cause daño psicológico, económico o sexual tanto en el ámbito privado como en el público,	Artículo 7. Las modalidades de violencia contra las mujeres son: (...) X. Violencia digital: Es cualquier acto realizado mediante el uso de materiales impresos, correo electrónico, mensajes telefónicos, redes sociales, plataformas de internet, correo electrónico, o cualquier medio tecnológico, por el que se obtenga, exponga, distribuya, difunda, exhiba, reproduzca, transmita, comercialice, oferte, intercambie y comparta imágenes, audios o videos reales o simulados o por inteligencia artificial de contenido sexual íntimo de una persona, sin su consentimiento, así como la difusión no consentida de datos personales identificables, tales como domicilios, números telefónicos, información familiar, laboral o de identificación personal, con la intención de infundir temor,



además de daño moral, tanto a ellas como a sus familias	intimidar, hostigar, perseguir o poner en riesgo la seguridad o integridad de la mujer o su familia; que atente contra la integridad, la dignidad, la intimidad, la libertad, la vida privada de las mujeres o cause 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.
---	--

Ley de Víctimas para la Ciudad de México	
TEXTO VIGENTE	TEXTO DE LA INICIATIVA
Artículo 3.- Para los efectos de la presente Ley, se entiende por: (...) XVIII. Hecho victimizante: Actos u omisiones que dañan, menoscaban o ponen en peligro los bienes jurídicos o derechos de una persona convirtiéndola en víctima. Éstos pueden estar tipificados como delito o constituir una violación a los derechos humanos reconocidos por la Constitución y los Tratados Internacionales de los que México forme parte, y la Constitución Política de la Ciudad de México;	Artículo 3.- Para los efectos de la presente Ley, se entiende por: (...) XVIII. Hecho victimizante: Actos u omisiones que dañan, menoscaban o ponen en peligro los bienes jurídicos o derechos de una persona convirtiéndola en víctima. Éstos pueden estar tipificados como delito o constituir una violación a los derechos humanos reconocidos por la Constitución y los Tratados Internacionales de los que México forme parte, y la Constitución Política de la Ciudad de México También se considerará un hecho victimizante la revelación o difusión no consentida de datos personales identificables, tales como domicilios, números telefónicos, información familiar o laboral, con la intención de intimidar, hostigar, amenazar o causar daño psicológico, físico o económico, configurando una violación a la privacidad y seguridad personal. (...)



DECRETO.

ÚNICO. Se adiciona el artículo 213 Bis al Código Penal para el Distrito Federal; un párrafo la fracción III, y la modificación del antepenúltimo párrafo del artículo 127 de la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad De México; se adiciona el artículo 64 Bis a la Ley de Responsabilidades Administrativas de la Ciudad de México; se modifica la fracción XVIII del artículo 3 de la Ley de Víctimas para la Ciudad de México; se modifica la fracción X del artículo 7 de la Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México, en los términos planteados.

TRANSITORIOS DE LA REFORMA

PRIMERO. Publíquese en la Gaceta Oficial de la Ciudad de México.

SEGUNDO. En un plazo no mayor a ciento ochenta días naturales contados a partir de la entrada en vigor del presente Decreto, las autoridades competentes deberán armonizar los reglamentos, protocolos y disposiciones administrativas en materia de protección de datos personales, ciberseguridad y responsabilidades administrativas, para asegurar la debida aplicación de las reformas al Código Penal para el Distrito Federal, a la Ley de Protección de Datos Personales en Posesión de Sujetos Obligados de la Ciudad de México y la Ley de Responsabilidades Administrativas de la Ciudad de México, Ley de Acceso de las Mujeres a una Vida Libre de Violencia de la Ciudad de México y la Ley de Víctimas para la Ciudad de México.

Por lo anteriormente expuesto y fundado, se propone ante el pleno de este Honorable Congreso de la Ciudad de México, la mencionada Iniciativa con proyecto de decreto por el que se reforma y adicionan diversos artículos al Código Penal para el Distrito Federal, a la Ley de Protección de Datos Personales en Posesión de



Sujetos Obligados de la Ciudad de México, y Ley de Responsabilidades Administrativas de la Ciudad de México

▪

OLIVIA
GARZA DE LOS SANTOS
6927AD555C91277B2C7E7CF2

Atentamente:

Dip. OLIVIA GARZA DE LOS SANTOS

Certificado de firma

26/11/2025 19:46

Documento electrónico

Solicitante del proceso de firma Almacenado

Identificador: 6927AC5D9DA721586E1C977B
Nombre y extensión: Iniciativa doxing corregida (1).pdf
Descripción:
Cantidad de páginas: 3
Estado: Firmado
Firmantes: 1
Huella digital del contenido del documento original:
1010acffc4b0ee240944acf19940893edcbee300fa560f7fc68b98e6707b3c9c
Huella digital del contenido del documento firmado:
5c81c948c09401e362ad796704ac9eec612d7555dcb71222a17a992f12181ec3

Nombre: Olivia Garza De Los Santos
Compañía: SR LUZ SA DE CV
Correo electrónico: olivia.garza@congresocdmx.gob.mx
Teléfono:
Dirección IP: 2806:2f0:9584:f35e:30e5:5efc:987c:7811
Fecha y hora de emisión
(America/Mexico_City):
26/11/2025 19:41

Constancia de conservación del documento firmado

Información de la constancia NOM-151

Información del emisor de la constancia NOM-151

Fecha de emisión:
27/11/2025 01:46:06 UTC (26/11/2025 19:46:06 Hora local de la Ciudad de México)
Nombre y extensión:
928e4c24-76d7-4c67-b880-12df0e8c6f22.cons
Huella digital contenida en la constancia:
5c81c948c09401e362ad796704ac9eec612d7555dcb71222a17a992f12181ec3

Prestador de Servicios de Certificación (PSC):
PSC WORLD S.A. DE C.V.
Certificado PSC válido desde: 2017-07-19
Certificado PSC válido hasta: 2029-07-19

Firmantes

Firmante 1. OLIVIA GARZA DE LOS SANTOS

Atributos

Firma

Fecha

Tipo de actuación: Por su Propio
Derecho
Compañía:
Método de notificación: Correo
Correo: olivia.garza@congresocdmx.gob.mx
Teléfono:
Emisor de la firma electrónica:
Dibujada en dispositivo
Plataforma: <https://app.con-certeza.mx>

ID: 6927AD555C91277B2C7E7CF2
IP: 2806:2f0:9584:f35e:30e5:5efc:987c:7811



Enviado: 26/11/2025
19:43:03
Aceptó Aviso de
Privacidad: 26/11/2025
19:45:54
Visto: 26/11/2025 19:45:57
Confirmado:
26/11/2025 19:45:58.081
Firmado:
26/11/2025 19:45:58.084

EL ESPACIO DEBAJO SE HA DEJADO EN BLANCO INTENCIONALMENTE

Método de validación de firmante:

Enlace de verificación

En el siguiente enlace se encuentra el portal para validar la constancia NOM-151 y el estado de integridad de este documento:
<https://app.con-certeza.mx/constancia/928e4c24-76d7-4c67-b880-12df0e8c6f22>

