CRIMINALIDAD INFORMÁTICA Y LA DISCUSIÓN SOBRE EL BIEN JURÍDICO PROTEGIDO EN LOS DELITOS INFORMÁTICOS

Jesús Cornejo Arismendi[1]

1. Introducción

El profesor Felipe Villavicencio fue reconocido a nivel nacional e internacional por su incansable labor como catedrático, académico y litigante. Dedicó su vida profesional al estudio y al ejercicio del derecho penal, motivando a generaciones de penalistas en las diversas facultades de derecho de nuestro país en las que compartió generosamente sus conocimientos. Entre sus tantas virtudes se sabe de su pasión por el conocimiento y su constante aspiración a la adaptación a los cambios y épocas en el derecho penal.

Así lo hizo ampliamente en el campo de la teoría del delito, pero también lo supo hacer en otros espacios más especializados del derecho penal. En el año 2014, al poco de tiempo de la publicación de la Ley N° 30171 que modificó la Ley N° 30096 – Ley de delitos informáticos, el profesor Villavicencio publicó un artículo titulado "Delitos informáticos" en el que expuso diversas ideas sobre la criminalidad informática, la ley de delitos informáticos, sus fuentes de inspiración y (en aquel entonces) su reciente modificatoria.

Los delitos informáticos, aunque tratados de forma esporádica en nuestra doctrina nacional, resultan de actualidad y de necesario tratamiento. En un mundo en el que la aceleración de los procesos tecnológicos es constante y en el que la tecnología permite realizar una gran cantidad de tareas de forma virtual, no sería difícil que la criminalidad se vea acrecentada.

En ese sentido, el presente trabajo, inspirado en el trabajo del profesor Villavicencio, pretende exponer brevemente algunas ideas referidas específicamente a la criminalidad informática y la actualización del debate sobre el bien jurídico protegido en los delitos informáticos, a partir del desarrollo académico desarrollado en nuestro país y en el extranjero, principalmente en España y Chile.

2. La Tipificación de los Delitos Informáticos en el Perú

Los delitos informáticos aparecieron por primera vez en nuestro ordenamiento con la publicación de la Ley N° 27309 el 17 de julio de 2000. Dicha norma incorporó los artículos 207-A°, 207-B° y 207-C° al Código Penal, a los que posteriormente se sumó el artículo 207-D° que fue introducido varios años después con la Ley N° 30076 publicada el 19 de agosto del año 2013.

---

1 Abogado por la Pontificia Universidad Católica del Perú. Miembro del Grupo de Investigación en Derecho Penal y Corrupción – DEPEC. Asociado del Área Penal del Estudio Benites, Vargas & Ugaz.

Los artículos mencionados constituyeron una suerte de primera generación de delitos informáticos en nuestro país, aunque fueron derogados posteriormente con la entrada en vigencia de la Ley N° 30096 titulada "Ley de Delitos Informáticos" (en adelante, la Ley o Ley de Delitos Informáticos) publicada el 22 de octubre del año 2013. La promulgación de una ley especial de delitos informáticos fue propuesta a través de dos proyectos de ley (034/2011-CR y 307/2011-CR). El Dictamen recaído en los proyectos mencionados fue emitido por la Comisión de Justicia y Derechos Humanos del Congreso de la República del Perú (2012) en el periodo anual de sesiones 2011 – 2012. En dicho Dictamen se identificó la necesidad de la creación de una ley especial ante la existencia de vacíos en el Código Penal respecto a sanción penal de los delitos cometidos a través herramientas y conocimientos informáticos.

Posteriormente, la Ley de Delitos Informáticos fue modificada por la Ley N° 30171, publicada el 10 de marzo de 2014. Esta modificación respondió a una adecuación y armonización de los delitos informáticos previstos en nuestro ordenamiento interno con el Convenio sobre Ciberdelincuencia del año 2001 (en adelante, Convenio de Budapest) (Villavicencio, 2014).

En efecto, la modificación de la Ley fue propuesta hasta en tres proyectos de ley (2991/2013-CR, 2999/2013-CR y 3017/2013-CR), a propósito de los cuales la Comisión de Justicia y Derechos Humanos de nuestro Congreso de la República, en el periodo anual de sesiones 2013 – 2014, señaló en su Dictamen que con posterioridad a la promulgación de la Ley se había evidenciado que algunas de sus disposiciones eran incompatibles con los estándares previstos en el Convenio de Budapest (2013).

Si bien el Convenio de Budapest había sido adoptado mucho tiempo antes de la modificación de la Ley (el 23 de noviembre del año 2001), el Perú no fue parte ni pudo adherirse al mismo hasta muchos años después, pues el 13 de febrero del año 2019 se publicó la Resolución Legislativa N° 30913, en cuyo artículo único, se aprobó el Convenio mencionado (Congreso de la República, 2019).

Según la Comisión del Congreso antes referida (2013), la adhesión del Perú al Convenio fue posible gracias a la invitación que el Comité de Ministros del Consejo de Europa extendió al Perú, pues al no ser miembro del Consejo de Europa y al no haber participado en la realización del Convenio, el Estado peruano no había podido adherirse al mismo con anterioridad.

Desde la aprobación del Convenio de Budapest hasta la actualidad la Ley no ha vuelto a ser modificada. En todo caso, desde antes, con la entrada en vigencia de la Ley N° 30171, ya se encontraban tipificados los delitos contra Datos y Sistemas Informáticos, entre ellos, el delito de Acceso Ilícito (artículo 2°), Atentado contra la integridad de datos informáticos (artículo 3°) y Atentado a la integridad de los sistemas informáticos (artículo 4°), así como otros delitos que protegen la Indemnidad y Libertad Sexual (artículo 5°), la Intimidad y el Secreto de las Comunicaciones (artículo 7°), el Patrimonio (artículo 8°) y la Fe Pública (artículo 9°), tipificación que guarda correlación con las conductas previstas también en el Convenio.

Más allá de la adhesión tardía de nuestro país al Convenio Budapest, es claro que la Ley de Delitos Informáticos y su modificatoria (que, ciertamente, la adecuó a los estándares del Convenio), marcaron un cambio decidido en la tipificación de los delitos informáticos.

En tal sentido, de forma previa a la revisión de la discusión del bien jurídico protegido en los delitos informáticos, conviene una revisión más conceptual de la criminalidad informática, así como del contexto criminológico identificado por el legislador y que impulsó la promulgación de la Ley de Delitos Informáticos, así como el que posteriormente ha desarrollado la doctrina. Del mismo modo, en la medida que en lo que sigue del presente artículo se emplean los términos *sistemas informáticos* y *datos informáticos*, es pertinente anotar la definición otorgada a estos en la Novena Disposición Complementaria Final de Ley de Delitos Informáticos en la que se estableció lo siguiente:

> Para efectos de la presente Ley, se entenderá, de conformidad con el artículo 1 del Convenio sobre la ciberdelincuencia, Budapest, 23.XI.2001:
> a. Por sistema informático: todo dispositivo o conjunto de dispositivos interconectados o relacionados entre sí, cuya función, o la de alguno de sus elementos, sea el tratamiento automatizado de datos en ejecución de un programa.
> b. Por datos informáticos: toda representación de hechos, información o conceptos expresados de cualquier forma que se preste a tratamiento informático, incluido los programas diseñador para que un sistema informático ejecute una función. (Ley N° 30096, 2013).

3. Criminalidad Informática y su Contexto Criminológico

La Organización de las Naciones Unidas – ONU (2000) citada por Lara, Martínez y Viollier (2014), señala que la criminalidad informática puede ser entendida en un sentido lato y en uno estricto. El primero de ellos se refiere a los delitos que son realizados con el empleo de un sistema o red informática, mientras que el segundo corresponde a aquellos delitos que tienen como fin el ataque de los sistemas informáticos o datos que estos procesan.

Asimismo, el profesor Villavicencio señalaba que la criminalidad informática puede ser entendida como aquella que concibe conductas dirigidas a burlar los sistemas de dispositivos de seguridad, ya sea que se trate de la invasión de computadoras, correos o sistemas de datos mediante una clave y que solamente pueden ser cometidas mediante tecnología en sentido estricto; mientras que en un sentido amplio podría entenderse a aquellas conductas en las que las tecnologías de la información o comunicación eran el objetivo, medio o el lugar de ejecución aunque se afectasen a distintos bienes jurídicos (2014).

Independientemente de la forma en que se desarrolla la criminalidad informática, la realidad nos muestra constantemente que la transformación tecnológica no se detiene, y su desarrollo sostenido ha permitido el surgimiento de nuevas formas de realizar nuestras actividades cotidianas, facilitar herramientas para la ejecución de tareas en el ámbito laboral y, en general, permitir el intercambio de información y diversas actividades de orden económico.

En efecto, la Comisión de Justicia y Derechos Humanos del Congreso peruano que evaluó los proyectos de ley para la promulgación de la Ley de Delitos Informáticos adelantaba que la expansión del uso de la informática había alcanzado todos los ámbitos de la vida contemporánea, por lo que en la medida que aumentaba la calidad de vida de las personas también se incrementaban los riesgos (2012). En tal sentido, la mencionada Comisión señalaba cuatro características de dichos riesgos:

a) No existe una estructura jerarquizada que permita establecer un sistema de control en la red.
b) Existe un creciente número de usuarios y, por lo tanto, de víctimas como de autores. A ello se suma el anonimato de los cibernautas lo que facilita la comisión de los delitos.
c) La facilidad en el acceso a la información y la alteración de datos.
d) La manifiesta capacidad de generar peligros globales.

Para aquel entonces, la mencionada Comisión en su Dictamen adelantaba que los delitos informáticos tipificados en los artículos 207-A°, 207-B° y 207-C° y 207-D° del Código Penal ya no podían ser aplicados con precisión (Congreso de la República, 2012). Esto tiene mucho sentido si se tiene en consideración que la mayoría de los delitos informáticos aparecieron en el año 2000, con lo que es entendible que la realidad y la criminalidad informática había superado lo previsto en el ordenamiento.

En los últimos tiempos ha sido innegable la convivencia en el mundo digital e informático. El empleo del internet a través de computadoras y celulares inteligentes (*smartphones*), así como el desarrollo de plataformas tecnológicas nos permiten hoy en día realizar diversas actividades, tales como la revisión de cámaras de seguridad, el pago de servicios básicos, transferencias bancarias, la revisión, recepción y envío de comunicaciones electrónicas, mensajería instantánea, entre otros.

Sin embargo, la criminalidad informática en lo absoluto ha dejado de ser un asunto de menor entidad. Para el año 2019, los fraudes informáticos alcanzaron un total de 2,097 denuncias penales, según informaba el jefe de la División de Investigación de Alta Tecnología de la Policía Nacional del Perú (Pichihua, 2020).

Al tiempo que se escribe este artículo se vive una pandemia mundial por la propagación del Covid-19 que, más allá de los efectos en la economía, ha generado una aceleración en el uso de la tecnología extendiéndose a aquellos ámbitos en los que, incluso, se asumía una necesaria participación física. Por ejemplo, podemos ver que las clases presenciales dictadas a los estudiantes escolares y universitarios hoy en día son dictadas a través de plataformas digitales; mientras tanto, también es posible que las compras en los supermercados puedan ser realizadas a través de internet, lo que supone tanto el pedido de productos como el pago por su adquisición.

Este contexto puede ser mejor comprendido con la ayuda de la autora chilena Laura Mayer, quien señala que la masificación de las tecnologías de la información y comunicación y, sobretodo, del internet, operaría como un factor criminógeno,

cuando menos, en dos sentidos. Por una parte, favorecería la comisión y el incremento de la criminalidad informática. En segundo término, favorecería la expansión de daños de grandes dimensiones (2018).

Además, la mencionada autora expone los contextos de la comisión de los delitos informáticos. En lo que concierne al acceso a internet, explica que estos ilícitos pueden ser realizados desde cualquier lugar (ya sea desde un domicilio, un lugar púbico con conexión a internet o desde un centro de labores) o país. Inclusive, en la doctrina, se ha trabajado la responsabilidad penal internacional en los ataques informáticos y su calificación como crímenes internacionales (Ambos, 2015).

Como apunte adicional, la profesora Mayer también nos indica que los autores del delito se caracterizan por tener conocimientos técnicos en informática, por lo que, ante una mayor preparación del autor, se requerirá un estándar técnico más elevado de quien vaya a investigar el crimen (2018); asimismo, cualquiera que emplee una computadora o que acceda a internet puede ser víctima de un delito informático.

4. Los Delitos Informáticos y el Bien Jurídico Protegido

Esta sección tiene por objeto poner sobre la mesa las principales posturas sobre el bien jurídico protegido en los delitos informáticos, y a partir de ello fomentar la actualización y el desarrollo del debate sobre esta materia. Para lo que me propongo, echaré mano del trabajo realizado por la profesora Laura Mayer, titulado "El bien jurídico protegido en los delitos informáticos" (2017) en el que, sobre la base de la experiencia chilena, expone el panorama actual de los postulados de la doctrina y realiza algunas propuestas.

4.1 La Tutela de Bienes Jurídicos Tradicionales

Esta hipótesis desarrollada por la doctrina, nos explica Mayer, sostiene que los delitos informáticos no buscan la protección de un bien jurídico específicamente informático, en la medida que este sería un contexto que sirve, en realidad, para la afectación de bienes jurídicos tradicionales tales como la intimidad, el patrimonio o la fe pública (2017).

De este parecer es el profesor chileno Fernando Londoño quien señala que, ciertamente, los delitos informáticos presentan una particularidad en la forma en que se realizan, pero, finalmente, la afectación producida se refiere a los bienes jurídicos tradicionales. De manera más específica señala lo siguiente:

> Si algo ha caracterizado al "derecho penal informático" es el de precisamente pretender ser un derecho penal informático, es decir un "algo especial" dentro del derecho penal en general. Si se pregunta a este pretendido "derecho penal especial" qué es lo que tiene de especial, deberá responder –con razón- que los que caracteriza a "sus delitos" es la especial (nueva, moderna, insólita) modalidad comisiva: la afectación de los "tradicionales" bienes jurídicos" (la intimidad, el patrimonio, la fe pública, etc.), pero no ya por la vía de actuaciones ejecutadas en el mundo real sino ahora por la vía de acciones llevadas a cabo en un mundo virtual de la informática. (Londoño, 2004, pág. 173)

En el mismo sentido de lo anterior se ha pronunciado el profesor español Norberto De la Mata al señalar que muchos de los conceptos que se emplean en los contextos digitales son afines a los de la "realidad más tradicional", entre ellos, archivos, firmas falsas, usurpación de identidades, por lo que no existiría diferencias sustanciales entre el mundo real y el virtual, sus participantes, ni en sus interrelaciones ni en los entornos en los que se desenvuelven aquéllos, en la medida que el contexto digital pretende reproducir dicha *realidad* de forma virtual (2007).

Entonces, para este sector de la doctrina si bien se reconoce y resulta de importancia el surgimiento de las herramientas informáticas y el desarrollo de un espacio "virtual", estos elementos aún no constituirían por sí mismos un interés que sea lo suficientemente relevante como para que pueda ser protegido por el derecho penal.

En todo caso, según esta teoría, el derecho penal no desmerecería la existencia de conductas en el ámbito informático que vulneran bienes jurídicos tradicionales como los ya mencionados. En efecto, la finalidad de las conductas estaría principalmente dirigida a defraudar patrimonialmente, o suplantar identidades o producir un engaño en la víctima con fines delictivos.

4.2 La Tutela de un Bien Jurídico Específico, Propiamente Informático: la Funcionalidad Informática

Esta postura parte de la evaluación de los delitos informáticos en sentido estricto y asume que el bien jurídico protegido es uno específico, propiamente informático, distinto del que protegen los delitos tradicionales, cuyo reconocimiento se justifica si dichos delitos inciden en un sistema informático o en las redes computacionales (Mayer, 2017). La misma autora, quien desarrolla en extenso esta postura en su trabajo, finalmente concluye que el interés a ser protegido es la *funcionalidad informática*.

La premisa de la que parte la referida profesora consiste en que un bien jurídico específico, propiamente informático, no será afectado en aquellos casos en los que se cometen delitos mediante el empleo de una computadora o cuando se afecta a una computadora entendida como soporte lógico (Mayer, 2017), como suele ocurrir, por ejemplo, en los fraudes informáticos (en los que se afecta el patrimonio a través del empleo de una computadora y el internet).

Según Mayer (2017), las computadoras adquieren una relevancia particular, dado que constituyen eslabones de una red de interconexión entre las personas, y es en dicho contexto en el que las funciones de los sistemas informáticos pueden verse afectadas. Por lo tanto, señalar la existencia de un bien jurídico específico, propiamente informático, tiene sentido cuando, conforme se señala líneas atrás, la conducta incide en el uso de un soporte lógico de un sistema informático y/o en el uso de redes computacionales.

Entonces, la *funcionalidad informática* equivale al conjunto de condiciones que permiten que los sistemas informáticos operen dentro de un marco tolerable de riesgo: por una parte, dicha funcionalidad se referirá a la capacidad de los sistemas

informáticos de realizar adecuadamente las operaciones que les son propias (por ejemplo, el intercambio o almacenamiento de datos o información); mientras que, por otro lado, se concentrará también en la seguridad de los sistemas informáticos (Mayer, 2017).

4.3 Postura Intermedia: los Delitos Informáticos son Pluriofensivos

Esta hipótesis está compuesta por parte de las propuestas anteriormente explicadas, dado que sostiene que los delitos informáticos protegen un bien jurídico específico, propiamente informático, a la vez que estos tutelan otros bienes jurídicos tradicionales como la intimidad o privacidad, el patrimonio y la fe pública (Mayer, 2017).

En Chile, Romina Moscoso señala que estos delitos informáticos protegen la confidencialidad del soporte lógico, a la vez que existen otros intereses que son afectados por estas conductas, pudiendo resultar afectadas la intimidad, el patrimonio, la fe pública o la vida (2014). En nuestro país, el profesor Villavicencio coincidió con este planteamiento mixto al señalar que nos encontramos ante delitos pluriofensivos, dado que el bien jurídico protegido en los delitos informáticos se aprecia en dos planos "de manera conjunta y concatenada" (2014, pág. 248). El primero de ellos corresponde a la protección de la *información* de manera general (la que es almacenada, tratada y transmitida mediante los sistemas de tratamiento automatizado de datos); mientras que el segundo abarca los demás intereses afectados, tales como la indemnidad sexual, la intimidad, el patrimonio, entre otros (Villavicencio, 2014).

Asimismo, el legislador peruano, con anterioridad, se había adherido a esta postura. En el año 2012, cuando se evaluaban los proyectos de ley que proponían la promulgación de la Ley de Delitos Informáticos, la Comisión de Justicia y Derechos Humanos del Congreso de la República (2012) echó mano de la doctrina de aquel entonces para admitir que, en su concepción, los delitos informáticos son delitos pluriofensivos.

Esta Comisión de nuestro Congreso de la República (2012), citando a Santiago Acurio del Pino (s.f.), señaló que el bien jurídico en general a ser protegido es la "información", cuyas formas (según el autor citado) pueden presentar un valor económico y, al mismo tiempo, acogen a la confidencialidad, integridad, disponibilidad de la información y de los sistemas informáticos donde se almacena o transfiere. Finalmente, la Comisión concluyó lo siguiente:

> Como podemos apreciar, el espectro de bienes jurídicos protegidos por los tipos penales denominados delitos informáticos es cada vez mayor, y eso, en buena cuenta demuestra el antes referido carácter de pluriofensivo de los mismos y, además, el cómo, tales delitos pueden afectar en simultáneo a más de un bien jurídico tradicional o de reciente incorporación en el sistema jurídico. (Congreso de la República, 2012, pág. 9)

Por lo demás, en la Ley de Delitos Informáticos se admite la protección de ambos tipos de intereses: la de los sistemas y datos informáticos, así como los bienes

jurídicos tradicionales. En efecto, en su artículo 1° se establece que aquella tiene como objeto:

> Prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia. (Ley N° 30096, 2013.)

Si bien dicho artículo no ha sido objeto de modificaciones, su lectura puede ser complementada con la finalidad establecida en el Convenio de Budapest, en cuyo preámbulo se establece que su adopción es necesaria "para prevenir los actos que pongan en peligro la confidencialidad, la integridad y la disponibilidad de los sistemas, redes y datos informáticos, así como el abuso de dichos sistema, redes y datos, garantizando la tipificación como delito de dichos actos." (Consejo de Europa, 2001, pág. 2).

Sin perjuicio de las posturas y nomenclaturas doctrinales, vemos que la Ley de Delitos Informáticos concibe la concepción amplia y estricta anteriormente explicada, dado que podemos ver que su articulado contiene delitos que implican la vulneración de bienes jurídicos tradicionales, así como delitos propiamente informáticos.

5. Conclusiones

Las posturas señaladas nos muestran que la identificación del bien jurídico protegido en los delitos informáticos dependerá, principalmente, si es que nos referimos al sentido amplio o al sentido estricto de los delitos informáticos.

Por una parte, no resulta complejo identificar el bien jurídico protegido en los delitos informáticos en sentido amplio, en la medida que aquel dependerá del interés vulnerado o puesto en peligro con la acción típica.

No obstante, cuando nos referimos a los delitos informáticos en sentido estricto encontramos diferencias entre quienes señalan que se protegen los datos o la información de los sistemas informáticos, quienes sostienen la protección de la funcionalidad informática y otras tantas (Mayer Lux expone muchas otras posturas en su trabajo del año 2017, las que podrían ser expuestas en detalle en otro trabajo de mayor extensión).

Sin perjuicio de lo anterior, resulta importante que se continúe el estudio y el desarrollo académico referido a los delitos informáticos o la criminalidad informática. En su momento, el profesor Villavicencio se ocupó de la novísima modificación a la Ley, ahora es nuestro turno de estudiar y abordar estos aspectos, el desarrollo tecnológico y la realidad lo sugieren.

REFERENCIAS

Ambos, K. (2015). Responsabilidad penal internacional en el ciberespacio. *InDret, Revista para el análisis del derecho.* Obtenido de: https://indret.com/wp-content/themes/indret/pdf/1129.pdf.

Ley N° 27309, 2000. *Ley que incorpora los delitos informáticos al Código Penal*. 15 de julio, 2000.

Congreso de la República. (2012, 20 de julio). *Dictamen de la Comisión de Justicia y Derechos Humanos recaído en los Proyectos de Ley 034/2011-CR, 307/2011-CR y 1136/2011-CR con un texto sustitutorio por el que se propone la Ley de los delitos informáticos. Comisión de Justicia y Derechos Humanos, periodo anual de sesiones 2011 – 2012.* Obtenido de: http://www2.congreso.gob.pe/Sicr/ApoyComisiones/comision2011.nsf/DictamenesFuturo/A720FCB4E0B6048A05257A4600510861/%24FILE/JUSTICIA.34.307.1136-2011-CR.May.Txt.Sust..pdf

Ley N°30076, 2013. *Ley que modifica el Código Penal Código Procesal Penal, Código de Ejecución Penal y el Código de los Niños y Adolescentes y crea registros y protocolos con la finalidad de combatir la inseguridad ciudadana.* 18 de agosto, 2013.

Ley N° 30096, 2013. *Ley de Delitos Informáticos.* 21 de octubre, 2013.

Congreso de la República. (2013, 18 de diciembre). *Dictamen de la Comisión de Justicia y Derechos Humanos, recaído en los Proyectos de Ley 2991/2013-CR, 2999/2013-CR y 3017/2013-CR con un texto sustitutorio mediante el cual se propone la Ley que modifica la Ley 30096, Ley de Delitos Informáticos.* Obtenido de: http://www2.congreso.gob.pe/Sicr/ApoyComisiones/comision2011.nsf/DictamenesFuturo/442F7718B092018B05257C580059541C/$FILE/JUSTICIA_2991.2999.3017-2013-CR_TxT.Fav.Sus.Mayor%C3%ADa.pdf

Ley N° 30171, 2014. *Ley que modifica la Ley 30096, Ley de Delitos Informáticos.* 09 de marzo, 2014.

Congreso de la República. (2019, 12 de febrero). *Resolución Legislativa que aprueba el Convenio sobre la Ciberdelincuencia, Resolución Legislativa N° 30913*. Lima: Diario Oficial El Peruano

Consejo de Europa. (2001, 23 de noviembre). *Convenio sobre la Ciberdelincuencia.* Obtenido de: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

De la Mata, N. (2007). Los delitos vinculados a las tecnologías de la información y la comunicación en el Código Penal: panorámica general. *Cuadernos penales José María Lidón.* (4), 41 – 84. Obtenido de: http://www.deusto-publicaciones.es/deusto/pdfs/lidon/lidon04.pdf

Lara, J., Martínez, M., Viollier, P. (2014). Hacia una regulación de los delitos informáticos basada en la evidencia. *Revista chilena de Derecho y Tecnología* (3)1, Centro de Estudios en Derecho Informático, Universidad de Chile, 101 - 137.

Londoño, F. (2004). Los Delitos Informáticos en el Proyecto de Reforma en Actual Trámite Legislativo. *Revista Chilena de Derecho Informático* (4), 171 - 190.

Mayer Lux, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista Chilena de Derecho,* (44) 1, 235 - 260.

Mayer Lux, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Revista Ius et Praxis*, (24) 1, 159 - 206.

Moscoso, R. (2014). La Ley 19.223 en general y el delito de *hacking* en particular. *Revista Chilena de Derecho y Tecnología* (3) 1, Centro de Estudios en Derecho Informático, Universidad de Chile, 11 – 78.

Pichihua, S. (17 de enero de 2020). Estos son los delitos informáticos más frecuentes en el Perú. Diario Oficial *El Peruano*. Obtenido de: https://www.elperuano.pe/noticia-estos-son-delitos-informaticos-mas-frecuentes-el-peru-88720.aspx#:~:text=DOMINGO%2028-,Estos%20son%20los%20delitos%20inform%C3%A1ticos%20m%C3%A1s%20frecuentes%20en%20el%20Per%C3%BA,amenazas%20fueron%20los%20m%C3%A1s%20frecuentes.&text=Cada%20mes%20hay%20m%C3%A1s%20de,de%20ellas%20a%20escala%20nacional.

Villavicencio, F. (2014). Delitos informáticos. *IUS ET VERITAS* (49), 284-304.