



276



**H. XVII LEGISLATURA DEL PODER LEGISLATIVO
DEL ESTADO DE QUINTANA ROO.**

PRESENTE.

El que suscribe, Diputado José María Chacón Chablé, presidente de la Comisión de Movilidad, integrante de esta H. XVII Legislatura del Estado de Quintana Roo, en ejercicio de lo dispuesto en la fracción segunda del artículo 68, de la Constitución Política del Estado Libre y Soberano de Quintana Roo y con fundamento en los artículos 140 y 141 de la Ley Orgánica del Poder Legislativo del Estado de Quintana Roo, me permito presentar a consideración de este Alto Pleno Deliberativo, la presente **INICIATIVA DE DECRETO POR LA CUAL SE REFORMA EL TITULO TERCERO, DEL LIBRO SEGUNDO PARTE ESPECIAL, SECCIÓN PRIMERA, DEL CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE QUINTANA ROO, PARA DENOMINARSE "DELITOS CONTRA LA INVIOABILIDAD DEL SECRETO Y EL ACCESO ILÍCITO A SISTEMAS INFORMÁTICOS", ADEMÁS DE ADICIONAR UN CAPÍTULO SEGUNDO, AL MISMO TÍTULO TERCERO, DENOMINADO ACCESO ILÍCITO A SISTEMAS INFORMÁTICOS, ADICIONANDO LOS ARTICULOS 126 BIS, 126 TER Y 126 QUATER,** con fundamento en la siguiente:

EXPOSICIÓN DE MOTIVOS.

La presente acción legislativa que se somete a consideración de esta H. XVII Legislatura, tiene como objetivo realizar reformas al Código Penal para el Estado Libre y Soberano de Quintana Roo, esto a efecto de incorporar un nuevo tipo penal en materia de Acceso ilícito a los Sistemas Informáticos. La iniciativa en cuestión, responde a la necesidad de regular una serie de comportamientos recientes, y comunes en la sociedad, derivadas del progreso de la tecnología y su uso constante.

Nulla poena sine lege y nullum crimen sine lege, son algunos de los principios rectores del Derecho punitivo; y el día de hoy el uso diario de las tecnologías de la información ha dado paso a un conjunto de conductas que, nos obligan como legisladores, a impulsar reformas que pongan fin a la comisión de conductas antijurídicas que se practican actualmente de manera impune.

En primer término, se pretende reformar la denominación del Título Tercero, del Libro Segundo Parte Especial, Sección Primera del Código Penal, para nombrarle “Delitos contra la Inviolabilidad del Secreto de Sistemas Informáticos y de Acceso Ilícito a Sistemas Informáticos”, de la misma manera, se reforma la nomenclatura del capítulo único correspondiente a la “Revelación del Secreto”, para pasar a ser un capítulo primero; y por último se adiciona un capítulo segundo denominado “Del Acceso Ilícito a Sistemas Informáticos”. En este sentido, se adiciona al nuevo capítulo segundo anteriormente referido los artículos 126 Bis, 126 Ter y 126 Quater. El primer numeral de la iniciativa, propone se imponga una pena de uno a dos años de prisión y de veinticinco a cien días multa, a quien, sin consentimiento o autorización para acceder, ingrese o entre a una base de datos, sistema, equipo o medio de almacenamiento informático, con el propósito de conocer, copiar, reproducir, interceptar, interferir, o recibir la información contenida en cualquiera de los mismos. En su segundo párrafo el artículo propuesto, busca sancionar al que sin autorización acceda ingrese o entre a una base de datos, sistema, equipo o medio de almacenamiento informático, con el propósito de obtener de manera ilícita un beneficio, bienes o información para sí o para una tercera persona; y de manera indebida, alterar, dañar, inutilizar o destruir la información o los datos contenidos, con una pena de dos a cuatro años de prisión y veinticinco a doscientos días multa.

De la misma manera se sugiere sancionar en el 126 ter, cuando el sujeto pasivo estando autorizado para su acceso, haga uso indebido de una base de datos, sistema, equipo o medio de almacenamiento informático, con ánimo de ilícitamente copiar, reproducir, interceptar, interferir, y la sanción será de uno a tres años de prisión y de veinticinco a cien días multa. En su segundo párrafo también se especifica que al que estando autorizado, acceda a una base de datos, sistema, equipo o medio de almacenamiento informático para alterar, dañar, borrar, sustraer, inutilizar o destruir la información, los datos, o la información reservada en el sistema, en perjuicio de terceros, o para beneficio propio o de terceros, la sanción sería de dos a cinco años de prisión y de veinticinco a doscientos días multa.





Respecto al contenido normativo del artículo 126 quater se establecen cinco agravantes para cuando el sujeto activo actúe con fines de lucro; cuando el sujeto pasivo sea el Estado, los municipios o los organismos autónomos, y si el hecho constitutivo de delito fue cometido contra base de datos, sistemas, equipos o medios de almacenamiento informáticos concernientes al régimen financiero de las entidades públicas; si el sujeto activo obró procurando la dilación dolosa de los procesos jurídicos en términos del artículo 176 quinquies de este Código, y si la conducta afectó un sistema, o base de datos relacionado con el servicio público de salud, administración de justicia, procuración de justicia, o la seguridad pública. Para mayor claridad, se presenta el siguiente cuadro comparativo:

CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE QUINTANA ROO.	
LEY VIGENTE	INICIATIVA.
LIBRO SEGUNDO	LIBRO SEGUNDO
PARTE ESPECIAL	PARTE ESPECIAL
SECCION PRIMERA	SECCION PRIMERA
Delitos Contra el Individuo	Delitos Contra el Individuo
TITULO TERCERO	TITULO TERCERO
Delito Contra la Inviolabilidad del Secreto	Delitos contra la Inviolabilidad del Secreto y de Acceso Ilicito a Sistemas Informáticos
CAPITULO UNICO	CAPITULO PRIMERO
Revelación del Secreto	Revelación del Secreto
ARTICULO 126-... ...	ARTICULO 126-... ...
SIN CORRELATIVO.	CAPITULO SEGUNDO



	<p style="text-align: center;">DEL ACCESO ILICITO A SISTEMAS INFORMÁTICOS</p> <p>Artículo 126 Bis. – A quien, sin consentimiento o autorización para acceder, ingrese o entre a una base de datos, sistema, equipo o medio de almacenamiento informático, con el propósito de conocer, copiar, reproducir, interceptar, interferir, o recibir la información contenida, se le impondrá una pena de uno a dos años de prisión y de veinticinco a cien días multa.</p> <p>Al que sin autorización acceda ingrese o entre a una base de datos, sistema, equipo o medio de almacenamiento informático, con el propósito de obtener de manera ilícita un beneficio, bienes o información para sí o para una tercera persona; y de manera indebida, alterar, dañar, inutilizar o destruir la información o los datos contenidos, se le impondrá una pena de dos a cuatro años de prisión y veinticinco a doscientos días multa.</p>
<p style="text-align: center;">SIN CORRELATIVO.</p>	<p>Artículo 126 Ter. – Quien estando autorizado para su acceso, haga uso indebido de una base de datos, sistema, equipo o medio de almacenamiento informático, con ánimo de ilícitamente copiar, reproducir, interceptar, interferir, la sanción será de uno a tres años de prisión y de veinticinco a cien días multa.</p> <p>Al que estando autorizado, acceda a una base de datos, sistema, equipo o medio de almacenamiento informático para alterar, dañar, borrar, sustraer, inutilizar o destruir la información, los datos, o la información reservada en el sistema, en perjuicio de terceros, o para beneficio propio o de terceros, la sanción será de dos a cinco años de prisión y de veinticinco a doscientos días multa.</p>
<p style="text-align: center;">SIN CORRELATIVO.</p>	<p>Artículo 126 Quater. Las penas previstas en los artículos 126 bis y 126 ter se incrementarán en una mitad más:</p> <p>I. Si el sujeto activo actuó con fines de lucro;</p> <p>II. Cuando el sujeto pasivo sea el Estado, los municipios o los organismos autónomos;</p> <p>III. Si el hecho constitutivo de delito fue cometido contra base de datos, sistemas, equipos o medios de almacenamiento</p>



	<p>informáticos concernientes al régimen financiero de las entidades públicas;</p> <p>IV. Si el sujeto activo obró procurando la dilación dolosa de los procesos jurídicos en términos del artículo 176 quinquies de este Código, y</p> <p>V. Si la conducta afectó un sistema, o base de datos relacionado con el servicio público de salud, administración de justicia, procuración de justicia, o la seguridad pública.</p>
--	--

Como se puede apreciar, el propósito de esta acción legislativa es la creación de un nuevo delito al interior del Código Penal para el Estado Libre y Soberano de Quintana Roo, el cual busca sancionar a todas las personas que cometen conductas antisociales, derivado del uso inadecuado de las tecnologías de la información y las comunicaciones, específicamente en materia de acceso ilícito a los sistemas informáticos.

En la actualidad el uso de la tecnología ha permeado en todos los aspectos de la vida diaria, es evidente que la automatización de datos mediante herramientas útiles y prácticas es un importante auxiliar y, al mismo tiempo, se convierte en un medio para que el gobernado acceda a la justicia de manera más fácil¹. Es decir, la información que puede ser almacenada en dispositivos, base de datos, sistemas, equipos o medios de almacenamiento informáticos, puede pertenecer tanto a una persona física como a una persona moral e incluso al Estado. De este punto deviene la importancia de la acción legislativa promovida por quien suscribe, toda vez, que el acceso ilícito a la información o bien, su uso indebido constituye una práctica, cada vez más común, que afecta a la sociedad en todas sus esferas.

Los sistemas y las nuevas tecnologías de la información se han convertido en un fenómeno intrínsecamente relacionado con la sociedad de la información. Siendo esta última, entendida como la comunidad integrada y permanentemente comunicada en una misma forma con múltiples medios y procesos, en un solo tiempo, trascendiendo fronteras y generando contenidos integrados por datos cada día más actuales, más

¹ <https://sistemabibliotecario.scjn.gob.mx/sisbib/2018/000291341/000291341.pdf>



verídicos y más congruentes con las propias necesidades que ella misma demanda².

La importancia que la tecnología de la información ha adquirido, es tal, que las Naciones Unidas han determinado, que la falta de acceso y manejo de la misma es equivalente al analfabetismo del siglo XXI. Siendo entonces, esta, la razón por la cual, los miembros de la sociedad en general demandan facilidades para la optimización de sus quehaceres tanto en su ámbito personal como laboral.

En el ámbito público, con el progreso de la tecnología, la informática se convierte en un instrumento al servicio del derecho cuando las computadoras, además de ser máquinas que facilitan el manejo de números, lo son también para la generación, almacenamiento y manipulación de textos³. Por dar un ejemplo, es pertinente mencionar que En América Latina, Brasil y Argentina han sido, junto con México, los principales países promotores de la informática parlamentaria. El primero de ellos inauguró, desde el año de 1972, el Centro de Información y Procesamiento de Datos del Senado Federal (PRODASEN), el cual ha logrado establecer una gran comunicación entre las distintas dependencias encargadas del manejo de información jurídica automatizada⁴.

Todo lo anterior, propicia el surgimiento de conceptos nuevos como el de "Seguridad de la Tecnología de la Información y la comunicación", concepto que hace referencia al total de procedimientos establecidos para garantizar los principios fundamentales de la información contenido en un sistema, como lo son la integridad, confidencialidad, disponibilidad y autenticación de la información. Siendo la Integridad entendida como la alteración de los componentes del sistema, la confidencialidad alude al acceso al sistema únicamente por los usuarios autorizados, mientras que la disponibilidad responde al acceso de los usuario cuando así sea deseado, y por último autenticidad, por cuanto a

² <http://www.ordenjuridico.gob.mx/Congreso/pdf/133.pdf>

³ PRADO, Pedro Antonio, *La informática y el abogado*, Ed. Abeledo Perrot, Argentina, 1988, p. 61

⁴ <https://sistemabibliotecario.scjn.gob.mx/sisbib/2018/000291341/000291341.pdf>



la garantía que la información es válida y utilizable. Este conjunto de elementos integran la seguridad de la información en un aspecto técnico y tecnológico.

En vista de lo anterior, el estado de Derecho tiene la obligación de garantizar la seguridad jurídica de los usuarios, a efecto de garantizar al individuo los derechos entorno a su persona y bienes. Por otra parte, la Corte Interamericana de Derechos Humanos recalcó que la fijación de los efectos en un tipo penal, debe ser legislada previo a la realización de la conducta, debido a que en esa proporción los destinatarios de la norma podrían orientar su comportamiento conforme al orden jurídico vigente y cierto. Además, indicó que el Juez al momento de aplicar la ley penal, debe atender a lo dispuesto por ésta y observar con la mayor rigurosidad la adecuación de la conducta al tipo penal, de tal forma en que no se sancionen comportamientos que no son punibles por el ordenamiento jurídico.

Es imprescindible que en la judicialización de la justicia, las autoridades se apeguen al principio de legalidad, toda vez que es el principal límite impuesto por las exigencias del Estado de derecho al ejercicio de la potestad punitiva, lo que incluye una serie de derechos para la ciudadanía, resultando imposible que el Estado intervenga penalmente más allá de lo que le permite la ley. De acuerdo con dicho principio, sólo se puede castigar un hecho si su punibilidad se encuentra prevista en una ley antes de su comisión. En este orden de ideas, la tipicidad es un presupuesto indispensable del acreditamiento del injusto penal, y constituye la base fundamental del principio de legalidad⁵.

Es importante tener en consideración, que actualmente en el Estado de Quintana Roo, no existe regulación en materia de acceso ilícito a los sistemas informáticos, esto debido a que el Código Penal de la Entidad no reconoce como delito, ninguna acción que contravenga los derechos de un tercero, derivado del acceso ilícito a sistemas informáticos.

⁵ Sobre el tema de taxatividad, se puede consultar: Acción de inconstitucionalidad 196/2020, resuelta en sesión de once de mayo de dos mil veintiuno, Acción de inconstitucionalidad 13/2016 y su acumulada 14/2016, resuelta en sesión de veinticinco de febrero de dos mil veinte, Amparo en revisión 455/2011, resuelto por la Primera Sala en sesión de veintinueve de junio de dos mil once y el Amparo directo en revisión 3056/2017, resuelto por la Primera Sala en sesión de veintidós de mayo de dos mil diecinueve.

En este sentido, el Estado no puede ejercer su facultad punitiva en contra de quienes lleven a cabo este tipo de conducta, toda vez, que es un requisito *sine qua non* para el ejercicio de esta facultad la existencia de un tipo penal debidamente establecido en el cuerpo legal correspondiente⁶.

Por consiguiente, resulta imperativo para el Poder Legislativo del Estado de Quintana Roo, evitar la omisión normativa y realizar las acciones pertinentes a efecto de crear un tipo penal específico que permita sancionar a las personas que cometen la conducta de acceso ilícito a sistemas informáticos.

Ahora bien, atendiendo al objetivo de la iniciativa, es relevante señalar, que para la creación de un nuevo delito el legislador debe observar se garantice la seguridad jurídica, la legalidad, en su vertiente de taxatividad en materia penal, la mínima intervención (*ultima ratio*), así como evitar en todo momento incurrir en lo ambiguo, evitando así se sancione a personas cuando la conducta no amerita hacerlo.

En este orden de ideas, cuando se trata de las conductas antisociales en materia de acceso ilícito a sistemas informáticos, es de suma importancia, hacer un estudio de la conducta que nos concierne. En este caso específico, el elemento conducta, radica específicamente en la acción de ingresar, acceder o entrar a una base de datos, sistema, equipo o medio de almacenamiento informático, con el propósito de obtener de manera ilícita un beneficio, bienes o información para sí o para una tercera persona; o de manera indebida conocer, copiar, reproducir, interceptar, interferir, recibir, alterar, dañar, inutilizar o

⁶ "EXACTA APLICACIÓN DE LA LEY PENAL. ESTE DERECHO FUNDAMENTAL, CONTENIDO EN EL TERCER PÁRRAFO DEL ARTÍCULO 14 DE LA CONSTITUCIÓN POLÍTICA DE LOS ESTADOS UNIDOS MEXICANOS, SALVAGUARDA LA SEGURIDAD JURÍDICA DE LAS PERSONAS. El derecho fundamental a la exacta aplicación de la ley penal tiene su origen en los principios *nullum crimen sine lege* (no existe un delito sin una ley que lo establezca) y *nulla poena sine lege* (no existe una pena sin una ley que la establezca), al tenor de los cuales sólo pueden castigarse penalmente las conductas debidamente descritas en la legislación correspondiente como ilícitas y aplicarse las penas preestablecidas en la ley para sancionarlas, con el fin de salvaguardar la seguridad jurídica de las personas, a quienes no puede considerárseles responsables penalmente sin que se haya probado que infringieron una ley penal vigente, en la que se encuentre debidamente descrito el hecho delictivo y se prevea la sanción aplicable." Fuente: Orellana Wiarco Octavio A. "Teoría del Delito, Sistemas Causalistas, Finalistas y Funcionalistas", Editorial Porrúa, Décima Sexta Edición, México, 2007.

destruir la información, o bien realizar la conducta en perjuicio de otros, específicamente transgrediendo el derecho a la intimidad personal y la vida privada del sujeto pasivo.

Siguiendo con la descripción del delito, es menester ser claros al respecto de la antijuridicidad de la acción como elemento del delito, es decir, sobre la transgresión de bienes jurídicos tutelados por el Estado Constitucional Mexicano⁷. En este sentido se pueden reconocer diversos derechos y bienes jurídicos tutelados por el Estado Constitucional del Derecho, los cuales son vulnerados y transgredidos por la conducta en cuestión, dentro de estos bienes jurídicos tutelados se encuentra la intimidad personal o la privacidad, e incluso el derecho a la propiedad y a la integridad de la información de los particulares.

En lo que respecta al derecho de la intimidad personal, se debe considerar lo siguiente:

Que intimidad personal es inherente a la vida humana, ya que para que el ser humano desarrolle y gesticione su propia personalidad e identidad es menester que goce de un área que comprenda diversos aspectos de su vida individual y familiar que esté libre de la intromisión de extraños. Así pues, debemos entender que todos los seres humanos tenemos una vida "privada" conformada por aquella parte de nuestra vida que no está consagrada a una actividad pública y que por lo mismo no está destinada a trascender e impactar a la sociedad de manera directa y en donde en principio los terceros no deben tener acceso alguno, toda vez que las actividades que en ella se desarrollan no son de su incumbencia, ni afectan la esfera de derechos de terceros.

Siendo entonces que el respeto a la vida privada, manteniendo alejadas injerencias no deseables e indiscreciones abusivas, permitirá que la personalidad del ser humano se desarrolle libremente.

De esta forma la protección a la vida privada se constituye en un criterio de carácter democrático. Sin duda alguna, el respeto a la vida privada y a la intimidad tanto personal como familiar se constituye en un valor fundamental del ser humano, razón por la cual el

⁷ Jiménez de Asúa Luis, "Tratado de Derecho Penal", Editorial Losada, Cuarta Edición, Buenos Aires 1986.



derecho ha considerado importante tutelarlos y dictar medidas para evitar su violación así como para intentar subsanar los daños ocasionados.

De esta manera surge el llamado derecho a la privacidad, a la vida privada o simplemente derecho a la intimidad, como un derecho humano fundamental, en virtud del cual se tiene la facultad de excluir o negar a las demás personas del conocimiento de ciertos aspectos de la vida de cada persona que solo a ésta le incumben.

Este derecho que tiende a proteger la vida privada del ser humano, es un derecho complejo que comprende y se vincula a su vez con varios derechos específicos que tienden a evitar intromisiones extrañas o injerencias externas en estas áreas reservadas del ser humano como son el derecho a la inviolabilidad del domicilio, el derecho a la inviolabilidad de correspondencia, el derecho a la inviolabilidad de las comunicaciones privadas, el derecho a la propia imagen, el derecho a la privacidad informática, el derecho a no participar en la vida colectiva y a aislarse voluntariamente, y el derecho a no ser molestado.⁸

Es de importancia resaltar, que la reforma presentada obedece también a lo señalado en el Pacto Internacional de Derechos Civiles y Políticos (ONU), que dispone lo siguiente:

Artículo 17.

1. Nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra o reputación.
2. Toda persona tiene derecho a la protección de la ley contra esas injerencias y esos ataques⁹

Y en un mismo sentido, la Convención Americana sobre Derechos Humanos, suscrita en San José de Costa Rica el 22 de noviembre de 1969, específicamente en el artículo 11 vela por la Protección de la Honra y de la Dignidad señalando lo siguiente:

⁸ <https://www.diputados.gob.mx/sedia/sia/spi/SPI-ISS-01-07.pdf>

⁹ <https://www.ohchr.org/es/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>



1. Toda persona tiene derecho al respeto de su honra y al reconocimiento de su dignidad.
2. Nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, ni de ataques ilegales a su honra o reputación.
3. Toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques¹⁰.

En adición a lo anterior y solo para hacer hincapié de la importancia de legislar sobre este tema, será retomado un comunicado de la Oficina Alto Comisionado de las Naciones Unidas para los Derechos Humanos, emitida en el período de sesiones 32° de 1988, el cual menciona lo siguiente:

A este respecto, el Comité desea señalar que en los informes de los Estados Partes en el Pacto no se está prestando la atención necesaria a la información relativa a la forma en que las autoridades legislativas, administrativas o judiciales y, en general, los órganos competentes establecidos en el Estado garantizan el respeto de este derecho. En particular, no se presta suficiente atención al hecho de que el artículo 17 del Pacto se refiere a la protección contra las injerencias tanto ilegales como arbitrarias. Esto significa que es precisamente en la legislación de los Estados donde sobre todo debe preverse el amparo del derecho establecido en ese artículo.

Actualmente, en los informes o bien no se hace mención alguna de dicha legislación o se proporciona información insuficiente al respecto.

El término "ilegales" significa que no puede producirse injerencia alguna, salvo en los casos previstos por la ley. La injerencia autorizada por los Estados sólo puede tener lugar en virtud de la ley, que a su vez debe conformarse a las disposiciones, propósitos y objetivos del Pacto.

¹⁰ <http://www.cidh.oas.org/Basicos/Spanish/Basicos2.htm>



La expresión "injerencias arbitrarias" atañe también a la protección del derecho previsto en el artículo 17. A juicio del Comité, la expresión "injerencias arbitrarias" puede hacerse extensiva también a las injerencias previstas en la ley. Con la introducción del concepto de arbitrariedad se pretende garantizar que incluso cualquier injerencia prevista en la ley esté en consonancia con las disposiciones, los propósitos y los objetivos del Pacto y sea, en todo caso, razonable en las circunstancias particulares del caso.

En cuanto al término "familia", los objetivos del Pacto exigen que, a los efectos del artículo 17, se lo interprete como un criterio amplio que incluya a todas las personas que componen la familia, tal como se entienda ésta en la sociedad del Estado Parte de que se trate. El término "home" en inglés, "manzel" en árabe, "zhùzhái" en chino, "domicile" en francés, "zhilishche" en ruso y "domicilio" en español, que se emplea en el artículo 17 del Pacto, ha de entenderse en su acepción de lugar donde una persona reside o ejerce su ocupación habitual. A ese respecto, el Comité invita a los Estados a indicar en sus informes la acepción que se da en sus respectivas sociedades a los términos "familia" y "domicilio"¹¹.

Y si bien es cierto, ya han pasado varios años del comunicado, arriba citado, lo cierto es que la legislación en México en esta materia es aun precaria, situación que se ha visto potenciada con el uso creciente de las tecnologías de la Información.

Siguiendo este orden de ideas, dentro del derecho mexicano, el derecho a la privacidad, es contemplado de distintas maneras. La Suprema Corte de Justicia de la nación, resolvió en el amparo en revisión 134/2008¹², que, cuando se comparten sin consentimiento

¹¹ <https://www.acnur.org/fileadmin/Documentos/BDL/2005/3584.pdf>

¹² Amparo en Revisión 134/2008. Sentencia del 30 de abril de 2008. México. Disponible en <<http://www2.scjn.gob.mx/ConsultaTematica/PaginasPub/DetallePub.aspx?AsuntoID=97847>> (3 de julio de 2013) En este juicio de amparo, cuyo ponente fue el Ministro Genaro Góngora Pimentel, un ciudadano reclamó la inconstitucionalidad de los artículos 2o., 5o. y 20 de la Ley para Regular las Sociedades de Información Crediticia (Ley) por ser violatorios del derecho a la privacidad debido a que autorizaba la entrega, "sin su consentimiento", de datos bancarios a las sociedades de información crediticia (burós de crédito) que los explotarian comercialmente. La SCJN señaló que la revelación de la historia de crédito tenía implicaciones en la situación patrimonial y económica de la persona y, por ende, en su privacidad, por lo que sí había una afectación a su vida privada. Incluso señaló que el secreto financiero podía quedar inmerso dentro del derecho a la privacidad. Sin embargo, precisó que se trataba de una limitación justificada, pues en esa reserva de información "coinciden más intereses que el del cliente, que obligan a la comunicación o divulgación de los datos crediticios cuando concurra causa que lo justifique", como podrían ser los casos de supervisión bancaria o persecución de delitos, en los que el propio legislador autoriza la solicitud de informes por parte de la autoridad judicial, la hacienda federal y la Comisión Nacional Bancaria y de Valores. Para la Corte, en estos supuestos, no hay una violación a la garantía de seguridad jurídica, pues "el interés de las autoridades es la protección del sistema bancario y crediticio por constituir uno de los motores del desarrollo económico". La SCJN también abordó el supuesto de cuando un particular (sociedad de información crediticia) entrega información (historia crediticia) a otro particular (por ejemplo, un deudor) y se preguntó si en este caso ocurría una violación al secreto

datos personales de los particulares, en este caso datos bancarios, se configura una violación a la privacidad. En este sentido la autoridad hizo reconocimiento del derecho a la persona que tiene su idea originaria en el respeto a la vida privada, siendo una de las libertades tradicionales protegidas por la [CPEUM] la inviolabilidad del domicilio, que tiene como finalidad principal el respeto a un ámbito de vida privada personal y familiar, que por regla general, debe quedar excluido del conocimiento ajeno y de las intromisiones de las demás, con la limitante que la propia Ley Fundamental establece para las autoridades¹³.

Incluso señaló, que la violación la privacidad puede constituirse no únicamente en un espacio físico, cómo sería en un domicilio determinado, o un lugar donde se desenvuelva la intimidad, sino también en aquellas intromisiones o molestias que causen afectación a la vida privada.

En este mismo sentido, el artículo 16 de la Constitución Política de los Estados Unidos Mexicanos protege el derecho a la intimidad personal siguiendo el espectro normativo de la Convención Internacional. Y entiende este derecho:

Como el derecho a aislarse de todos, sin importar si se trata de la familia, la comunidad o el Estado. Esta dimensión le permite al individuo escudarse física y emocionalmente de las entrometedoras miradas de los demás.

Contemplando además un doble aspecto, que abarca el derecho a la integridad de la información de los particulares:

El derecho a controlar la información de uno mismo, incluso después de haberla divulgado. Esta última dimensión en algunos otros países se le denomina como derecho a la autodeterminación informativa y es de suma relevancia en cualquier democracia, pues les permite a los ciudadanos intervenir activamente en la comunidad sin renunciar al

financiero o bancario. Al respecto, concluyó que ocurría una salvedad importante y es que, para que dicha entrega pudiera verificarse, los propios particulares, de acuerdo con la propia Ley (art. 28), debían otorgar su autorización expresa a la sociedad de información crediticia. Asimismo, destacó que la Ley le otorga a los particulares el control sobre los datos personales que afectan su intimidad, pues les confiere las facultades de acceder al conocimiento de las informaciones que se encuentran en la base de datos; de rectificar la que resulte errónea; de cancelar las que no tiene derecho a poseer y de conocer las que han sido comunicadas a terceros.

¹³ Ibidem



control de sus datos personales, por lo que son ellos quienes deciden "cuándo participan en sociedad y cuando se retiran".

El derecho a la protección de los datos personales se encuentra vinculado a este segundo componente, pues protege un aspecto importante de nuestra privacidad: los datos personales.

Los orígenes de este derecho se remontan a 1983, cuando el Tribunal Constitucional Alemán determinó que:

...El libre desarrollo de la personalidad presupone, en las modernas condiciones para el procesamiento de datos, la protección de los individuos frente a la ilimitada recolección, archivo, empleo y retransmisión de sus datos personales. [...] El derecho fundamental garantiza de esta manera la capacidad del individuo principalmente para determinar la transmisión y empleo de sus datos personales¹⁴

Por todo lo anterior, se corrobora plenamente la constitucionalidad del bien jurídico tutelado en la presente acción legislativa, y siendo ya identificada la importancia de proteger y sancionar la transgresión del derecho a la privacidad e integridad de la información de los particulares, es menester resaltar la importancia de establecer un nuevo delito que sancione las conductas que transgredan los derechos referidos, y en este sentido establecer una punibilidad clara como elemento del delito, a efecto de garantizar una efectiva impartición de justicia, en los casos que se actualice el supuesto jurídico establecido en la norma penal¹⁵; para el caso concreto de esta acción legislativa se prevé una sanción que dependerá si se tiene o no autorización para acceder al sistema, al equipo de cómputo o a la base de datos que contenga la información, así como del móvil que origine el comportamiento; debiendo también, observar el juzgador, si el sujeto pasivo de la conducta es el Estado, los municipios o los organismos autónomos o bien un particular. De la misma manera se proponen agravantes, cuando la multicitada conducta sean realizadas en contra de una institución de seguridad pública, por fines de lucro; Si el hecho constitutivo de delito fue cometido contra base de datos, sistemas, equipos o

¹⁴ <https://archivos.juridicas.unam.mx/www/bjv/libros/8/3567/39.pdf>

¹⁵ Jiménez de Asúa Luis, "*Ley del delito*", primera edición, Editorial Hermes Sudamericana, México, 1986.

medios de almacenamiento informáticos concernientes al régimen financiero de las entidades públicas; si el sujeto activo obró procurando la dilación dolosa de los procesos jurídicos en términos del artículo 176 quinquies, y Si la conducta afectó un sistema o dato referente a la salud, administración de justicia, procuración de justicia, o la seguridad pública.

A efecto de dotar de una mayor claridad sobre los posibles alcances de la iniciativa en cuestión, es pertinente definir el sujeto pasivo y activo de la conducta antisocial de mérito. Entendiendo como sujeto activo de delito a la persona individual con capacidad que realiza la conducta típica, mientras que el sujeto pasivo, es la persona titular del bien jurídico tutelado el cual es vulnerado o transgredido.¹⁶ En este caso en particular, el sujeto activo del tipo penal de acceso ilícito a sistemas informáticos corresponderá a la persona que estando o no autorizada, acceda a una base de datos, sistema o equipos de almacenamiento con el propósito de obtener un beneficio indebido para sí o para terceros, ya sea por alterar copiar, conocer, compartir o modificar de cualquier manera la información o datos contenidos de dichos equipos cibernéticos.

Siendo entonces, el sujeto pasivo del tipo penal en análisis, la persona particular titular de la información, o bien El Estado a través de sus instituciones, municipios, órganos autónomos o áreas en cargadas de la seguridad pública, o de la impartición de justicia, cuando, sin su consentimiento o sin la correspondiente autorización, sean víctimas del uso indebido de una base de datos, sistema, equipo o medio de almacenamiento informático, por parte del sujeto activo, con ánimo de ilícitamente copiar, compartir interceptar, interferir, alterar, dañar, borrar, sustraer, inutilizar o destruir la información, los datos, o la información reservada en el sistema, en perjuicio de terceros, o para beneficio propio o de terceros.

Es imposible soslayar que, el Estado de Quintana Roo, no contempla en su legislación penal el multicitado delito, sin embargo, si puede encontrarse en el Código Penal Federal, en su capítulo II, denominado "Acceso ilícito a sistemas y equipos de informática", pues se

¹⁶ Ibidem.



trata de una omisión por parte de nuestro estado, una omisión que en otras Entidades Federativas ha sido subsanada.

El acceso ilícito a sistemas informáticos y el uso indebido de la información que la tecnología permite almacenar, es una conducta cada vez más común y por esta razón, por lo menos trece Estados de la República han incorporado el delito señalado, a su respectivo Código Penal, considerando en su legislación secundaria la presente conducta antijurídica. Para una mayor claridad, a continuación, se presenta el siguiente cuadro con las entidades que si contemplan el delito:

ENTIDADES FEDERATIVAS QUE CONTEMPLAN EL DELITO.	ARTICULOS DEL CODIGO PENAL	LINK DIGITAL DE LA FUENTE DE INFORMACIÓN.	CÓDIGO QR
1).- Estado de Yucatán.	Artículos 243 Bis 5- 243 Bis 12	https://www.poderjudicialyucatan.gob.mx/digestum/marcoLegal/03/2012/DIGESTUM03002.pdf	
2).- Estado de Baja California.	Si, en sus artículos 175 BIS, TER y QUATER.	https://www.congresobc.gob.mx/Documentos/ProcesoParlamentario/Leyes/TOMO_V/20210813_CODPENAL.PDF	
3).- Estado de Chihuahua.	Si, en sus artículos 327 Bis, Ter, Quater y Quinquies.	http://www.congresochihuahua2.gob.mx/biblioteca/codigos/archivosCodigos/64.pdf	



4).- Estado de Coahuila.	Si, en sus artículos 281 BIS 1, 2, 3 y 4.	https://congresocoahuila.gob.mx/transparencia/03/Leyes_Coahuila/coa08_1990528.pdf	
5).- Estado de Durango.	Si, en sus artículos, 256, 257, 258, 259 y 260.	http://congresodurango.gob.mx/Archivos/legislacion/CODIGO%20PENAL%20(NUEVO).pdf	
6).- Estado de Jalisco.	Si, en su artículo 143 ter.	https://congresoweb.congresoajl.gob.mx/bibliotecavirtual/busquedasleyes/Listado.cfm#Codigo	
7).- Estado de Nuevo León.	Si, en sus artículos 225 BIS 1 y 225 BIS 2.	http://www.hcnl.gob.mx/trabajo_legislativo/leyes/codigos.php	
8).- Estado de Oaxaca.	Si, en sus artículos 434, 435, 436, 437, 438, 439 y 440.	http://docs64.congreso0oaxaca.gob.mx/documents/legislacion_estatales/Codigo_Penal_para_el_Estado_de_Oaxaca_(Ref_dto_2458_aprob_LXIV_Legis_24_mar_2021_PO_20_8a_secc_15_may_2021).pdf	



9).- Estado de Querétaro.	Si, en sus artículos 159 TER y 159 QUÁTER.	https://site.legislaturaqueretaro.gob.mx/CloudPLQ/InvEst/Codigos/COD007_59.pdf	
10).- Estado de Sinaloa.	Si, en su artículo 217	https://www.congresosinaloa.gob.mx/leyes-estatales/	
11).- Estado de Sonora.	Si, en su artículo 144 BIS 2.	http://www.congresoson.gob.mx:81/Content/Doc_leyes/Doc_443.pdf	
12).- Estado de Tabasco.	Si, en sus artículos 326 BIS, 326 BIS 1, 326 BIS 2 y 326 BIS 3.	https://congresotabasco.gob.mx/wp/wpcontent/uploads/2019/12/Codigo-Penal-para-el-Estado-de-Tabasco-1.pdf	
13).- Estado de Veracruz.	Si, en sus artículos 181, BIS, TER, QUATER, QUINQUIES y SEXIES.	https://www.legisver.gob.mx/leyes/LeyesPDF/CODIGOPENAL20072021FF.pdf	

Como se puede apreciar en el cuadro, en diversos Estados de la República Mexicana ya se tiene una legislación específica en materia penal respecto al tema en cuestión, siendo

que el Estado de Quintana Roo se encuentra en un claro rezago legislativo en atención a las conductas antisociales que son realizadas a través de los medios informáticos y electrónicos.

Por cuanto a la competencia estatal para legislar en esta materia, es relevante citar El **amparo en revisión 720/2008, el cual, retoma para su análisis que:**

...En el contexto internacional, la Organización de las Naciones Unidas ha reconocido que los delitos por computadora constituyen un grave problema, ya que las leyes, los sistemas de impartición de justicia y la cooperación internacional no se han adecuado a los cambios tecnológicos. La propia Organización instó a los Estados miembros a intensificar sus esfuerzos para combatir este tipo de conductas, entre otras medidas, mediante la creación de nuevos tipos penales y procedimientos de investigación. Para hacer frente a estas nuevas y sofisticadas formas de actividad criminal. La magnitud de los daños ocasionados por estas conductas depende de la información que se vulnere, al grado que pueden tener un fuerte impacto en el desarrollo de la economía, en la seguridad nacional o en las relaciones comerciales.

... Advierte que el legislador federal estimó necesario prever el delito en cuestión en el Código Penal Federal, debido a que:

La tecnología informática facilita a la sociedad su desarrollo económico y cultural, por lo que muchas actividades, educativas, culturales, comerciales, industriales, financieras, de comunicación no podrían realizarse sin el uso de equipos y sistemas informáticos¹⁷.

Y advierte también que el bien jurídico protegido por el delito de acceso ilícito a sistema y equipos de información, es decir el derecho a la privacidad y a la integridad de la información no corresponde a una materia de exclusiva competencia federal, sino que se trata de un delito que debe ser contemplado por todas las entidades federativas.

Es en virtud, de expuesto y fundado en el presente documento, que se somete a consideración del Alto Pleno Deliberativo la siguiente:

¹⁷ https://www.scjn.gob.mx/sites/default/files/actas-sesiones-publicas/documento/2018-01-04/actasespub20090218_0.pdf



INICIATIVA DE DECRETO POR LA CUAL SE REFORMA EL TITULO TERCERO, DEL LIBRO SEGUNDO PARTE ESPECIAL, SECCIÓN PRIMERA, DEL CÓDIGO PENAL PARA EL ESTADO LIBRE Y SOBERANO DE QUINTANA ROO, PARA DENOMINARSE "DELITOS CONTRA LA INVIOABILIDAD DEL SECRETO Y EL ACCESO ILÍCITO A SISTEMAS INFORMÁTICOS", ADEMÁS DE ADICIONAR UN CAPÍTULO SEGUNDO, AL MISMO TÍTULO TERCERO, DENOMINADO ACCESO ILÍCITO A SISTEMAS INFORMÁTICOS, ADICIONANDO LOS ARTICULOS 126 BIS, 126 TER Y 126 QUATER.

UNICO.- Se reforma el inciso a reforma el Titulo Tercero, del Libro Segundo parte especial, Sección Primera, del Código Penal para el Estado Libre y Soberano de Quintana Roo, para denominarse "Delitos contra La Inviolabilidad Del Secreto y el Acceso Ilícito a Sistemas Informáticos, de adicionar un Capítulo Segundo, al mismo Título Tercero, denominado Acceso Ilícito A Sistemas Informáticos.

LIBRO SEGUNDO

PARTE ESPECIAL

SECCION PRIMERA

Delitos Contra el Individuo

TITULO TERCERO

Delitos contra la Inviolabilidad del Secreto y de Acceso Ilícito a Sistemas Informáticos

CAPITULO PRIMERO

Revelación del Secreto

ARTICULO 126.-...

...

CAPITULO SEGUNDO

DEL ACCESO ILIICTO A SISTEMAS INFORMÁTICOS

Artículo 126 Bis. – A quien, sin consentimiento o autorización para acceder, ingrese o entre a una base de datos, sistema, equipo o medio de almacenamiento informático, con el propósito de conocer, copiar, reproducir, interceptar, interferir, o recibir la información contenida, se le impondrá una pena de uno a dos años de prisión y de veinticinco a cien días multa.

Al que sin autorización acceda ingrese o entre a una base de datos, sistema, equipo o medio de almacenamiento informático, con el propósito de obtener de manera ilícita un beneficio, bienes o información para sí o para una tercera persona; y de manera indebida, alterar, dañar, inutilizar o destruir la información o los datos contenidos, se le impondrá una pena de dos a cuatro años de prisión y veinticinco a doscientos días multa.

Artículo 126 Ter. – Quien estando autorizado para su acceso, haga uso indebido de una base de datos, sistema, equipo o medio de almacenamiento informático, con ánimo de ilícitamente copiar, reproducir, interceptar, interferir, la sanción será de uno a tres años de prisión y de veinticinco a cien días multa.

Al que estando autorizado, acceda a una base de datos, sistema, equipo o medio de almacenamiento informático para alterar, dañar, borrar, sustraer, inutilizar o destruir la información, los datos, o la información reservada en el sistema, en perjuicio de terceros, o para beneficio propio o de terceros, la sanción será de dos a cinco años de prisión y de veinticinco a doscientos días multa.

Artículo 126 Quater. Las penas previstas en los artículos 126 bis y 126 ter se incrementarán en una mitad más:

- I. Si el sujeto activo actuó con fines de lucro;
- II. Cuando el sujeto pasivo sea el Estado, los municipios o los organismos autónomos;
- III. Si el hecho constitutivo de delito fue cometido contra base de datos, sistemas, equipos o medios de almacenamiento informáticos concernientes al régimen financiero de las entidades públicas;
- IV. Si el sujeto activo obró procurando la dilación dolosa de los procesos jurídicos en términos del artículo 176 quinquies de este Código, y
- V. Si la conducta afectó un sistema, o base de datos relacionado con el servicio público de salud, administración de justicia, procuración de justicia, o la seguridad pública.

ARTÍCULOS TRANSITORIOS

PRIMERO.— El presente decreto entrará en vigor al día siguiente al de su publicación en el Periódico Oficial del Estado de Quintana Roo.

SEGUNDO.— Se derogan todas las disposiciones que se opongan al presente decreto.

Dado en la Ciudad de Chetumal Quintana Roo

A los 19 días del mes de junio de 2023.



Diputado José María Chacón Chablé
Presidente de la Comisión de Movilidad
de la H. XVII Legislatura.

