ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

INOHVBSM3C

Trámite 396137
Código validación INOHVBSM3C
Tipo de documento MEMORANDO INTERNO
Fecha recepción 05-feb-2020 11:08
Numeración documento 036-dml-an-2020-o
Fecha oficio 04-feb-2020
Remitente MARIN LAVAYEN DENNIS GUSTAVO
Función remitente ASAMBLEISTA
Revise el estado de su trámite en http://camites.asambleanacional.gob.ec/dts/estadoTramite.jsf

Oficio - 2 folios
Anexo 16 Pags

Quito, a 04 de febrero de 2020

Oficio No. 036-DML-AN-2020-O

Asambleísta:
César Litardo
PRESIDENTE DE LA ASAMBLEA NACIONAL
ASAMBLEA NACIONAL DE LA REPÚBLICA DE ECUADOR
En su despacho.-

De nuestra consideración:

Por intermedio del presente, remitimos a Usted el siguiente **alcance al Memorando No. 094-DML-AN-2019-M de 07 de enero de 2020**, a través del cual, de conformidad con la Ley Orgánica de la Función Legislativa, presentamos el Proyecto de "Ley reformatoria del Código Orgánico Integral Penal (Ley para la Promoción de Lucha contra el Cibercrimen)", trámite No. 392108, remitido por la Secretaria General de la Asamblea Nacional al Coordinador General de la Unidad de Técnica Legislativa, el 20 de enero de 2020, mediante Memorando No. SAN-2020-2385. Por intermedio del presente alcance hemos acogido en el texto original del proyecto las siguientes sugerencias del orden de la técnica legislativa, entre otras que naturalmente se derivan de aquellas:

1. Se ha modificado el nombre del proyecto de ley. A la fecha, ha adoptado el nombre de Proyecto de "Ley orgánica reformatoria del Código Orgánico Integral Penal."

2. Se han ampliado y complementado la exposición de motivos describiendo con mayor precisión el marco jurídico y técnico que sustenta las modificaciones que se proponen realizar al Código Orgánico Integral Pernal.

3. Se han mejorado y armonizado los "considerandos"con el articulado del Proyecto de "Ley orgánica reformatoria del Código Orgánico Integral Penal."

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

4. Se han revisado los artículos y disposiciones propuestas y se han corregido algunos aspectos de forma.

Acompañamos el texto integro del proyecto de ley en el que se han acogido las sugerencias enunciadas.

Atentamente,

Dennis Marín Lavayén
Asambleísta Nacional

ASAMBLEA NACIONAL
REPÚBLICA DEL ECUADOR

PROYECTO DE LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL

Exposición de motivos:

El 15 de abril de 2019, María Paula Romo, Ministra de Gobierno,en la ciudad de Cuenca, en una ceremonia en la que se oficializó la llegada de 187 nuevos policías para reforzar la seguridad en la provincia del Azuay, dijo que le preocupaba que Ecuador sea uno de los pocos países de la región que no cuenta con una ley para luchar contra ciberdelitos, con tecnología y personal. Enfatizó que el país no ha firmado ni ratificado el Convenio sobre Ciberdelincuencia, vigente desde el 1 de julio del 2004, con países de Europa, además de Canadá, Japón, Estados Unidos, Sudáfrica, Panamá, Perú, entre otros.[1] Dicho instrumento, también llamado Convenio de Budapest, es el primer tratado internacional que busca armonizar leyes nacionales, desarrollar técnicas de investigación y fortalecer la cooperación entre naciones para hacer frente a los delitos informáticos y los delitos en Internet. Romo hizo mención, también, de permanentes ataques cibernéticos a páginas de gobiernos seccionales y del gobierno central.[2]

La Oficina de Naciones Unidas contra la Droga y el Delito (UNODC, por su sigla en inglés) describió en el año 2013, en su reporte sobre Ciberdelincuencia denominado *"Comprehensive Study on Cibercrime"*, que en una sociedad hiperconectada como la de hoy en día, con acceso universal a Internet, casi no existe delito informático e inclusive delito común que no involucre evidencia electrónica ligada a una conexión a Internet, situación que requiere de cambios fundamentales en el enfoque legal, en la recolección de pruebas y en los mecanismos de cooperación internacional para resolver estos asuntos penales.[3]

Entre sus principales hallazgos, el reporte enfatizó la fragmentación del marco normativo que regula la ciberdelincuencia a nivel internacional, lo que refleja la

---

1 Ecuador es uno de los pocos países de Sudamérica que no se ha adherido al Convenio de Budapest, lo que implica una gran limitación en la realización de investigaciones y en la lucha contra el delito informático.

2 <https://www.elcomercio.com/actualidad/ministra-mariapaula-romo-ciberataques-ecuador.html>, consulta: enero de 2020.

3 UNODC, *Comprehensive Study on Cybercrime*, 2013, <https://www.unodc.org/documents/organized-crime/cybercrime/CYBERCRIME_STUDY_210213.pdf>.

existencia de regímenes con múltiples instrumentos, diferentes temáticas y ámbitos geográficos de aplicación, lo que podría llevar a grupos de países a formar clústeres de cooperación en estas materias, situación que no se ajustaría en forma adecuada a la naturaleza global del cibercrimen.[4] Señala, asimismo, que a nivel mundial son 82 estados los que han ratificado algún instrumento internacional de lucha contra el cibercrimen -a la fecha son muchos más-, y que, a partir de una encuesta realizada por el equipo de UNODC, el acuerdo multilateral más utilizado para desarrollar la legislación de combate al cibercrimen ha sido el Convenio del Consejo de Europa sobre Ciberdelincuencia (Convenio de Budapest).[5]

El Convenio de Budapest tiene como objetivo armonizar la legislación relativa al cibercrimen, mejorar las capacidades de investigación de estos delitos y establecer un régimen efectivo de cooperación y asistencia internacional. Entre sus principales disposiciones destacan la obligación de tipificar delitos contra la integridad de los sistemas o datos informáticos y su contenido, y establecer procedimientos que faciliten la investigación penal. La Convención resuelve también los aspectos de la cooperación y asistencia internacional en materias como extradición, acceso y consentimiento transfronterizo y el establecimiento de un equipo experto en una Red 24/7 como punto de contacto localizable las 24 horas del día. Existe, además, un Protocolo Adicional al Convenio sobre la penalización de actos de índole racista y xenófoba.[6]

En consecuencia, el Convenio sobre ciberdelincuencia o Convenio de Budapest es un tratado internacional que hace frente a los delitos informáticos y los delitos en Internet mediante la armonización de leyes entre naciones, la mejora de las técnicas de investigación y el aumento de la cooperación entre los convenios firmantes. De acuerdo al Preámbulo del Convenio, *"la lucha efectiva contra la Ciberdelincuencia requiere una cooperación internacional reforzada, rápida y eficaz en materia penal"*. Ahora bien, el Convenio, en su artículo 37, número 1, establece que: *"Tras la entrada en vigor del presente Convenio, el Comité de Ministros del Consejo de Europa, previa consulta con los Estados Contratantes del Convenio y una vez obtenido su consentimiento unánime, podrá invitar a adherirse al presente Convenio a cualquier Estado que no sea miembro del Consejo y que no haya participado en su elaboración. La decisión se adoptará por la mayoría establecida en el artículo 20.d)*

4 Ibídem, XI.

5 Ibídem, XIX.

6 Asesoría Técnica Parlamentaria, *Convenio sobre la Ciberdelincuencia: Convenio de Budapest*, Julio 2018, Chile, <https://www.bcn.cl/obtienearchivo?id=repositorio/10221/26882/1/Convenio_de_Budapest_y_Ciberdelincuencia_en_Chile.pdf>.

del Estatuto del Consejo de Europa y con el voto unánime de los representantes con derecho a formar parte del Comité de Ministros."

La adhesión de Ecuador a este convenio significaría, sin lugar a dudas, un avance enorme en materia de la lucha contra la ciberdelincuencia, pues, el carácter transnacional de la ciberdelincuencia necesariamente empuja a todas las naciones a adoptar un enfoque normativo de cooperación y armonización regulatoria entre todos los países para enfrentar la naturaleza global del fenómeno; y si bien, la adhesión pende de la invitación del Comité de Ministros del Consejo de Europa, cae indiscutiblemente en el ámbito de la diligencia debida del Presidente de la República -y del Ejecutivo- solicitar formalmente y por los medios diplomáticos convencionales tal invitación y, de la Asamblea Nacional, facilitar dicho proceso hacia la invitación y futura adhesión al tratado internacional, adoptando, lo más pronto posible, las medidas dispuestas para el ámbito nacional en la antedicha Convención, en particular e inicialmente las de contenido de derecho penal sustantivo. Las medidas subsecuentes deberán ser integradas en el ordenamiento jurídico nacional una vez, Ecuador se adhiera al Convenio de Budapest.

El Capítulo II de la Convenión detalla las medidas que deben adoptar los estados suscriptores a nivel nacional de contenido de derecho penal sustantivo. Prevé la tipificación de los delitos -describiendo comportamientos específicos- en cuatro categorías: delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, delitos informáticos, delitos relacionados con la pornografía infantil y delitos relacionados con infracciones de la propiedad intelectual y derechos afines. La Convención también dispone que deben ser sancionadas las figuras de tentativa y complicidad en tales delitos, exige responsabilidad penal a las personas jurídicas y hace hincapié en que las sanciones deben ser efectivas, proporcionadas y disuasorias, incluyendo penas privativas de libertad.

En los delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, la Convención refiere a los siguientes: el *acceso ilícito* (tipificación del acceso deliberado e ilegítimo a todo o parte de un sistema informático), la *interceptación ilícita* (tipificación de la interceptación deliberada e ilegítima por medios técnicos de datos informáticos en transmisiones no públicas dirigidas a un sistema informático, originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos), los *ataques a la integridad de los datos* (tipificación de

todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos), los *ataques a la integridad del sistema* (tipificación de la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de datos informáticos), el *abuso de los dispositivos* (tipificación de la comisión deliberada e ilegítima de actos como a) de producción, venta, obtención para su utilización, importación, difusión u otra forma de puesta a disposición de: i) cualquier dispositivo, incluido un programa informático, concebido o adaptado principalmente para la comisión de los delitos señalados anteriormente; ii) una contraseña, código de acceso o datos informáticos similares que permitan acceder a todo o parte de un sistema informático, con intención de que sean utilizados para cometer los delitos señalados anyteriormente; y, b) la posesión de algunos de los elementos contemplados en i) o ii) del apartado a) con intención de que sean utilizados para cometer cualquiera de los delitos previstos anteriormente).[7]

En la actualidad, Ecuador cuenta con normas que sancionan este tipo de delitos con penas de privación de libertad. El artículo 178 del Código Orgánico Integral Penal (COIP) sanciona con pena privativa de la libertad de uno a tres años la violación del derecho a la intimidad. El artículo 229 *ejusdem* sanciona asimismo con uno a tres años de privación de libertad la revelación ilegal de información de bases de datos. El artículo 230 sanciona con una pena de tres a cinco años de privación de libertad la interceptación de comunicaciones. El artículo 232, con la misma pena, al ataque a la integridad de sistemas informáticos. El artículo 233 sanciona de la misma manera los delitos contra la información pública reservada legalmente. Y, el artículo 234, establece la misma pena, al acceso no consentido a un sistema informático, telemático o de telecomunicaciones.

En los delitos informáticos, la Convención refiere a la *falsificación informática* (tipificación de la introducción, alteración, borrado o supresión deliberados e ilegítimos de datos informáticos que genere datos no auténticos con la intención de que sean tomados o utilizados a efectos legales como auténticos, con independencia de que los datos sean legibles e inteligibles directamente) y al *fraude informático* (tipificación de los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a) la introducción, alteración, borrado o supresión de datos informáticos; b) cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para

7 Ibídem.

otra persona).[8] En Ecuador, el COIP sanciona en particular el *phishing* y el *pharming* en el artículo 230, numeral 2, con una pena de de tres a cinco años de privación de la libertad; y en el artículo 231, sanciona con la misma pena el fraude informático para procurarse la transferencia electrónica de un activo patrimonial. Y en los artículos del 190 al 194, sanciona la apropiación fraudulenta por medios electrónicos.

En los delitos relacionados con la pornografía infantil la Convención dispone tipificar la comisión deliberada e ilegítima de los siguientes actos: a) producción de pornografía infantil con la intención de difundirla a través de un sistema informático; b) oferta o puesta a disposición de pornografía infantil a través de un sistema informático; c) difusión o transmisión de pornografía infantil a través de un sistema informático; d) adquisición, para uno mismo o para otros, de pornografía infantil a través de un sistema informático; y, e) posesión de pornografía infantil en un sistema informático o en un dispositivo de almacenamiento de datos informáticos.[9] En Ecuador, no se han tipificado con especificidad la integralidad de tales comprotamientos, pero el artículo 91 del COIP, numeral 2, sanciona con una pena privativa de libertad de 13 a 16 años, la explotación sexual de personas incluida la prostitución forzada, el turismo sexual y la pornografía infantil y los artículos 103 y 104 *ejusdem* sancionan con una pena privativa de libertad de 13 a 16 años y de 10 a 13 años, respectivamente, la producción y comercialización de prornografía con utilización de niños, niñas y adolescentes.[10]

Y en los delitos relacionados con infracciones de la propiedad intelectual y derechos afines, la Convención dispone tipificar las infracciones de la propiedad intelectual conforme las obligaciones contraídas en aplicación del Acta de París de 24 de julio de 1971 con la cual se revisó el Convenio de Berna para la protección de las obras literarias y artísticas, del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Derechos de Autor, a excepción de cualquier derecho moral otorgado por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático. Asimismo, dispone tipificar las infracciones de los derechos afines, de

8 Ibídem.

9 Ibídem.

10 El Convenio entiende por pornografía infantil todo material pornográfico que contenga la representación visual de: a) un menor adoptando un comportamiento sexualmente explícito; b) una persona que parezca un menor adoptando un comportamiento sexualmente explícito; c) imágenes realistas que representen a un menor adoptando un comportamiento sexualmente explícito. Asimismo, entiende por menor a toda persona menor de 18 años.

conformidad con las obligaciones que haya asumido en aplicación de la Convención Internacional sobre la Protección de los Artistas, Intérpretes o Ejecutantes, los Productores de Fonogramas y los Organismos de Radiodifusión (Convención de Roma), del Acuerdo sobre los aspectos de los derechos de propiedad intelectual relacionados con el comercio y del Tratado de la OMPI sobre Interpretación o Ejecución y Fonogramas, a excepción de cualquier derecho moral conferido por dichos Convenios, cuando tales actos se cometan deliberadamente, a escala comercial y por medio de un sistema informático.[11]

En Ecuador, la disposición derogatoria vigésima segunda del COIP, derogó los artículos 319 al 331, y el segundo inciso del artículo 342 de la Codificación de la Ley de Propiedad Intelectual, publicada en el Suplemento del Registro Oficial No. 426 de 28 de diciembre de 2006, que tipificaban tales conductas entre otras; por lo que, en Ecuador la transgresión particular de los derechos de propiedad intelectual no constituye en realidad delito penal. Situación que debe corregirse a fin de integrarnos al entramado normativo de la Convención de Budapest.

Ahora bien, para Téllez, los delitos informáticos son conductas típicas, antijurídicas y culpables que tienen a las computadoras como instrumento o fin.[12] Los delitos informáticos -como se ha indicado anteriormente- están tipificados en Ecuador en el Código Orgánico Integral Penal (COIP) y engloban ciertamente más allá de los referidos brevemente con anterioridad con relación a lo dispuesto por la Convención de Budapest. El COIP integra los siguientes delitos informáticos y otras disposiciones relacionadas con ellos: 1) violación a los derechos humanos, diversas formas de explotación, artículo 103;[13] 2) delitos contra el derecho a la intimidad personal y familiar, artículos 178,179 y 180;[14] 3)

---

11 Ibídem.

12 J. Téllez Valdés, *Derecho informático*, (México: MC Graw Hill, 2008), 188.

13 "Art. 103.- Pornografía con utilización de niñas, niños o adolescentes.- La persona que fotografíe, filme, grabe, produzca, transmita o edite materiales visuales, audiovisuales, informáticos, electrónicos o de cualquier otro soporte físico o formato que contenga la representación visual de desnudos o semidesnudos reales o simulados de niñas, niños o adolescentes en actitud sexual; será sancionada con pena privativa de libertad de trece a dieciséis años.

Si la víctima, además, sufre algún tipo de discapacidad o enfermedad grave o incurable, se sancionará con pena privativa de libertad de dieciséis a diecinueve años.

Cuando la persona infractora sea el padre, la madre, pariente hasta el cuarto grado de consanguinidad o segundo de afinidad, tutor, representante legal, curador o pertenezca al entorno íntimo de la familia; ministro de culto, profesor, maestro, o persona que por su profesión o actividad haya abusado de la víctima, será sancionada con pena privativa de libertad de veintidós a veintiséis años."

14 "Art. 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe, reproduzca, difunda o publique

delitos contra el derecho al honor y buen nombre, artículo 182;[15] 4) delitos contra el derecho a la propiedad, artículos 190,191,192,193,194 y 195;[16] 5) delitos contra el derecho a la integridad, artículo 232; 6) prueba, disposiciones generales, artículos 453 y 454; 7) delitos contra la seguridad de los activos, sistemas de información y comunicación, artículos 229, 230, 231, 232, 233 y 234;[17] 8) actualizaciones especiales de investigación, artículos 475, 476 y 477; 9) medios de prueba, artículo 498; 10) documentos, reglas generales, artículos 499 y 500; y, 11) la pericia, reglas generales artículo.[18] Sin embargo, no tipifica el ciberbulling, los ciberataques, las subastas y ventas ilegales en internet, el uso de redes robot

---

datos personales, mensajes de datos, voz, audio y vídeo, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y vídeo en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo previsto en la ley.

Art. 179.- Revelación de secreto.- La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

Art. 180.- Difusión de información de circulación restringida.- La persona que difunda información de circulación restringida será sancionada con pena privativa de libertad de uno a tres años.

Es información de circulación restringida:

1. La información que está protegida expresamente con una cláusula de reserva previamente prevista en la ley.
2. La información producida por la Fiscalía en el marco de una investigación previa.
3. La información acerca de las niñas, niños y adolescentes que viole sus derechos según lo previsto en el Código Orgánico de la Niñez y Adolescencia."

15 "Art. 182.- Calumnia.- La persona que, por cualquier medio, realice una falsa imputación de un delito en contra de otra, será sancionada con pena privativa de libertad de seis meses a dos años.

No constituyen calumnia los pronunciamientos vertidos ante autoridades, jueces y tribunales, cuando las imputaciones se hubieren hecho en razón de la defensa de la causa.

No será responsable de calumnias quien probare la veracidad de las imputaciones. Sin embargo, en ningún caso se admitirá prueba sobre la imputación de un delito que hubiere sido objeto de una sentencia ratificatoria de la inocencia del procesado, de sobreseimiento o archivo.

No habrá lugar a responsabilidad penal si el autor de calumnias, se retractare voluntariamente antes de proferirse sentencia ejecutoriada, siempre que la publicación de la retractación se haga a costa del responsable, se cumpla en el mismo medio y con las mismas características en que se difundió la imputación. La retractación no constituye una forma de aceptación de culpabilidad."

16 "Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada

o zombi, entre otras conductas,[19] situación que a la fecha parcialmente se ha corregido.

De manera que, Ecuador ciertamente ha evolucionado en la tipificación de los delitos informáticos y en la lucha generalizada -desde la perspectiva normativa- contra el cibercrimen, manteniendo incluso relación cercana con los cuatro ejes principales dispuestos por la Convención de Budapest: delitos de tecnología como fin, de tecnología como medio, de contenido e infracciones a la propiedad intelectual,[20] siendo esta última, lamentablemente, la menos favorecida. No obstante, a fin de fortalecer en particular el último de los ejes y promover de

---

con pena privativa de libertad de uno a tres años.
La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura a distancia, o violación de seguridades electrónicas, informáticas u otras semejantes.
Art. 191.- Reprogramación o modificación de información de equipos terminales móviles.- La persona que reprograme o modifique la información de identificación de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.
Art. 192.- Intercambio, comercialización o compra de información de equipos terminales móviles.- La persona que intercambie, comercialice o compre bases de datos que contengan información de identificación de equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.
Art. 193.- Reemplazo de identificación de terminales móviles.- La persona que reemplace las etiquetas de fabricación de los terminales móviles que contienen información de identificación de dichos equipos y coloque en su lugar otras etiquetas con información de identificación falsa o diferente a la original, será sancionada con pena privativa de libertad de uno a tres años.
Art. 194.- Comercialización ilícita de terminales móviles.- La persona que comercialice terminales móviles con violación de las disposiciones y procedimientos previstos en la normativa emitida por la autoridad competente de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.
Art. 195.- Infraestructura ilícita.- La persona que posea infraestructura, programas, equipos, bases de datos o etiquetas que permitan reprogramar, modificar o alterar la información de identificación de un equipo terminal móvil, será sancionada con pena privativa de libertad de uno a tres años.
No constituye delito, la apertura de bandas para operación de los equipos terminales móviles."
17 "Art. 229.- Revelación ilegal de base de datos.- La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.
Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será sancionada con pena privativa de libertad de tres a cinco años.
Art. 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

modo general la lucha contra el cibercrimen es necesario modificar algunos textos legales contenidos en el COIP e incluir otros, a fin de facilitar -en definitiva- la adhesión de Ecuador al Convenio de Budapest y optimizar la legislación penal sustantiva del ámbito nacional, en materia de los ciberdelitos.

En particular -a tono con el Convenio de Budapest-, debería precisarse la descripción típica del delito de *violación a la intimidad* contenido en el artículo 178 del COIP, a fin de que el mecanismo normativo de protección del derecho fundamental a la intimidad incluya sin lugar a dudas -tomando en consideración que el sistema de interpretación de la norma en esta materia

---

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información registrada o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito descrito en el inciso anterior.

Art. 231.- Transferencia electrónica de activo patrimonial.- La persona que, con ánimo de lucro, altere, manipule o modifique el funcionamiento de programa o sistema informático o telemático o mensaje de datos, para procurarse la transferencia o apropiación no consentida de un activo patrimonial de otra persona en perjuicio de esta o de un tercero, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena, será sancionada la persona que facilite o proporcione datos de su cuenta bancaria con la intención de obtener, recibir o captar de forma ilegítima un activo patrimonial a través de una transferencia electrónica producto de este delito para sí mismo o para otra persona.

Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

respecto de los tipós penales es literal y restringido-[21] la información personal contenida en soportes informáticos, digitales, ópticos, magnéticos u otros de similar naturaleza que almacenen información personal en cualquier tipo de formato; pues, si bien la norma *-lato sensu-* refiere a soportes de información y podemos comprender por aquellos, cualquier clase de dispositivos que nos permitan almacenar información en formato electrónico y, en general, sean fáciles de transportar, actualmente (y a la par con el desarrollo de la ciencia en materia de tecnologías de la información y comunicaciones) están proliferando, en la medida en la que el volúmen de información va creciendo, una gran variedad de dispositivos de toda clase en los que se puede almacenar información.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Art. 233.- Delitos contra la información pública reservada legalmente.- La persona que destruya o inutilice información clasificada de conformidad con la Ley, será sancionada con pena privativa de libertad de cinco a siete años.

La o el servidor público que, utilizando cualquier medio electrónico o informático, obtenga este tipo de información, será sancionado con pena privativa de libertad de tres a cinco años.

Cuando se trate de información reservada, cuya revelación pueda comprometer gravemente la seguridad del Estado, la o el servidor público encargado de la custodia o utilización legítima de la información que sin la autorización correspondiente revele dicha información, será sancionado con pena privativa de libertad de siete a diez años y la inhabilitación para ejercer un cargo o función pública por seis meses, siempre que no se configure otra infracción de mayor gravedad.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, desviar o redireccionar de tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años."

18 N. Ortiz Campos, "Normativa Legal sobre Delitos Informáticos en Ecuador". En: *Revista Científica Hallazgos 21*, 2019, vol. 4, No. 1, 100-111, 104, <http://revistas.pucese.edu.ec/hallazgos21/>.

19 Ibídem.

20 La propiedad intelectual se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio. Las legislaciones protegen la propiedad intelectual a través de las patentes, el derecho de autor y las marcas. Las legislaciones protegen la propiedad intelectual a través de las patentes, el derecho de autor y las marcas. (Ibídem, 107).

21 COIP, "Art. 13.- Interpretación.- Las normas de este Código deberán interpretarse de conformidad con las siguientes reglas... 2. Los tipos penales y las penas se interpretarán en forma estricta, esto es, respetando el sentido literal de la norma."

Además, conviene precisar asimismo en dicha norma la exclusión que realiza sobre la aplicación de la misma a las personas que divulgan audios o videos en los que intervienen personalmente, pues, de conformidad con el artículo 66, numeral 20, de la Constitución de la República y artículo 5, numeral 10, del mismo cuerpo normativo (COIP), todas las personas tienen el derecho a la intimidad personal y familiar, y por ello resulta razonable que se excluya de la sanción penal a aquellos que voluntariamente divulgan videos o audios sobre sí mismos, y no a quienes podrían divulgar audios o videos sobre terceras personas sin su autorización manifiesta bajo la supuesta excusa legal de la sola intervención o participación personal en el mismo de quien finalmente lo divulga. Es claro e indiscutible que el alcance y contenido del derecho reconocido constitucional y legalmente a la intimidad personal y familiar -y que actúa como bien jurídico protegido por la norma penal- es de corte y orientación individual pues, se encuentra entre los derechos de libertad declarados por la Constitución de la República en el artículo 66, en cuyo caso, el ejercicio de la libertad de una persona indefectiblemente concluye en donde empieza el ejercicio de la libertad del otro. No conviene desde ningun punto de vista que se autorice la divulgación de un audio o un video de un tercero que no ha consentido en ello por el solo hecho de que quien divulga a participado en el mismo.[22]

Así también -a tono con el Convenio de Budapest y en consideración al sistema de interpretación normativa de los tipos penales descritos en el Código Orgánico Integral Penal vigente- conviene complementar la descripción de los comportamientos penados en los artículos 104 y 232 del COIP, tomando como referente la relación de acciones u omisiones relatadas en el Capítulo 2 del Convenio de Budapest, en especial, aquellos verbos rectores previstos que no han sido considerados por la norma nacional. Es más, resulta recomendable precisar e incorporar en el artículo 232 de la codificación nacional, que tipifica el delito de ataque a la integridad de sistemas informáticos, la conducta ilícita particular de la creatura de programas informáticos que aprovechen las fallas previamente desconocidas en los software de equipos de terceros a fin de filtrar datos confidenciales, dañar infraestructura clave o desarrollar una base para futuros ataques.

---

22 Considérese a modo de ejemplo un caso en el que, un individuo realiza un video de un encuentro sexual con su pareja sin que la pareja conozca y menos aun consienta en ello y luego el individuo divulgue el mismo por haber participado personalmente en dicho encuentro. En una situación así, el derecho de la pareja de quien divulgaría el video, bajo la exclusión hecha legalmente por el actual artículo 178 del COIP, quedaría completamente desprotegido, tornándose la exclusión legal en un mecanismo de vulneración de los derechos de la tercera persona involucrada, es decir, de la pareja de quien divulgaría el video.

De la misma manera resulta adecuado integrar en la tipificación de los delitos contenidos en los artículos 182 (calumnia) y 208A (falsificación de marcas y piratería lesiva contra los derechos de autor) la posibilidad de que las acciones lesivas ahí descritas se realicen a través de medios informáticos, digitales o virtuales, o aquellos vinculados a ellos. Si bien, la tipificación actual tiende a acoger la frase "por cualquier medio", el convencionalismo social ha tendido a excluir o a desconocer la capacidad nociva de algunos medios de comunicación, informáticos, digitales o virtuales de uso cada vez más frecuente por la ciudadanía en general, bajo el velo de la protección aparente de ciertos derechos como la libertad de expresión o la libre iniciativa económica privada, siendo indispensable, a efectos de acoger el régimen jurídico contenido en el Convenio de Budapest, incorporar en la redacción legal, tales instrumentos (medios), debiendo ciertamente respetar los estándares internacionales y nacionales en materia de derechos humanos y fundamentales.

Finalmente, debe, en igual sentido -y a tono con el Protocolo adicional al Convenio de Budapest respecto de la criminalización de actos de naturaleza racista y xenofóbica cometidos a través de sistemas de ordenador-, clarificarse en el ordenamiento punitivo nacional que las expresiones de descrédito o deshonra contra una o más personas con contenido xenofobo, racista o discriminatrio, realizadas a través de medios de comunicacioón, informáticos, digitales o virtuales constituyen acciones configuradoras del delito de odio y no pueden ser consideradas como una infracción penal "menor" (contravención penal), pues, en el marco normativo del Convenio de Budapest, tal comportamiento equivaldría a una conducta delictiva calumniosa; en cuyo caso, atendiento la estructura legal prevista por el COIP, conviene, en todo caso, ratificar que tal comportamiento dañoso configura en particular un delito, pues, supondría al menos un régimen de protección superior al de la contravención y consecuente con el régimen regulatorio de la Convención. Cabe por último especificar (en tono al protocolo antes mencionado y al sistema constitucional ecuatoriano) que, la difusión de material racista o xenófobo por medio de sistemas informáticos constituye un acto de odio que debe ser sancionado de conformidad con el COIP.

En dicho contexto se propone la presente Ley reformatoria del Código Orgánico Integral Penal, a fin de promover la lucha contra el cibercrimen y adecuar nuestra legislación al marco normativo internacional del Convenio de Budapest.

EL PLENO DE LA ASAMBLEA

CONSIDERANDO:

Que, la Constitución de la República si bien no menciona delito informático alguno, enarbola con claridad un esquema de protección de ciertos bienes jurídicos que son objeto de las conductas que sancionan tales ilícitos, en particular, el acceso universal a las tecnologías de información y comunicación de acuerdo a lo declarado por el artículo 16 de la Carta Magna y el derecho a la intimidad personal y familiar incorporado en el número 20 del artículo 66 de la misma;

Que, la Ministra de Gobierno ha manifestado públicamente su preocupación porque Ecuador sea uno de los pocos países de la región que no ha firmado ni ratificado el Convenio sobre Ciberdelincuencia, conocido como: *Convenio de Budapest;*

Que, el Convenio de Budapest tiene como objetivo armonizar la legislación relativa al cibercrimen, mejorar las capacidades de investigación de delitos informáticos y establecer un régimen efectivo de cooperación y asistencia internacional;

Que, la adhesión de Ecuador a este convenio significaría, sin lugar a dudas, un avance enorme en materia de lucha contra la ciberdelincuencia, pues, el carácter transnacional de la ciberdelincuencia necesariamente empuja a todas las naciones a adoptar un enfoque normativo de cooperación y armonización regulatoria entre todos los países para enfrentar la naturaleza global del fenómeno;

Que, la Asamblea Nacional debe facilitar el proceso de invitación y futura adhesión de Ecuador al Convenio de Budapest, adoptando las medidas legislativas dispuestas para el ámbito nacional en dicha convención internacional, en particular e inicialmente las de contenido de derecho penal sustantivo;

Que, el Capítulo II del Convenio de Budapest detalla las medidas que deben adoptar los estados suscriptores a nivel nacional de contenido de derecho penal sustantivo y prevé la tipificación de cuatro categorías de delitos: delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos, delitos informáticos, delitos relacionados con la pornografía

infantil y delitos relacionados con infracciones de la propiedad intelectual y derechos afines;

Que, si bien en el Código Orgánico Integral Penal (COIP) se han tipificado varias de las conductas detalladas por el Convenio de Budapest, a tono con éste y en consideración al sistema de interpretación normativa de los tipos penales descritos en el Código Orgánico Integral Penal vigente, conviene complementar la descripción de los comportamientos penados por el mismo tomando como referente la relación de acciones u omisiones relatadas en el Capítulo 2 del Convenio de Budapest, en especial, aquellos verbos rectores previstos en el marco regulatorio internacional que no han sido considerados por la normativa nacional, debiendo, además, precisar con claridad aquellas conductas sancionadas que se realizan por intermedio de sistemas o herramientas informáticas;

Que, a fin de promover la lucha contra el cibercrimen en Ecuador es necesaria realizar la reforma legal propuesta a fin de facilitar la adhesión de Ecuador al Convenio de Budapest y al Protocolo adicional respecto de la criminalización de actos de naturaleza racista y xenofóbica cometidos a través de sistemas de ordenador; y,

En ejercicio de la facultad prevista en el número 6 del artículo 120 de la Constitución de la República y artículos 52, 53, 54 y siguientes de la Ley Orgánica de la Función Legislativa, el Pleno de la Asamblea Nacional expide la siguiente:

LEY ORGÁNICA REFORMATORIA DEL CÓDIGO ORGÁNICO INTEGRAL PENAL

Art. 1.- Agréguese en el primer inciso del artículo 178, luego de "información contenida en soportes informáticos" y antes de "comunicaciones privadas o reservadas de otra persona por cualquier medio" la frase: "digitales, ópticos, magnéticos u otros de similar naturaleza que almacenen información personal en cualquier tipo de formato".

Art. 2.- Refórmese el segundo inciso del artículo 178, que en adelante dirá:

"No son aplicables estas normas para la persona que divulgue grabaciones de audio y video personales, ni cuando se trate de información pública de acuerdo

con lo previsto en la ley. La divulgación de audios y videos personales que involucre a terceras personas requerirá la autorización manifiesta de aquellas."

Art. 3.- Agréguese al numeral 1 del artículo 232, luego de "adquiera" y antes de "envíe" la palabra: "posea".

Art. 4.- Agréguese al artículo 232, previamente a su último inciso, un numeral 3, que en adelante dirá:

"3. Cree programas informáticos que aprovechen las fallas previamente desconocidas en los software de equipos de terceros a fin de filtrar datos confidenciales, dañar infraestructura clave o desarrollar una base para futuros ataques."

Art. 5.- Refórmese el artículo 104, que en adelante dirá:

"Art. 104.- Comercialización de pornografía con utilización de niñas, niños o adolescentes.- La persona que publicite, adquiera, compre, posea, porte, transmita, difunda, descargue, almacene, importe, exporte, oferte, ponga a disposición o venda, por cualquier medio, sistema o dispositivo de almacenamiento de datos, para uso personal o para intercambio, pornografía de niños, niñas y adolescentes, será sancionada con pena privativa de libertad de diez a trece años."

Art. 6.- Refórmese el primer inciso del artículo 182, que en adelante dirá:

"Art. 182.- Calumnia.- La persona que realice una falsa imputación de un delito en contra de otra, por cualquier medio, inclusive prensa, radio, televisión o a través de páginas web o cuentas en redes sociales, será sancionada con pena privativa de libertad de seis meses a dos años."

Art. 7.- Agréguense, en el tercer inciso del artículo 208A, luego de "produzca, reproduzca o comercialice a escala comercial" y antes de "mercancía pirata que lesione el derecho de autor para las obras registradas o no", la frase: "por cualquier medio, inclusive a través de sistemas informáticos".

Art. 8.- Agréguese al artículo 396 un inciso luego del numeral 1, que en adelante dirá:

"Las expresiones de descrédito o deshonra contra una o más personas en razón de su nacionalidad, etnia, lugar de nacimiento, edad, sexo, identidad de género u orientación sexual, identidad cultural, estado civil, idioma, religión, ideología, condición socioeconómica, condición migratoria, discapacidad, estado de salud o portar VIH, por cualquier medio, inclusive prensa, radio, televisión o a través de páginas web o cuentas en redes sociales, se considerarán actos de odio y se sancionarán de conformidad con el artículo 177 de este Código."

Art. 9.- Agréguese al artículo 177 un inciso final, que en adelante dirá:

"La difusión de material racista y xenófobo por medio de sistermas informáticos se considerará un acto de odio que será sancionado de conformidad con el presente artículo."

DISPOSICIÓN FINAL.- La presente ley entrará en vigencia a partir de la fecha de su publicación en el Registro Oficial.

Dado y suscrito en la sede de la Asamblea Nacional, ubicada en el Distrito Metropolitano de Quito, provincia de Pichincha, a los ... días del mes de ... de dos mil ...